International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 03 Issue: 12 | Dec -2016 www.irjet.net p-ISSN: 2395-0072

IMAGE FORGERY DETECTION USING IMPROVED SLIC

M.Ramya[1], Mrs.P.Sridevi[2]

[1]*Research Scholar, Dept. of Computer Science, Vellalar College for women, Tamil Nadu, India*
[2] *Assistant Professor, Dept. of Computer Science, Vellalar College for women, Tamil Nadu, India*

Abstract - *The usage of digital photography has enlarged over the past few years, a trend which opens the door to perform image forgery. Image forgery has become a critical concern in many applications. Common techniques used to create forged digital images that are Copy-move and image splicing. The existing system integrates block-based and key point-based forgery detection methods with SLIC Super-pixel Segmentation algorithm. Adaptively, this algorithm segments the host image into non-overlapping and irregular blocks, the feature points are extracted from each block, and the block features are matched with one another to locate the labelled feature points. Existing procedure can approximately indicate the suspected forgery regions. SLIC image segmentation used single and global stopping criterion which reduced the accuracy of image forgery detection and it detects copy-move image forgery. The main contribution of this proposed work is to use a local termination criterion for each cluster to avoid revisiting clusters and image areas without any major changes since the last iteration. Pre-emptively stops the evolution of segment boundaries in homogeneous image regions. Another contribution of this work is to detect splicing attack also.*

Key Words: Image Manipulation, Copy-Move, Splicing, Tampering, SLIC, Pre-emptive SLIC.

I. INTRODUCTION

Image Processing is a technique to develop raw images received from cameras or sensors placed on satellites, space probes and aircrafts or pictures taken in normal day-to-day life for various applications. Digital image processing is the procedure of computer algorithms to execute image processing on digital images.

Image Forgery: Increasing applications of digital imaging includes different types of software for image processing. Such software can do an alteration in digital image by changing blocks of an image without any visually identifiable effect in the forged image. These modifications cannot be noticed by human eyes.

Image tampering is defined as adding features in to an image or eliminating important features from an image without leaving any obvious traces of tampering and image tampering is deliberate manipulation of images for malicious purposes.

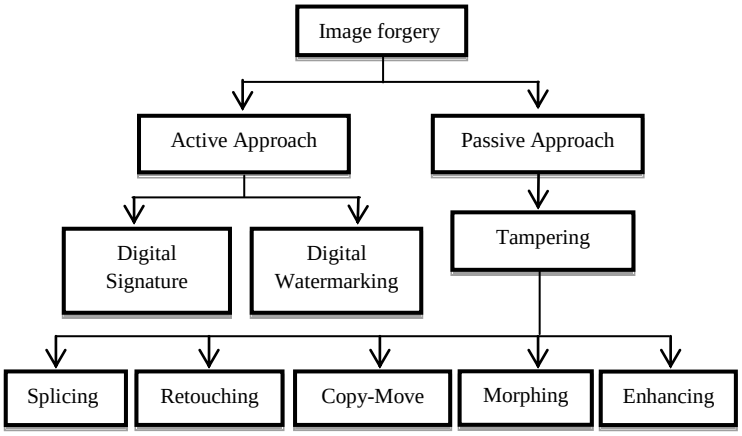

Fig-1.1 Classification of forgery techniques

Copy-move forgery (CMF) - It is an explicit type of image manipulation, somewhere a part of the image itself is copied and pasted into additional part of the same image.

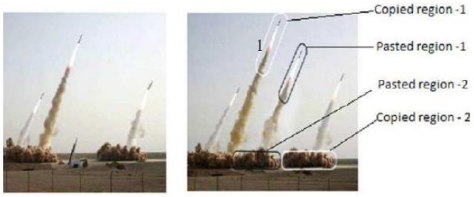

Fig-1.2 Copy-Move

Image Splicing – It is a common form of digital image manipulation or image forgery. Different elements from the multiple images are superimposed into the single composite image.

