Study of Image Forgery Detection Using Scale Invariant Feature Transform

Jyothi V
Department of Computer Science and Engineering
Gokaraju Rangaraju Institute of Engineering and Technology
Hyderabad, India
jyothi1687@grietcollege.com

Sree Kavya M
Department of Computer Science and Engineering
Gokaraju Rangaraju Institute of Engineering and Technology
Hyderabad, India
sreekavya0402@gmail.com

Shvithi Reddy P
Department of Computer Science and Engineering
Gokaraju Rangaraju Institute of Engineering and Technology
Hyderabad, India
shvithireddy@gmail.com

Sri Priya Reddy G
Department of Computer Science and Engineering
Gokaraju Rangaraju Institute of Engineering and Technology
Hyderabad, India
sripriyareddy5544@gmail.com

Harshitha Reddy K
Department of Computer Science and Engineering
Gokaraju Rangaraju Institute of Engineering and Technology
Hyderabad, India
harshithareddy0369@gmail.com

Abstract— **Images are a crucial source of information and are also used as a legal references and proofs sometimes, but since the availability of it has made easy due to internet hence it is prone to many manipulations and tampering. Altering an original image in order to create fake image by means of any fraud or other reason is known as Image Forgery and has many forms of its own, the most widely used type of forgery is copy-move forgery wherein the parts of image are cut or copied and pasted in other area of same picture. As how there are different types of forgeries performed, there are also different types of forgery detection methods like block-based method, key-point based method etc. In this paper the proposed method helps in detecting the forgery performed on an image by comparing it with its original image. Using Scale Invariant Feature Transform (SIFT) algorithm, extract the invariant features from the original and tampered picture. The advantages of SIFT over other algorithms is that it helps in reducing computational expenses, increases accuracy, and provides better results.**

Keywords— **Image Forgery, Scale invariant feature transform, tampering.**

I. INTRODUCTION

In a world of constant upgrades, people have shifted from analog to digital images in an instant, this has made the access for pictures easy. Since images are carriers of information, they are used in court rooms as an evidence or proof. Digital images have their applications extended from medical to forensics.

In the present-day scenario, digital images have a major role to play. Manipulating the images have become an effortless job to most of the people using certain specific tools. Here, image processing comes into play and use it to enhance the image or get some valuable information out of it.Image Processing system is considering images as two dimensional signals. Apply signal processing methods to them which are already been set. There are different characteristics of image processing. Few of them are image enhancement, image restoration, image compression etc. Basically, the image processing undergoes three main steps. Firstly, import the image with the help of optical scanner. Next, analyze and then manipulate the image which includes data compression and image enhancement and spotting patterns. Output is the last stage in which result can be altered image or report that is based on image analysis.

Image forgery means manipulation of digital image to conceal meaningful information of the image. The primary focus is on the copy move forgery which can be detected by feature point extraction. Here, the image undergoes segmentation and divided into blocks. From each block the features are extracted and compared to one another. To find out the forgery region more accurately, forgery region extraction algorithm is proposed which replaces the features point with small pixels as feature blocks and then merges the neighboring blocks that have similar local color features into the feature block to generate the merged regions. Finally, the morphological operation is applied to merged regions to generate the detected forgery regions.

This project mainly deals with the images related to many fields. In the market, few people tend to manipulate the original image of a certain field and manipulate or alter the image which looks like the original one. Then, they try to misuse the false image thereby deceiving the customers. This in turn affects the functioning of the original field. In order to prevent this situation from happening, SIFT[14] algorithm is used to distinguish the original image from the altered image.

II. LITERATURE SURVEY:

In early 1840, the first record of image forgery was found. The person named Hippolyta barnyard was first to create a fake image.

1.proposed a method based on Transform invariant features. The method is helpful in detecting or finding the tampering within the same image.

2.Another supervised learning technique used is the Decision Tree algorithm[1] which is a popular classifier but it can be extremely sensitive to outliers in the training set, thereby, affecting the overall accuracy.

3.The survey[3] also details some unsupervised learning techniques that were employed with an improved digest algorithm or on the basis of string equivalence. Though these approaches are unconventional and not widely used, they provided satisfactory results.

4. Various methods were used to identify the forgeries out of which the frequency based methods are numerous. The [9]FMT method proposed by Bayram,Sencar and Memon is robust against post-processing operations like blurring,scaling etc but this method fails in detecting blocks with scaling more than 10%, while the [10]PHT method proposed by Leida LI, Sushang Li and Jun Wang does not yield good result when the copied region go through scaling and local lending before pasting**.**

III. PROPOSED METHOD:

Modules:

1.Feature Extraction from Original Image

2.Detection of Forgery Region

Module Description:

1.Feature Extraction from Original Image

1.1.Image Acquisition:

It is briefly described as a process of retrieving an image from any source, commonly from a hardware-based source, so that it can be processed accordingly afterwards.This step is always important and must be performed as a first step in the flow of work sequence because without an image or picture no processing can be done. The acquired image is completely unprocessed and is the raw output of the hardware source used.The original image now undergoes many stages of pre-processing required for it which helps it preparing the image for the purpose of the operations which are to be performed on it. Here the image is first converted into a gray scale image for future processing.

