International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 4 Issue 10, October-2015

Copy-Move Forgery Attack Detection using Enhanced SIFT

Prinkle Rani
M.Tech Student
Department of Computer Science & Engineering
GZS PTU Campus, Bathinda (Punjab)

Er. Jyoti Rani
Assistant Professor
Department of Computer Science & Engineering
GZS PTU Campus, Bathinda (Punjab)

***Abstract* — In today's time of computerized innovation, security turns into a noticeable issue while exchanging information starting with one spot to next spot. Information is gone in type of computerized pictures in different regions like security organizations, military, secured systems and so forth. With the headway in innovation & altering instruments like Photoshop, Corel Draw and other programming devices, it is anything but difficult to alter the pictures. Picture legal sciences decide the genuineness of the images. Image manipulation (altering) is additionally named as Image Forgery. Copy-move forgery is more basic in which one piece of the picture is replicated and stuck into another area of the same picture to conceal points of interest. It can be urgent undertakings where pictures are utilized as proof prefer court, restorative office etc. Forgery detection can be troublesome if it has connected some post handling operations like re-sizing, sifting, revolution, JPEG pressure etc. In this paper, we are going to represent a new method of Copy-Move attack detection using E-SIFT. Proposed system will detect the forgery and also estimate the parameters of transformation used (i.e. rotation, scaling etc.). It will reduce the time to detect the forgery, & enhance the overall throughput.**

Keywords* — *E-SIFT, Copy-move forgery, SIFT, Passive techniques for forgery detection.

I. INTRODUCTION

The appearance in advanced world is changing our way in which we store and control the information.Computerized pictures are speediest method for data exchange in light of their simplicity of procurement and stockpiling. These pictures can be utilized as proof prefer the pictures that are demonstrated in TV news can be acknowledged as confirmation for the honesty of that news. Forgery is the procedure of making fake pictures. Fraud is effectively conceivable with the product's similar to Adobe Photoshop, GIMP, and Corel Paint shop. Forgery may be performed to conceal essential elements of a picture or to pass on some wrong data by changing the substance. Forgerd image can change the meaning of original image.

Image tampered techniques can be divided into two major groups; Active Method and Passive Method.

Active Method requires that certain information is embedded inside an image during the creation or before the image is being disseminated to the public. The information can be used to either detect the source of an image or to detect possible modification of an image. One of the techniques under active method is watermarking.

The problem with watermarking is that it requires special hardware or software in order to insert certain information to the image. However, most of the images that we see in the internet for example, in any photo sharing websites, are not watermarked. This may be due to the fact that the digital camera that is used to create these images does not have any special hardware for inserting watermark information.

Passive method on the other hand, does not require any pre-'image distribution' information to be inserted into digital image. The method works purely by analyzing binary information of digital image, without any need for external information.

Techniques in passive method for detecting image forgery can divided into two main category, one that is based on the pixel value of the image (Statistical Method) and one that tries to detect inconsistencies in the image itself based on visual cues (Visual Method). Visual Method is the easiest because sometimes it can be performed without the need for special hardware. One way of detecting traces of image forgery by visual method is to compare lighting information from different parts of an image.

The level of details in faked image varies depending on various factors which include the competency of the perpetrator with computer graphics editing software, the time that he or she has, and the quality of the original image. Sometimes, the quality of a faked image is so convincing that it is impossible to use Visual Method to detect traces of image forgery. In these cases, techniques which are based on Statistical Method can be used to analyze these kinds of images.

Passive approach follows two steps:-

i. Image source identification:-

This category concerns with the challenges associated with the data source identification. It checks whether the image is computer generated or a natural image and also identifies the device which is used to acquisition of the image.

ii. Tampering detection:-

It detects the manipulation of images. Image forgery detection can be manipulated in numerous ways with many operations like translation, scaling and Compensation operations like colors, contrast adjustments, brightness etc., Suppression operations filtering, compression, noise extraction etc.