Fig-1.3 Splicing

II. LITERATURE SURVEY

Someone can alter a digital image simply without leaving noticeable traces. This harms legal forensics in the digital images such as authentication of the digital image, the copyright of image media, and so on. A blind-based method

has been considered as a new research area during the past few years. Thus, authentication of digital images is very important. Currently, many blind-based techniques for digital image forgery detection have been introduced. Some of them proposed to detect different kinds of tampered images that may be 2D composite images.

COPY-MOVE

RajdeepKaur et al., [2016]., [3] reviewed some techniques based on Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT) CMF is a special type of image forgery. An image forgery is very easily achieved due to extensive development in software technologies. The purpose of CMF is to hide or conceal some region of the image with a copied portion of original image and pasted in similar image in another area and as a result forged image is created.

A.Maria Venitta et al., [2016]., [1] discussed detection methods are Block-based and Key-point based. The forgery techniques are proposed novel CMF detection scheme using the adaptive over-segmentation and feature-point matching. Algorithm is proposed to segment host image into non-overlapping and irregular blocks adaptively according to given host images using this approach, for each image, conclude appropriate block initial size to improve the accuracy of the forgery recognition results and, at the same time, reduce the computational operating expense.

SPLICING

Bo Liu et al., [2015]., [2] It expose splicing forgery in digital images. The forged are a spliced from other picture contains some features which may be inconsistent with the rest part of image. Noise pattern and level is a potential factor to reveal such discrepancy. To detect such noise discrepancies, the test picture is initially segmented into small pieces by SLIC super-pixels algorithm. The noise features constructed in this step are utilized in energy-based graph cut to expose forged area in the final step. Experimental results show that our method provides good illustration of regions with noise inconsistency in various scenarios.

Xudong Zhao, et al., [2011]., [4] Conditional Co-occurrence Probability Matrix (CCPM) is used to detect the splicing in image based on the third order statistical features. CCPM contains the discriminative evidence which is comprised in higher order statistical features and independent to the image features. However, the higher dimensionality of features is, the more complex computation is. As a result, Principle Component Analysis (PCA) is also used to recover the computational complexity of the proposed method which is robust and better than Markov features both in spatial domain and block discrete cosine transform (BDCT) domain.

FEATURE EXTRACTION

Xunyu Pan et al., [2010]., [5] proposed a method for region duplication detection by estimating the transform between matched SIFT key-points and then finding the duplicated regions after discounting the estimated transforms. It is effective even when the duplicated regions are distorted. SIFT algorithm cannot find the reliable key-points in regions with little visual structures. Also, smaller regions having fewer key-points hard to detect. Images having intrinsically identical regions cannot be differentiated from intentionally duplicated regions.

Irene Amerini et al., [2011]., [6] proposed a methodology to support image forensics investigation based on SIFT features. It can reliably detect if a certain region has been duplicated and, determine the geometric transformation applied to perform such tampering. In a cloned image patch with highly uniform texture, salient key-points are not recovered by SIFT-like techniques.

III. SYSTEM METHODOLOGY

The Pre-emptive SLIC algorithm is used to detect Image Forgery more accurately. The splicing attack also detected by using both SLIC and Pre-emptive SLIC. An adaptive over segmentation method is proposed to segment the host image into non- overlapping and irregular blocks are called Image Blocks (IB) .Then apply Scale Invariant Feature Transform (SIFT) in each block to extract the SIFT feature points as Block Features (BF). Consequently, the block features are matched to one another are determined by labeled feature points (LFP), which approximately indicate the forgery regions. The forgery region extraction algorithm to detect the forgery region from host image according to their extracted LPF.

- To reduce the time complexity significantly
- To introduce local termination criterion for each cluster
- To detect splicing image forgeries
- To introduce new segmentation Algorithm for increasing performance

The Improved SLIC segmentation algorithm is used to detect the forged areas accurately rather than SLIC.