1.2.Object Detection:

To achieve object detection, perform two specific operations which are known as thresholding and morphological operations.These two methods can be described briefly such as,

1.2.1.Thresholding Method:

The Grayscale image is converted into binary image using LBPH algorithm i.e,linear binary pattern histogram,Here,the binary image is called as thresholding image.Thresholding makes it possible to highlight blocks or pixels in an image. Thresholding can be applied to gray scale images or color images. In this discussion gray scale images are used.During the process of thresholding,as we use a grayscale image we now convert this image into black and white.Here,the pixels with low intensity becomes zero and the pixels which are left over becomes 1.This results in a image which is binary image that consists ofblack and white pixels.

1.2.2.Morphological Operation:

A wide range of image processing techniques known as morphology process images based on forms. A structuring element is added by morphological processes to an input image to produce an output image of the same size. When performing a morphological operation, each output pixel's value is determined by comparing it to its neighbours in the input image. A wide range of image processing techniques known as morphology process images based on forms. A structuring element is added by morphological processes to an input image to produce an output image of the same size. When performing a morphological operation, each output pixel's value is determined by comparing it to its neighbours in the input image.It is used for removing the small object in segmented image. Finally, object was detected.

1.3.Feature Extraction:

In feature extraction, we used Scale Invariant Feature Transform (SIFT) features for forgery detection.

1.3.1.SIFT:

Scale Invariant Feature Transform algorithm helps in extracting features irrespective of scale, rotation, illumination, viewpoint.It consists of four steps,starting off with scale-space extrema detection,followed by key point localization,then the orientation assignment and finally key point descriptor.

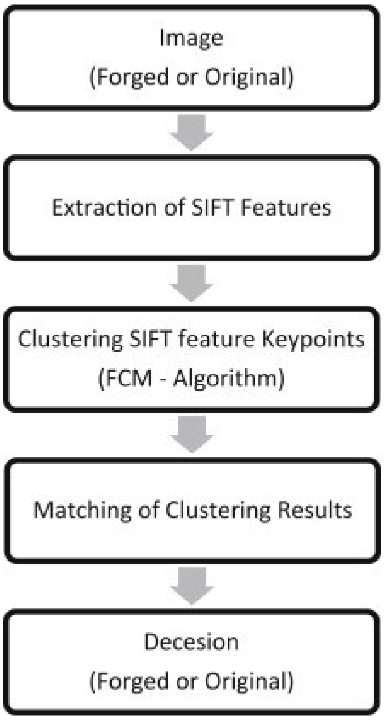


Image
(Forged or Original)
Extraction of SIFT Features
Clustering SIFT feature Keypoints
(FCM - Algorithm)
Matching of Clustering Results
Decesion
(Forged or Original)

Fig 1.1 Workflow of SIFT

1.Scale- Space Extrema Detection: In this step we apply a gaussian blur operator for smoothing the image. Smoothing is done to remove small details and noise. For an image I(x,y) the scale space of image is defined as :

$$L(x, y,\sigma)=G(x,y, \sigma)*I(x,y)$$

Gaussian function is defined as:

$$G(x,y,\sigma)=(1/2\pi\sigma^2)e^{(x^2+y^2/ \sigma^2)}$$

Where * is the convolution operator, G(x, y, σ) is a variable-scale Gaussian and I(x, y) is the input image.Here σ represents the factor of scale space. To detect potential points which are not variant to scale and orientation are also known as key points in Scale Invariant Feature Transform (SIFT), the method used in scale-space extrema in the difference-of-Gaussian(DoG) function convolved with the image, D(x,y, σ), which can be computed from the difference of two nearby scales separated by a multiplicative factor k.

Difference of Gaussians is one such technique, locating scale-space extrema, D(x, y, σ) by computing the difference between two images, one with scale k times the other. D(x, y, σ) is then given by:

$$D(x,y,\sigma)=[G(x,y,k\sigma)G(x,y,\sigma)]*I(x,y)=L(x,y,k\sigma)-L(x,y,\sigma)$$

The images are then grouped into an octave corresponding to doubling the value of σ. After the DoG images are obtained keypoints [15] are identified as local minima or maxima of the DoG image, this is achieved by comparing each pixel in DoG image to its corresponding eight neighbours at same scale and nine pixels of neighbouring scales, when compared if the value is maximum or minimum than the compared value we store it as an interested point.

