Nonoverlapping Adaptive Oversegmentation Method for ICMF Detection

Parvathy R. Krishnan
M.Tech Student
Department of Computer Science and Engineering
Sarabhai Institute of Science and Technology
Vellanad, Trivandrum, India

Shine V.
Assistant Professor
Department of Computer Science and Engineering
Sarabhai Institute of Science and Technology
Vellanad, Trivandrum, India

***Abstract*— Pictures are the most common and convenient means of transmitting information. Due to improvement in computing and network technologies is used for manipulating digital images and creating different forgery in image which is very difficult to identify. Image forgery can be defined as the manipulation of images using the advanced technological tools. Copy-move technique is the most popular image forgery. In this paper, to detect forgery implementing an Image Copy-Move Forgery Detection (CMFD) is using Adaptive Oversegmentation. This scheme based on adaptive oversegmentation. Adaptive oversegmentation segments the host image into nonoverlapping and irregular blocks adaptively. In this scheme, segment the test image into semantically independent patches. Copy-move regions can be identified by matching between these patches. The matching process consists of two processes, firstly find the suspicious pairs of patches that may contain CMF regions, and roughly estimate the transform matrix. After that an EM based algorithm is designed to refine the estimated matrix and to confirm the existence of copy-move forgery.**

***Keywords*— Copy move forgery, adaptive oversegmentation, image forgery**

I. INTRODUCTION

A picture is worth a thousand words. Pictures provide information about positions, sizes and inter-relationships between objects. The aim of digital image forensics is to analyze images to determine their authenticity. Digital crime, together with constantly upcoming software technologies, is growing at a rate that far surpasses defensive measures. The basic idea of image forensics is to uncover the traces left during the image creation or other successive processing regarding different stages of image life cycle. Image forgery means manipulation of images using the advanced technological tools like photoshop, corel draw, ERDAS etc [2]. These advanced tools are so expert that manipulated images become difficult to detect the forgery part by genuine sight of the human being.

An image can be manipulated easily through image-processing tools and use for hiding some meaningful or useful information to make forged images. Image forgery is seen in all area of our life, from fabricated insurance claim to scientific fraud, from magazine cover to false propaganda, from defamation to newspaper, images are no longer displaying the truth. The basic aim of image forensics is to address image integrity and authenticity.

An image can be manipulated with variety of manipulation techniques such as scaling, rotation, resizing, blurring, resampling, filtering, tampering, cropping, adding noise, removing/inserting an object etc. and integrity of image is lost. In copy-move forgery (or cloning), [1] part of the image of any size and shape is copied and pasted to another location in the same image to hide the important information or to duplicate portions of the image. As the copied part came from the same image, its properties such as noise, color and texture do not change and make the detection process difficult. CMF may be performed by a forger aiming either to cover the truth or to enhance the visual effect of the image. Normal human might neglect this malicious operation when the forger deliberately hides the tampering trace. Such a challenge triggered a wide interest among researchers to develop an effective CMF detection (CMFD) method to automatically identify the clone regions in the image. So CMFD is becoming one of the most important and popular digital forensic techniques currently. In the Fig1: the building is hided with some other parts of the same image

Fig 1: CMF examples: The left column gives the original image and right column gives the image with CMF

The remaining paper is organized as follows. Section II discusses related works .In section III, the proposed system has been described which includes architectural design. Section IV includes implementation details of the proposed system. Section V summarizes the contents of the paper.

II. RELATED WORKS

In recent years many works has been done in the area of copy move forgery detection. In [3] the authors proposed a wavelet based approach and in this technique forged image is reduced in dimension using DWT. Here the compressed image is divided into overlapping blocks of fixed size then these blocks are sorted using lexicographic sorting. Duplicated blocks are identified using Phase Correlation. This method has lower computational complexity but not suited for rotated and scaled regions.

Another method [4] based on a scheme to detect duplicated regions undergone reflection, rotation or scaling. Here overlapping pixel-blocks are mapped to color-dependent features and then lexicographically sorted to bring similar blocks closer to each other. To perform the efficient search, every pixel-block is also mapped to a 1-D descriptor. This method is not suited for images with large regions with very little textural information.

In [5] the authors aim to answer which copy-move forgery detection algorithms and processing steps perform best. Here created a challenging evaluation framework. Evaluation is conducted in two steps: per image basis and per pixel basis Experiments show that keypoint based (SIFT) can be very efficiently executed but In block based, recommend to use Zernike.

In [6] proposed a block-based matching approach based on DCT. Here divide the input image into overlapping blocks and apply DCT then search for the duplicated blocks in the image. Duplicated regions were detected by lexicographical sorting.
This method is robust to noise and compression but fail for any type of geometrical transformations of the query block and this method is better than PCA.