(i). ADAPTIVE OVER SEGMENTATION USING SLIC

The vital idea overdue SLIC is to use k-means in a local manner by reducing the potential member pixels for each cluster to a local neighborhood. SLIC uses a single, global termination criterion, the improved SLIC to use a local termination criterion for each cluster to avoid revisiting clusters and image areas without any major changes since the last iteration. Preemptively stops the evolution of segment boundaries in homogeneous image regions.

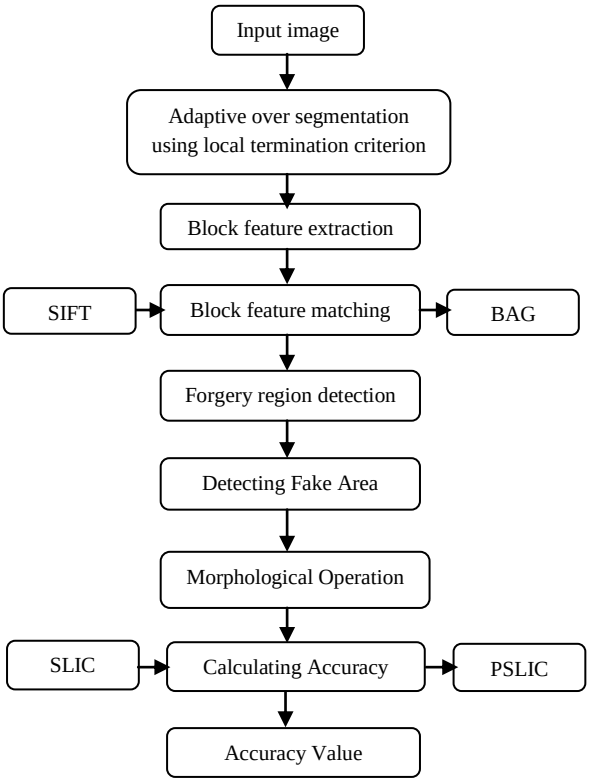

Fig-3.1. Architecture Diagram for PSLIC

Adaptive Over-Segmentation is used which determines the initial block size based on the texture of the host image. When the texture of the image is smooth, the initial size of the super-pixels is relatively large, which can ensure not only that the super-pixels will get close to the edges, but also will contain sufficient feature points to be used for forgery detection. Larger super-pixels imply a smaller number of blocks, which can reduce the computational expense when the blocks are matched with each other.

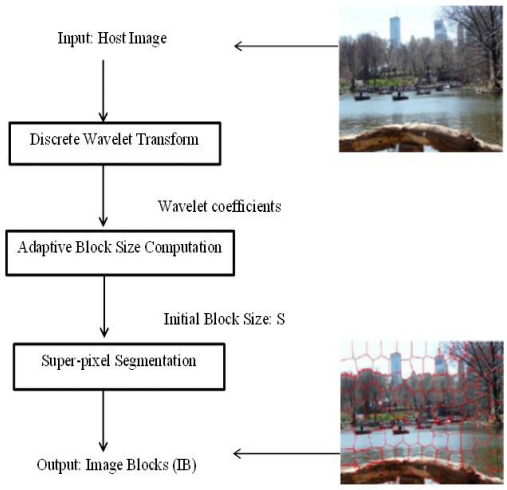

Fig-3.2. Flowchart of the Adaptive Over-Segmentation algorithm

The Discrete wavelet Transform (DWT) is used to analyze the frequency distribution of the host image. Roughly, when low-frequency energy accounts for the majority of the frequency energy, the image will appear to be smooth; otherwise, if the low-frequency energy accounts for only a minority of the frequency energy, the host image appears to be a detailed image. In this project, four-level DWT is performed, using the 'Haar' wavelet, on the host image to calculate the low-frequency energy E_{LF} and high-frequency energy E_{HF} and then the percentage of the low-frequency distribution P_{LF} is calculated, according to which the initial size S of the super-pixels is defined.