Pixel based techniques can be categorized into three groups, based on the method used for performing forgery:

a. Image Retouching

Image Retouching does not change or edit the whole image instead it is used for enhancing or reducing the features of an image. This method is mostly adopted by magazine or newspaper photo editors. We can say almost all magazine covers employ this technique for enhancement of pictures for making them more attractive along with ignoring the fact that this technique is ethically wrong.

b. Image Splicing

Image splicing is a technique that involves composition of two or more than two images to create a new fake image. Image splicing is defined as a paste-up produced by sticking together photographic images. This forgery is considered more harmful than Image Retouching.

c. Copy-Move Attack

Copy-Move Forgery is most commonly used forgery in which a part of an image is copied and pasted into another location of the same image. This forgery is performed in order to hide some information or to change the meaning of an image. Copy-Move attack & Image Splicing are similar in the fact that both methods modify the image regions, difference is that in Copy-Move attack, instead of taking another external image as source, it uses a part of original base image as its source we can say the source and the destination of the adjusted picture are begun from the same picture. Blurring is usually applied with the border of the tampered region to reduce the effect of irregularities between the original & the pasted region.

Copy-Move Forgery challenges:

The duplicated region may not be the exact original region. It may include some preprocessing.

- Image may be saved under Lossy compression.
- Noise may be added to image to make the forgery detection difficult.
- Region may be rotated before performing forgery.
- Copied region may be blurred.
- Copied region's texture may be changed. It may be made lighter or darker.

Fig1. Copy-Move Forgery

II. LITERATURE SURVEY

Takwa Chihaoui et al. [1] proposed a method that automatically detect duplicated regions by identifying local characteristics of the image using SIFT (Scale Invariant Feature Transform) and by using SVD (Singular Value Decomposition) for matching between identical features. This hybrid method is vigorous to Geometrical Transformations & can detect high performance duplicated regions. Sudhakar.K et al. [2] presents an effective method for detecting copy move forgery using SIFT features and used Chan-Vese's Level Set approach to reduce the volume of these features. Multiple forged object detection, high speed, invariant to scale and rotation, robustness and simplicity in implementation are strengths of this method. Mohammad Farukh Hashmi et al. [3] proposed a method based on DWT (Discrete Wavelet Transform) that is used for dimension reduction and also improves the accuracy of results. It localizes the forgery. Cao et al. [4] proposed a robust copy-move detection algorithm based on DCT for finding DC coefficients. Irene Amerini et al [5] proposed a novel methodology based on SIFT that detects the copy-move forgery and also recuperate the Geometric Transformation used for tampering. It also deals with multiple cloning.

III. PROPOSED METHOD

SIFT:-

The Scale-Invariant Feature Transform (SIFT) is used to detect & describe local features in an image. SIFT keypoints of objects are extracted from a set of images. To help the extraction of these features the SIFT algorithm applies following 4 stage filtering approach:

a) Scale-Space Extrema Detection: -Process begins with detecting points of interest, called keypoints. Image id convolved with Gaussian blurs at different scales, and then Keypoints are taken as maxima/ minima of Difference of Gaussians.

b) Keypoint Localization: -After that, SIFT algorithm discards low contrast keypoints& filters out only those that are located on edges.

c) Orientation Assignment: -One or more orientations are assigned to each keypoints based on local image gradient descriptor. This step is for achieving invariance to rotation.

d) Keypoint Descriptor: -This step computes a descriptor for every keypoint that is highly distinctive & partially invariant to the variations such as illumination, 3D viewpoint etc.

PROPOSED SYSTEM:

The proposed approach uses SIFT algorithm to extract the robust features that can allows it to discover if an area of an image was copied & pasted as well as detects which geometrical transformation was applied to perform tampering. The proposed system use cluster based approach to detect the forgery in the image. Proposed system works in the following phases:

A. Preprocessing

In this module we have to remove if any noise occurred in our input image. Noise is nothing but any undesired information that contaminants an image. Proposed system use Gaussian filter to remove the noises.

The one-dimensional Gaussian filter has an impulse response given by

$$g(x) = \sqrt{\frac{a}{\pi}} \cdot e^{-a \cdot x^2}$$

And the frequency response is given by the Fourier transform

$$\hat{g}(f) = e^{-\frac{\pi^2 f^2}{a}}$$

B. Feature Extraction

It is an algorithm in used to detect and describe the local features in an image. Interesting points on the object can be extracted to give a "feature description" of the object in an image. These features are based on color and texture values of the image. In this phase local key points are calculated along with their normalized values to make clusters in the next phase.

C. Hierarchical Clustering

Hierarchical clustering generates a hierarchy of clusters which is represented by a tree structure. These clusters are extracted using the features extracted in the previous phase.