SIFT and SURF for the purpose of feature extraction and forgery detection. Here the input image is first converted into gray scale. The feature vectors are identified using SIFT or SURF. Then the matching process is done for single and multiple cloning detection. Finally post processing is done and forged region is detected. Experiments shows that SIFT is more accurate but SURF reduces the time complexities. [7]

III. PROPOSED SYSTEM

The main challenge in the image forgery area is the **a**dvanced tools are so expert, that manipulated images became difficult to detect the forgery part by genuine sight of human beings. Also not easy to accurately locate and distinguish the copying source region and the pasting target region, Existing systems are not efficient in detecting flat, rotated or scaled duplicate regions. Overlapping of blocks occurs due to pixel size variation. Recall and precision rate is low because in blocking method is in regular shape. Calculations are carried out using mean and standard deviations and also no tables are used for keeping data so data may be missed and unable to get better detection. Forgery regions cannot detected correctly due to overlapping of blocks

The work proposed by this paper is to create a scheme based on adaptive oversegmentation. Adaptive oversegmentation [8] method segments the host image into nonoverlapping and irregular blocks adaptively. The main advantage of this proposed scheme is overlapping can be avoided by implementing adaptive oversegmentation. Proposed method can detect forged regions accurately and can be applicable to geometrically transformed regions also tables are used for keeping data so obtain better results. This scheme integrates both the traditional block-based forgery detection methods and keypoint-based forgery detection methods.

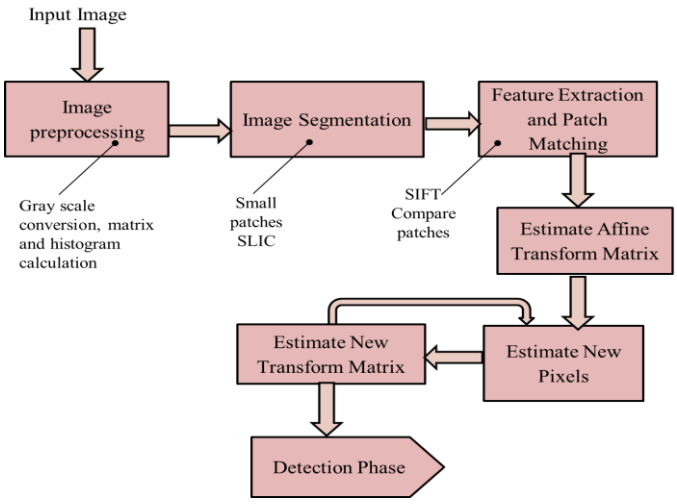

Fig 2: Architectural Design of Image Copy Move Forgery Detection System using Adaptive Oversegmentation

Fig 2 shows the architectural Design of Image Copy Move Forgery Detection System using Adaptive Oversegmentation. In the proposed design, the input image is browsed and converted to gray scale. This can be done in image processing process. Then matrix value and histogram is calculated. In image segmentation, the image should be segmented in to small patches. SLIC method is used for this. In feature extraction, keypoints can be detected using SIFT method. After that check for suspicious pairs of patches that have many similar keypoints. Then estimate the relationship between two regions in the form of transform matrix. For accurate value, search new pixels and re-estimate the affine transform matrix. Here EM method is used and repeat the process till get a converging value.

IV. IMPLEMENTATION

Segmentation is used in this proposed scheme. In order to separate the copying source region from the pasting target region, the image must be segmented into small patches, each of which is semantically independent to the others. Feature extraction can be carried out using SIFT method. To avoid overlapping of blocks and address significant geometrical transformations use adaptive oversegmentation.

A. *Image Segmentation*

The input image is converted into gray scale image. After gray scale conversion, binarization is performed. Then generate a histogram. In order to separate the copying source region from the pasting target region, the image should be segmented to small patches, each one is semantically independent to the others. Segmentation can be carried out using Simple Linear Iterative Clustering (SLIC) method [9]. SLIC adapts k means clustering but it is somewhat different from k means. Proposed method generate superpixels which is faster than existing methods, more memory efficient, exhibits state-of-the-art boundary adherence, and improves the efficiency of segmentation algorithms.

Simple linear iterative clustering is an adaptation of k-means for superpixel generation, with two important distinctions:

- The number of distance calculations in the optimization is dramatically reduced by limiting the search space to a region proportional to the superpixel size. This reduces the complexity to be linear in the number of pixels N and independent of the number of superpixels k.

- A weighted distance measure combines color and spatial proximity while simultaneously providing control over the size and compactness of the superpixels.