$$E_{LF} = \sum |CA_4|$$

$$E_{HF} = \sum_i (\sum |CD_i| + \sum |CH_i| + \sum |CV_i|) \qquad i = 1,2,....,4$$

Where CA_4 indicates the approximation coefficients at the 4^{th} level of DWT and CD_i ,CH_i and CV_i indicate the detailed coefficients at the i^{th} level of DWT,i1,2,...,4.

$$P_{LF} = \frac{E_{LF}}{E_{LF} + E_{HF}}.100\%$$

$$S = \begin{cases} \sqrt{0.02 \times M \times NP_{LF}} > 50\% \\ \sqrt{0.01 \times M \times NP_{LF}} \le 50\% \end{cases}$$

Where S means the initial size of the super-pixels, MXN indicates the size of the host image and P_{LF} means the percentage of the low-frequency distribution. The flow chart of the proposed Adaptive Over-Segmentation method is shown in Fig.3.2.First, consider the DWT to the host image to obtain the coefficients of the low-and high-frequency sub-bands of the host image. Then, calculated the percentage of the low-frequency distribution $P_{LF,}$ according to which determined the initial size *S*. Finally, employed the SLIC segmentation algorithm calculated initial size *S* to segment the host image to obtain the image blocks (IB).

(ii). SUPER-PIXEL SEGMENTATION

Super pixels provide a convenient primitive from which to compute local image features. They capture redundancy in the image and greatly reduce the complexity of subsequent image processing tasks. They have verified gradually useful for applications such as depth estimation, image segmentation, skeletonization, body model estimation, and object localization. For super pixels to be useful they must be fast, easy to use, and produce high quality segmentations. As will demonstrate, they often suffer from a high computational cost, poor quality segmentation, inconsistent size and shape, or contain multiple difficult-to-tune parameters. SLIC is simple to

implement and easily applied in practice – the only parameter specifies the desired number of super pixels.

(iii). SCALE INVARIANT FEATURE TRANSFORM

The original SIFT feature detection algorithm developed and pioneered by David Lowe is a four stage process that creates unique and highly descriptive features from an image. These features are designed to be invariant to rotation and are strong to deviations in scale, illumination, noise and small changes in viewpoint. The features can be used to indicate if there is any communication between areas within images. Clusters of features from an image that are related to a cluster of features from another image may indicate, with a high likelihood, areas that match. This permits object recognition to be executed by comparing features generated from input images to features generated from images of target objects. The four stages of the SIFT algorithm are as follows,

- ***Scale-space extrema***
- ***Feature localization***
- ***Orientation assignment.***
- ***Creating the feature descriptor.***

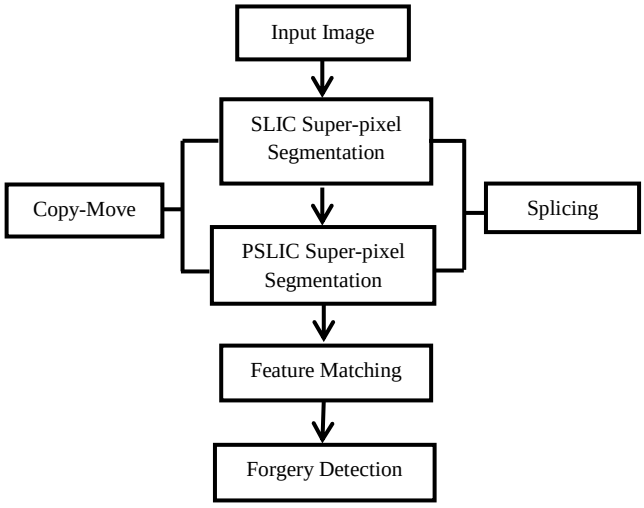

Fig-3.3. Framework for the proposed Detection scheme

(iv). BLOCK ARTIFICIAL GRID

In this module extract BAG features in the each block is extracted. It is universally known that the lossy JPEG compression will introduce some visually vertical or horizontal breaks in the image.