In the proposed work Euclidean distance metric is used in hierarchical clustering. Equation for Euclidean distance is as below:

$$\|a - b\|_2 = \sqrt{\sum_i (a_i - b_i)^2}$$

Algorithm to perform hierarchical clustering is as below:

Given a set of N items to be clustered, and an N x N distance (or similarity) matrix, perform following operations:

Step 1: Assign each item to its own cluster, if you have N items, now you have N clusters, each containing only one item. Let the distances between the clusters equal to the distances between the items they contain.

Step 2: Find the nearest (most similar) pair of clusters& then merge them into a single cluster, so that now you have one less cluster.

Step 3: Compute distances between the new cluster & each of the old clusters.

Step 4: Repeat steps 2 and 3 until all items are clustered into a single cluster of size N.

D. Cluster Mean value calculation and comparison

Calculate the mean values of the clusters and compare these mean values with other clusters mean values using SIFT Operations. Brute force algorithm is used for accessing the cluster from a given set of clusters. If mean value of one cluster is matched with the mean value of other cluster than process the clusters pixel by pixel otherwise skip the cluster to save the processing time of the system.

E. Estimate the Geometric Transformation

Estimate the geometric transformations like rotation, scaling by using RANSAC (Random sample consensus) algorithm to detect the forgery.

RANSAC algorithm can explained as below:

Step 1: Selects N data items at random

Step 2: Estimates parameter

Step 3: Finds how many data items (of M) fit the model with parameter vector within a user given tolerance. Call this K.

Step 4: If K is big enough, accept fit and exit with success.

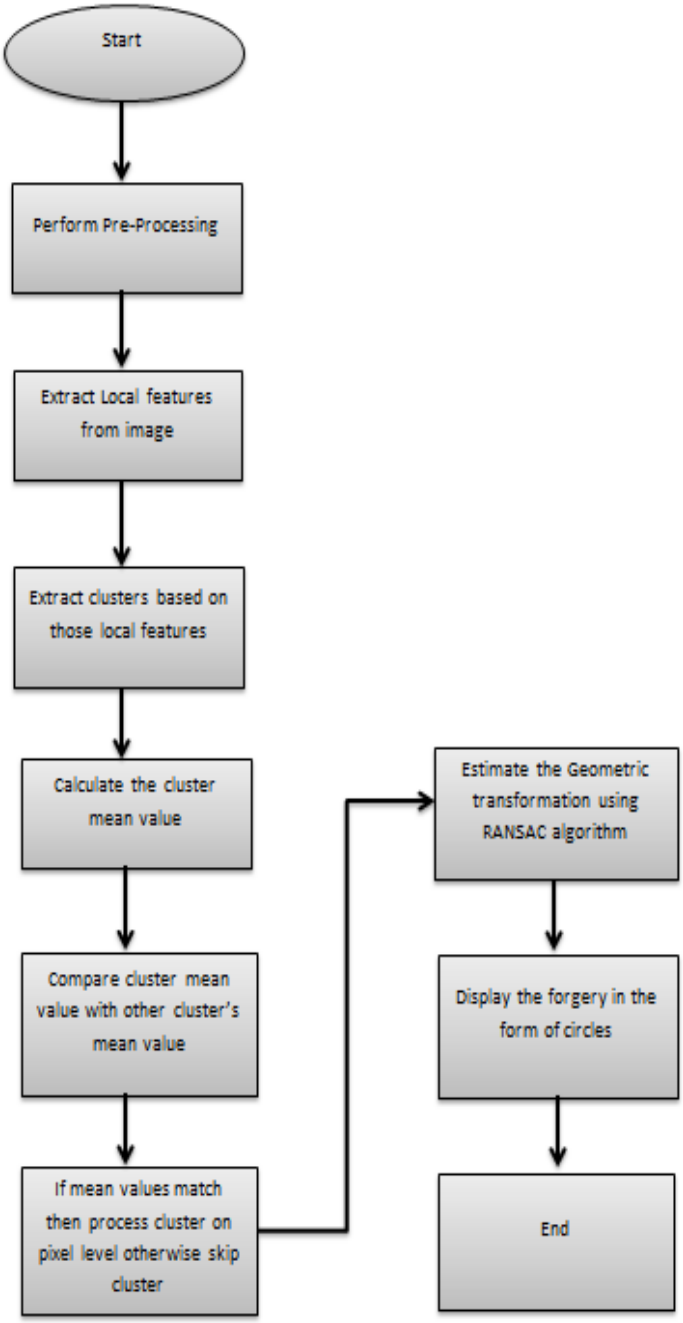
Step 5: Repeat 1...4 L times

Step 6: Fail if you get here

F. Detect Forgery

Calculate the total number of clusters matched with the other clusters and display the matching points on the image in form of circles and ellipse. These will be treated as forged areas in the given image.