SLIC is simple to use. By default, the only parameter of the algorithm is k, the desired number of approximately equally sized superpixels. SLIC algorithm consists of five steps:

Step 1: Initialize cluster centers C_k

Step 2: Assign each pixel i is associated with the nearest cluster center then introduce a distance measure D, which determines the nearest cluster center for each pixel

Step 3: Compute new cluster centers by averaging all of the pixels in the cluster

Step 4: compute a residual error E between the new cluster center locations and previous cluster center locations

Step 5: Repeat assignment and update steps iteratively until the error converges

Fig 3: Images segmented using SLIC into superpixels of size 64, 256, and 1,024pixels (approximately)

The main difference between k means and SLIC are in the conventional k-means algorithm, distances are computed from each cluster center to every pixel in the image and SLIC only computes distances from each cluster center to pixels within a 2S×2S region. The expected superpixel size is only S×S, indicated by the smaller square.

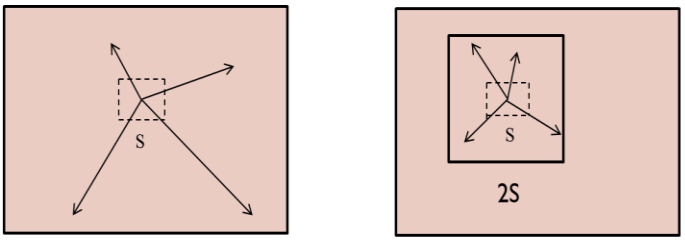

Fig 4: Reducing the superpixel search regions

B. *First Stage of Matching*

First stage of matching includes:

- Feature Extraction
- Patch Matching
- Affine Transform Matrix Estimation

Keypoints or features can be detected using SIFT (Scale Invariant Feature Transform) method [10]. This method can be summarized as the following four steps:

1. Scale-space extrema detection: Features are detected at different scales using a scale space representation. The interest points are calculated as local extrema in the scale space.
2. Keypoint localization: The keypoints are taken from extrema detection. For accurately locating the keypoints, reject low contrast and poorly localized keypoints.
3. Assignment of one (or more) canonical orientations: Each keypoint is assigned one or more orientations based on local image gradient directions. To achieve rotation invariance canonical orientation is needed.
4. Generation of keypoint descriptors: Considering the keypoint as a high dimensional vector. Compute a descriptor vector for each keypoint such that the descriptor is highly unique and partially invariant to the remaining variations such as illumination, 3D viewpoint, etc.

After SIFT method, adaptive oversegmentation can be carried out. First, employ the DWT to the host image to obtain the coefficients of the frequency sub-bands of the input image. Compute the adaptive block size and employ SLIC segmentation method to obtain the image blocks.

In patch matching, check for the suspicious pairs of patches that have many similar keypoints. This process is performed by comparing each patch with the others. Assume that patch A is considered. Define the distance between two keypoints by the L-2 norm of the difference between their descriptors. In patch A for each keypoint, search its *K* nearest neighbors that are located in the other patches. Considering there are usually more than one couple of copy-move regions in the image, set $K = 10$ in implementation. Then should not take all the *K* searched keypoints into consideration, but only if the difference is smaller than a threshold (0.04 in implementation), the two keypoints are considered to be matched.

In other words, each keypoint in patch A is corresponding to no more than K keypoints in the remaining patches. The target and source regions should have a large proportion of matched keypoints. If a large proportion of the matched correspondences of A are located in another certain patch, say B. A and B are considered to be a suspicious pair of patches where may find CMF regions. So a threshold ϕ is defined to find the matched patches.

In affine transform matrix estimation, after detecting a suspicious pair of patches, understand where the copying source region and pasting target region are. Then we estimate the relationship between these two regions in terms of a transform matrix H, such that

$$\vec{x'} = H\vec{x}$$

where $\vec{x}$ and $\vec{x'}$ are the coordinates of the pixels in the copying source region and pasting target region, respectively. In forensic method, need better value, so there is a need of second stage of matching.

C. *Second Stage of Matching*

In the first stage of matching process found that the suspicious pairs of patches as well as the transform matrix between them. Some of the detected patches may be just false alarm containing not any CMF regions. So introduce a second stage of matching process where the estimation of the transform matrix is refined via an EM-based algorithm and the false alarm patches might also be eliminated in this stage.