These interruptions called block artificial grid (BAG) appear at the boundary of each 8 × 8 pixel block. This property can be used to determine whether a picture is altered or not. If the picture is complete, block artificial grids should only contemporary on block borders, while there is a great possibility that copied and pasted or spliced regions will bring their original BAGs which may appear within the 8 × 8 block rather than at borders. Artificial grids are visually vertical and horizontal lines, and they are very weak when comparing to the border lines of objects in the picture. The core tenacity of extraction procedures is to enhance these weak lines and to make them visible.

(v). NOISE ESTIMATION

In this module identify the pattern and level of noise presented in the image. When the picture is not highly compressed and stored in high quality, the way by using BAG only becomes harder to detect forgery. To increase the versatility of the algorithm, use noise feature. The noise comes from imaging sensor and internal circuits with in a camera. And the number of noise changes in accordance with camera settings especially ISO sensitivity and exposure time. The noise can be used to help distinguish difference sources of a picture. When two pictures are spliced together the noise level or patterns are inconsistent between regions.

The noise in the image is calculated and it is used to identify the image forgeries. The similarities between the blocks are calculated to identify the copy-move or splicing attacks by Pearson correlation coefficient.

The image is considered to spatially depend on the current pixel xm, and the surrounding pixels $(m-p)$ $(n-q)$ for $(p,)\in N$ and is represented by the following model:

$$x(m,n) = \sum_{(p,q)\in N} \sum a_{p,q} x(m-p)(n-q) + u(m,n)$$

Where N represents the range of pixels neighboring xm, used in the linear sum, and $(p,)$ denotes the coordinate centered on the current pixel xm,.$u(m,n)$ indicates derived Noise and it is measured to be white Noise having a zero mean when a huge N is selected. The Noise reduction is improved in the reconstruction of an image, including additive Noise and blurred Noise. The original image model is given by

$$x(k) = AX(k-1) + U(k)$$

Where $X(k) = [X_0(k), X_1(k), \ldots X_n(k)]^T$ denotes the state variable at time k.

(vi). BLOCK FEATURE EXTRACTION ALGORITHM

It extracts block features from the image blocks (IB). The traditional block-based forgery detection methods extracted features of the same length as the block features or directly used the pixels of the image block as the block features. Conversely, those features mainly reflect the content of the image blocks, leaving out the location information. In addition, the features are not resistant to various image transformations.

In proposed algorithm, the SIFT as the feature point extraction method to extract the feature points from each image block, and each block is described by the SIFT feature points that were extracted in the corresponding block. Therefore, each block feature contains irregular block region information and the extracted SIFT feature points.

(vii). BLOCK FEATURE MATCHING ALGORITHM

It have obtained the block features (BF), must locate the matched blocks through the block features. In most of the existing block-based methods, the block matching process outputs a specific block pair only if there are many other matching pairs in the equivalent related position, assuming that they have the same shift vector. When the shift vector exceeds a user-specified threshold, the matched blocks that contributed to that specific shift vector are acknowledged as regions that might have been copied and moved. In our algorithm, because the block feature is composed of a set of feature points, proposed a different method to locate the matched blocks. Fig. 3.4 shows the flowchart of the Block Feature Matching algorithm.