FLOW CHART:



IV. DATASET

We have used the standard dataset that contains more than 30 images to evaluate the performance of the proposed system. In this dataset, forged images contains various categories of transformations like scaling, rotation etc. proposed system evaluates the results of these types of images.

TABLE I.DATASET for proposed system

S.No.	Type of Forgery	No. of Images
1	Copy-Move Forgery	16
2	Copy-Move Forgery with Scaling	7
3	Copy-Move Forgery with Rotation	7
4	Un-Forged	10

IV. EXPERIMENTAL RESULTS

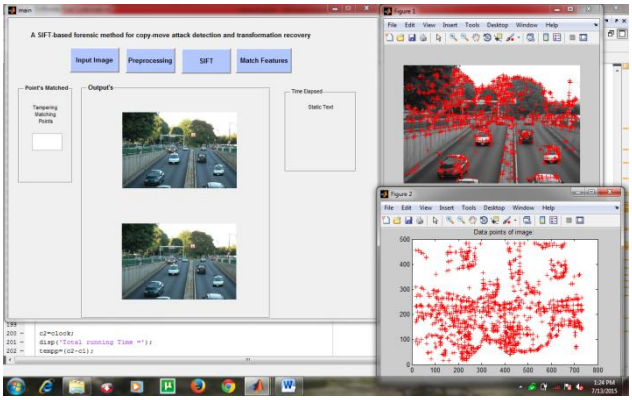


Fig 2

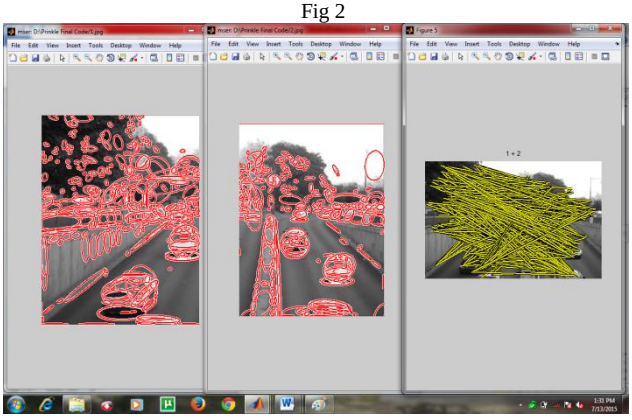


Fig 3

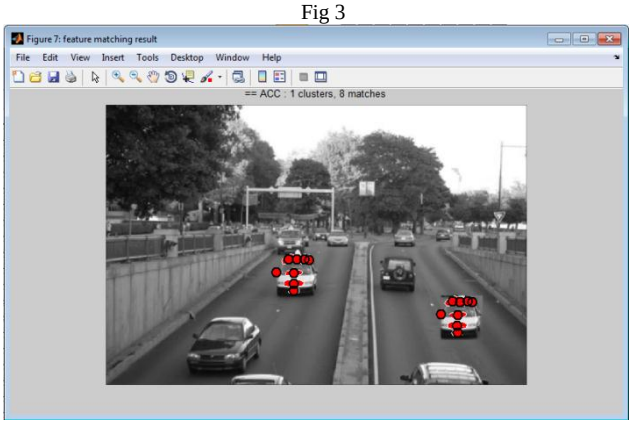


Fig 4

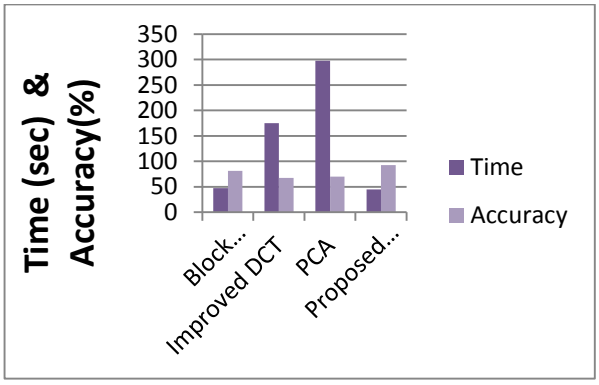
TABLE II. Result statistics shown by the proposed system:

Type of Forgery	Total No. of Images	Positive Results	Results
Copy Move Forgery	16	15	93%
Copy Move Forgery With Rotation	7	6	86%
Copy Move Forgery With Scaling	7	6	86%
Un forged	10	9	90%

TABLE III. Comparison of proposed system with existing techniques

Technique	Time	Accuracy
Block Representing method	47.05	81.27
Improved DCT	175.20	67.17
PCA	297.47	70.17
Proposed Method	45.02	92.50

GRAPH I. Graph showing the comparison between the proposed and existing systems:



V. CONCLUSION & FUTURE SCOPE

In the proposed work, we have implemented the Enhanced SIFT (E-SIFT) algorithm to detect the copy move forgery in the digital images. Proposed system is tested on various images of standard dataset. Overall Accuracy of the proposed system is calculated to as 92% which is better than that of existing algorithms. It is concluded that the proposed system shows considerably high improvement than the previous systems. Average time taken to process the input by the proposed system calculated as 45 seconds which is again less than that of existing systems. In proposed work, we use clusters and their mean values to find the forged area within the image to reduce the overall processing time. Proposed system also shows good accuracy in the images that can contain scaled forgery or forgery with geometric transformations. In future, system can be enhanced to minimize the processing time to detect the forgery in the images to few seconds or even microseconds.

VI. REFERENCES

[1] Takwa Chihaoui, Sami Bourouis, and Kamel hamrouni, 2014, "Copy-Move Image Forgery Detection based on SIFT Descriptors and SVD-Matching", 1st International Conference on Advanced Technologies for Signal and Image Processing-ATSIP'2014, Sousse, Tunisia.

[2] Sudhakar. K, Sandeep V.M, Subhash Kulkarni, 2014, "Speeding-Up SIFT based Copy-Move Forgery Detection Using Level set Approach", International Conference on Advances in Electronics, Computers and Communications (ICAECC).

[3] Mohammad Farukh Hashmi, Aaditya R. Hambarde, Avinash G. Keskar, , 2013, "Copy Move Forgery Detection using DWT and SIFT Features", IEEE 13thInternation Conference on Intelligent Systems Design and applications.

[4] Yanjun Cao, T. Gao, and qunting Yang, 2012, "A Robust Detecton algorithm for Copy-Move Forgery in Digital Images", Forensic Int. Volume 214, pp. 33-43.

[5] L.Kang, X.-P. Cheng, 2010, "Copy-Move Forgery Detection in Digital Image", 3rd International Congress on Image and Signal Processing, IEEE Computer Society, pp. 2419-21.

[6] Irene Amerini, Lamberto Ballan, 2011, "A SIFT-Based Forensic Method for Copy–Move Attack Detection and Transformation Recovery "IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 6, NO. 3.

[7] Lu Liu, Rongrong Ni, Yao Zhao, Siran Li, 2014, "Improved SIFT-based Copy-Move Detection using BFSN Clustering and CFA Features", IEEE Tenth International Conference on Intelligent Information Hiding and Multimedia Signal Processing.

[8] M.Ghorbani, M.Firouzmand, A.Faraahi, 2011, "DWT-DCT (QCD) based Copy-Move Image Forgery Detection", 18th IEEE International Conference on Systems, Signals and image Processing, pp.1-4.

[9] Bo Liu and Chi-Man Pun, 2014, "A SIFT and Local Features based Integrated Method for Copy-Move Attack Detection in Digital Image", Proceedings of the IEEE International Conference of Information and Automation Yinchuan, China.

[10] H.-J.Lin, C.W.Wang, Y.-T.Kao,"Fast Copy-Move Forgery Detection", in WESAS Transaction on Signal Processing, 2009, pp.188-97.

[11] Ms.P.G.Gomase, Ms. N.R. Wankhade, 2014, "Advanced Digital Image Forgery Detection: A Review", IOSR Journal of Computer Science (IOSR-JCE), e-ISSN: 2278-0661, p-ISSN: 2278-8727, PP 80-83.

[12] Amanpreet Kaur, Richa Sharma, 2013, "Copy-Move Forgery Detection using DCT and SIFT", International Journal of Computer Applications (0975-8887), Volume 70-No.7.