Here searching new pixels for more accurate estimation. Then adaptive oversegmentation can be carried out here. Affine transform matrix is re-estimated to get the accurate value. EM algorithm is used here. EM algorithm consists of E (Expectation) and M (Maximization) steps. The EM algorithm is a useful method for statistical parameter estimation of the samples with underlying distributions. The algorithm repeats a procedure until a target variable converges. The procedure consists of an E-step and an M-step. In the E-step, calculate the following value which is an expectation of the log likelihood $P(X, z|H_n)$, with respect to the conditional distribution $P(z|X, H_{n-1})$ ie.,

$$Q(H_n|H_{n-1}) = E_{z|X,H_{n-1}} l_n[P(X, z|H_n)],$$

where X represents all the coordinates of the pixels in the current patch, namely $X = (\vec{x1}, \vec{x2}, \ldots\ldots \vec{xn})$, if pixel located in the CMF region then z = 1 else z=0, Hn-1 is the affine transform matrix.

Then in the M-step calculate H_n via maximizing Q. If the new estimated matrix H_n is similar to Hn-1, stop the iteration and output $H = H_n$. Otherwise, take H_n as the initial estimation and repeat the above two steps.

These two steps can be explained as follows. The estimation of transform matrix Hn-1, and want to obtain a new one Hn which is more accurate than the last one. With the help of Hn-1, for the pixels of the current patch obtain the correspondences in the matched patch. Then for each pixel a new correspondence around the original one is re-detected.

After that calculate the probability of the pixel being in the copy-move region, namely $P(z|X, H_{n-1})$. Then re-estimate a new transform matrix Hn such that the pixels in the CMF region are able to match their newly obtained correspondences as much as possible. From a statistical point of view, it is to maximize the expectation of the log-likelihood function $P(X, z|H_n)$. The entire process is repeated for all blocks. Identify whether the image is forged or not by analyzing the pixel size variation.

V. CONCLUSION

This paper is based on adaptive oversegmentation. After image preprocessing, image can be divided into patches through SLIC segmentation. Features are extracted through SIFT method and affine transform matrix is generated. But in forensic method, need better values so second stage of matching is needed. For that EM algorithm is used to re-estimate the transform matrix. In this proposed scheme, given an input image and identify whether the image is forged or not by analyzing the pixel size variation.

ACKNOWLEDGMENT

I would like to express my sincere gratitude to Dr. C.G. Sukumaran Nair (HOD), Associate Professor, Ms. Sudha S.K. and Assistant Professor, Mr. Shine V., Department of Computer Science and Engineering, Sarabhai Institute of Science and Technology, for their valuable guidance.

REFERENCES

[1] Jian Li, Xiaolong Li, Bin Yang, and Xingming Sun,"Segmentation-Based Image Copy-Move Forgery Detection Scheme*" IEEE Transactions on Information forensics and security*, Vol 10,No. 3, pp.507-518, 2015

[2] Neha Thakur and Harish Kundra,"A Survey on the Digital Image Copy Move Forgery Detection Techniques", International Journal of Advances in Science and Technology (IJAST), 2013

[3] S. Khan and A. Kulkarni, "Robust Method for Detection of Copy-Move Forgery in Digital Images" IEEE International conference on signal and image processing 2010

[4] Sergio Bravo-Solorio and Asoke K. Nandi, "Exposing duplicated regions affected by reflection, rotation and scaling,‖ in Proc. IEEE Int. Conf. Acoust.,Speech Signal Process (ICASSP), May 2011, pp. 1880–1883

[5] V. Christlein, C. Riess, J. Jordan, C. Riess, and E. Angelopoulou, "An evaluation of popular copy-move forgery detection approaches", ‖IEEE Trans. Inf. Forensics Security, vol. 7, no. 6, pp. 1841–1854,Dec. 2012

[6] Ashima Gupta, Nisheeth Saxena and S.K Vasistha, "Detecting copy-move forgery using DCT" international Journal of Scientific and Research Publications, Volume 3, Issue 5, May 2013

[7] Swapan Debbarma, Angom Buboo Singh and Kh.Manglem Singh, "Keypoints Based Copy-Move Forgery Detection of Digital Images", IEEE 2014

[8] Chi-Man Pun, Xiao-Chen Yuan and Xiu-Li Bi, "Image Forgery Detection Using Adaptive Oversegmentation and Feature Point Matching" IEEE Transactions on Information forensics and security, VOL. 10, NO. 8, 2015

[9] R. Achanta, A. Shaji, K. Smith, A. Lucchi, P. Fua, and S. Süsstrunk, "SLIC superpixels compared to state-of-the-art superpixel methods", IEEE Trans. Pattern Anal. Mach. Intell., vol. 34, no. 11, pp. 2274–2282, Nov. 2012.

[10] Swapan Debbarma, Angom Buboo Singh and Kh.Manglem Singh,"Keypoints Based Copy-Move Forgery Detection of Digital Images", IEEE 2014