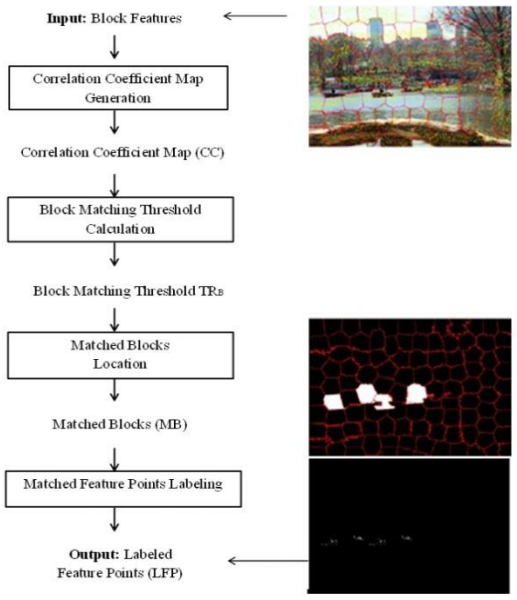

Fig-.3.4. Flowchart of the Block Feature Matching algorithm

The quantity of matched feature points is calculated, and the correlation coefficient map is generated, then, the corresponding block matching threshold is calculated adaptively with the result, the corresponding block pairs are located and lastly, the matched feature points in the matched block pairs are extracted and labeled to locate the position of the suspected forgery region. The detailed steps are explained as follows.

Algorithm: Block Feature Matching algorithm

Input: Block feature (BF)

Output: Labeled feature points

1. Load the Block Features $BF = \{BF_1, BF_2, \ldots BF_N\}$ where N means the number of image blocks
2. Calculate the correlation coefficient of the image blocks $d(f_a, f_b).TR_B \leq d(f_a, f_i)$
3. Calculate the block matching threshold TR_B according to the distribution of correlation coefficients $.\nabla^2(CC_S) > \overline{\nabla(CC\_S)}$
4. Locate the matched blocks *MB* according to the block matching threshold TR_B
5. Label the matched feature points in the matched blocks *MB* to indicate the suspected forgery regions.

(viii). FORGERY REGION EXTRACTION ALGORITHM

In this algorithm, extracted the labeled feature points (LFP), which are only the locations of the forgery regions, and locate the forgery regions. Considering that the super-pixels can segment the host image very well, proposed a method by replacing the LFP with small super-pixels to obtain the suspected regions (SR), which are combinations of labeled small super-pixels. Furthermore, to improve the *precision* and *recall* results, measure the local color feature of the super-pixels that are neighbors to the suspected regions (SR) if their color feature is similar to that of the suspected regions, then merge the neighbor super-pixels into the corresponding suspected regions, which generates the merged regions (MR).

Finally, a close morphological operation is pragmatic to the merged regions to make the detected copy-move forgery regions. Fig.3.5 shows the flowchart of the Forgery Region Extraction algorithm, which is explained in detail as follows.

Algorithm: Forgery Region Extraction

STEP-1: Load the Labeled Feature Points (LFP), apply the SLIC algorithm with the initial size *S* to the host image to segment it into small super-pixels as feature blocks, and replace each labeled feature point with its corresponding feature block, thus generating the Suspected Regions (SR).

STEP-2: Measure the local color feature of the super-pixels neighbor to the SR, called neighbor blocks when their color feature is similar to that of the suspected regions, merge the neighbor blocks into the corresponding SR, therefore creating the merged regions (MR).

STEP-3: Apply the morphological close operation into MR to finally generate the detected forgery regions.

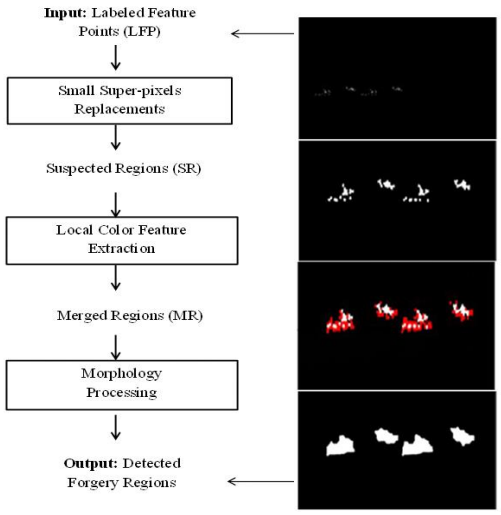

Fig-.3.5. Flowchart of the Forgery Region Extraction algorithm

(ix). SLIC & PSLIC

SLIC : Simple linear iterative clustering (SLIC), which adapts k-means clustering to generate super-pixels. While strikingly simple, SLIC is shown to yield state of-the-art adherence to image boundaries on the Berkeley benchmark and outperforms existing methods when used for segmentation on the PASCAL and MSRC datasets. **PSLIC :** Preemptive SLIC, is a faster version of SLIC. It runs at frame-rate (30 Hz) on a standard desktop CPU and conserves the high segmentation quality level of SLIC. The runtime improvement comes from two step, an optimized implementation and an preemptive termination criterion for each local cluster. Preemptive SLIC also showed to create more stable segmentations.

Step-1: Segment the input image using Improved SLIC Segmentation (Local Criterion Segmentation).
Step-2: Using the segmented image, estimate image noise and extract SIFT features for detecting Forged area.
Step-3: Analyze noise pattern of each segment for using noise estimation.
Step-4: The image is forged by copy –move if the correlation between the blocks is high.
Step-5: The Improved SLIC method is also detect Splicing attack.

IV. RESULTS AND DISCUSSION

Super-pixel Segmentation is used to measure the accuracy of Image forgery detection area, the Sensitivity (Recall) and Specificity (Precision) values are calculated for SLIC and PSLIC.

(i). EXPERIMENTAL ANALYSIS

The existing and proposed work detects Copy-Move and Splicing image Forgery using SLIC and PSLIC Super-pixel Segmentation, Feature Extraction, Feature Matching and Region Extraction. The Process of proposed work includes the following steps:

- Dataset is extracted from Forensic Repository.
- Images are segmented through Adaptive Over-segmentation process using SLIC in existing work, the features are extracting from block-based image and the feature points are matching using feature point matching algorithm. The SLIC includes the Global criterion function. The forged area is detected and extracted using Forgery Region extraction algorithm.
- Images are segmented through Adaptive Over-Segmentation process using PSLIC Super-pixel Segmentation algorithm in the proposed work, the BAG features are extracting based on feature point matching algorithm, the PSLIC includes local criterion function implies of global criterion function. The forged area is detected and it's extracted using Forgery Region extraction algorithm. Forgery attacks are detected using both SLIC & PSLIC, Finally Sensitivity and Specificity values are calculated to compute the accuracy of the algorithm.

(ii). CONFUSION MATRIX

Confusion matrix is appraised to make decision that can be made by classifier.

Table-1,2 Confusion matrix of Copy-Move & Splicing

EXISTING SLIC		Predicted	
		Background	Forged
True	Background	57301.0	55.0
	Forged	7797.0	383.0
PROPOSED PSLIC		Predicted	
		Background	Forged
True	Background	60078.0	25.0
	Forged	5020.0	413.0

EXISTING SLIC		Predicted	
		Background	Forged
True	Background	56636.0	196.0
	Forged	7255.0	1449.0
PROPOSED PSLIC		Predicted	
		Background	Forged
True	Background	58543.0	128.0
	Forged	5348.0	1517.0

(iii). COMPARISON RESULT

Table-3. Comparison result

	PRECISION		RECALL	
	SLIC	PSLIC	SLIC	PSLIC
Image 1	0.5815	0.6094	0.5815	0.6094
Image 2	0.5232	0.5405	0.5232	0.5405
Image 3	0.5229	0.5378	0.5229	0.5378
Image 4	0.5349	0.5514	0.5349	0.5514
Image 5	0.5328	0.5487	0.8887	0.9150
Image 6	0.5843	0.6200	0.8684	0.9136
Image 7	0.5397	0.5563	0.8872	0.9151

	F-MEASURE		ACCURACY	
	SLIC	PSLIC	SLIC	PSLIC
Image 1	0.7014	0.7329	88.6307	91.6443
Image 2	0.6560	0.6832	88.1317	92.9703
Image 3	0.6553	0.6823	88.0188	92.3019
Image 4	0.6634	0.6892	87.5900	91.2567
Image 5	0.6662	0.6860	87.6450	91.7648
Image 6	0.6986	0.7387	87.2360	91.1835
Image 7	0.6711	0.6920	87.3260	91.1377

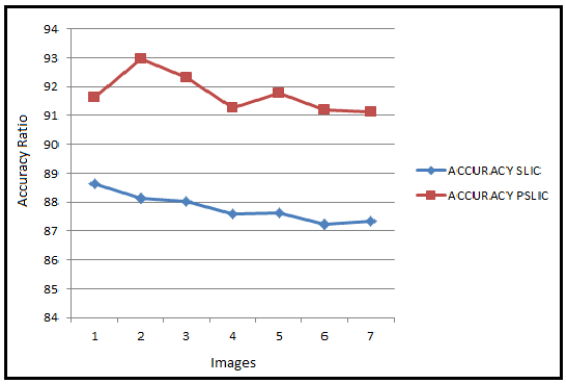

Chart-1. Comparison of Accuracy values for existing and proposed work

(iv). DETECTION RESULTS

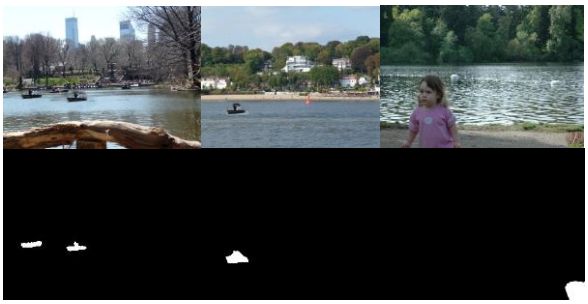

Fig-4.1. The Experimental Result for the Forged Area

Fig-4.2 (a)Original Image (b)DWT Image (c)SLIC Segmentation (d)PSLIC Segmentation (e)Detection Result of SLIC (f)Detection Result of PSLIC

V. CONCLUSION

This Research Work discussed the two main types of image manipulation, copy-move and splicing forgery. The existing Simple Linear Iterative Clustering (SLIC) includes block based, key point based algorithm and feature point matching algorithm to detect the forgery region. The forgery area is not accurately detected, time complexity and efficiency is very poor in existing system. To overcome the drawbacks the improved Pre-emptive Simple Linear Iterative Clustering (PSLIC) algorithm is used. The proposed PSLIC super-pixel segmentation algorithm using the same approach for each image with improved segmentation algorithm and local criterion function. The forgery area is detected, more accurately than the existing system with minimum error rate and maximum accuracy. The proposed algorithm detects both Copy-Move and Splicing forgery effectively. Future work may focus on applying the proposed method to detect other kind of forgery and other types of media, for example, video and audio.

BIBLIOGRAPHY

[1] **A.MariaVenitta, V.SheejaKumari,** "Image Forgery Detection Using Feature Point Matching", International Journal of Innovative Research in Science, Engineering and Tech , Volume 5, Special Issue 3, March 2016

[2] **Bo Liu and Chi-Man Pun,** "Splicing Forgery Exposure in Digital Image by Detecting Noise Discrepancies", *International Journal of Computer and Communication Engineering, Vol. 4, No. 1, January 2015*

[3] **RajdeepKaur and AmandeepKaur,** "A Review of Copy-Move Forgery Detection Techniques", RACST - International Journal of Computer Science and Inf. Tech & Security (IJCSITS), Vol.6, No.2, Mar-April 2016

[4] **Xudong Zhao, Shilin Wang, Shenghong Li and Jianhua Li,** "Passive Detection of Image Splicing using Conditional Co-occurrence Probability Matrix", 2011 Asia Pacific Signal and Inf. Processing Association, Xi'an, China, 18-21 Oct. 2011.

[5] **X. Pan and S. Lyu,** "Region duplication detection using image feature matching," IEEE Trans. IFS, vol. 5, no. 4, pp. 857–867, Dec. 2010.

[6] **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 Trans, IFS vol. 6, no. 3, pp. 1099–1110, Sep. 2011.