2.Keypoint Localization:

Scale-space extrema detection generates an excessive number of key point candidates, some of which are unstable. In this stage, key points are filtered such that only stable key points are maintained. Once a key point candidate has been identified by comparing a pixel to its neighbours, a comprehensive fit to the neighbouring data is performed to determine the correct location, scale, and ratio of primary curvatures. This information permits points with low contrast (and hence vulnerable to noise) or that are poorly located along an edge to be eliminated.

3.Oriental Assignment:

We now assign orientation to the keypoints which we have obtained in the previous step. For assigning orientation we must make it rotation invariant, for doing so we create 36 bin histogram each with 10degree magnitude. Then the maximum orientation is assigned to the keypoint.. This This assignment contributes to the stability of matching and helps in getting accurate results. For each image sample L(x,y) at the keypoints scale σ, the gradient magnitude m(x,y) and orientation θ(x,y) is computed using pixel differences, let

$$m(x,y)=\sqrt{L1^2+L2^2}$$

$$\theta(x,y)=\arctan(L2/L1)$$

4.Keypoint Descriptor:

The preceding procedures assigned an image position, scale, and orientation to each keypoint, ensuring image rotation, location, and scale invariance. Then, for each keypoint, we want to compute descriptor vectors that are different and resistant to other perturbations, such as illuminations, etc. As a series of orientation histograms on 4 × 4 pixel neighbourhoods, compute the feature descriptor. The orientation histograms are relative to the keypoint orientation, and the orientation data is derived from the Gaussian picture with the same scale as the keypoint. Histograms have 8 bins apiece, and each descriptor has a 4x4 array of 16 histograms centred on the keypoint. As a result, a Scale Invariant Feature Transform (SIFT) feature vector of (4 x 4 x 8 =) 128 elements is produced.

2.1.Forgery Region Detection:

In this step, forgery image was loaded. Then, it was converted into grayscale image.

After, Scale Invariant Feature Transform (SIFT) feature extraction was performed in grayscale image.

Finally, based on the matched key points forgery regions and tampering percentage are identified

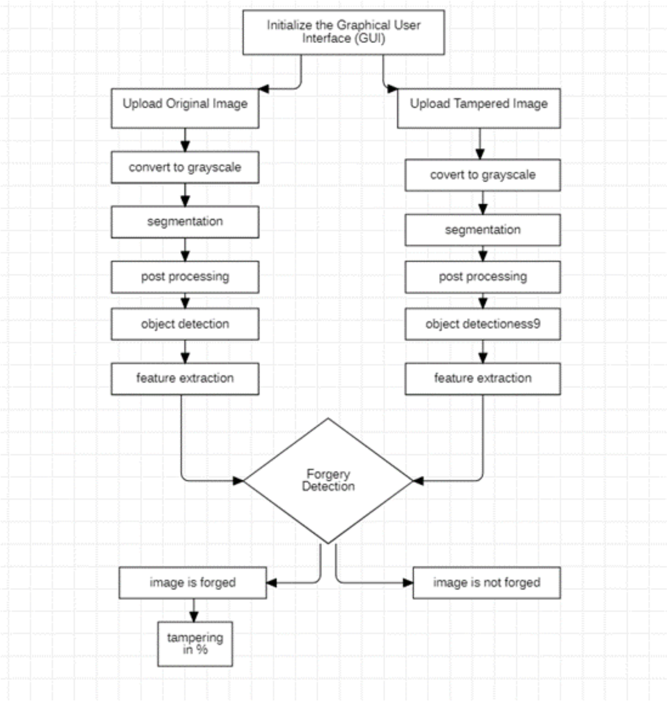
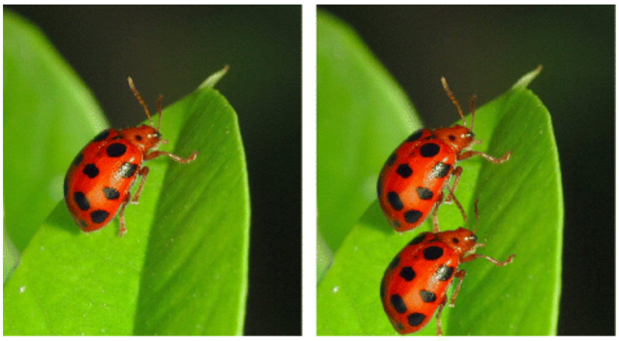


Fig 1.2 Flow Process of the Proposed System

IV. RESULT:

The proposed system can help in detecting the tampering performed for achieving this MATLAB software is used. Matrix Laboratory(MATLAB) provides wide range of toolboxes which helps in matrix manipulation, plotting of functions, creation of user interface etc.The results of our project are shown below.



(a) original image (b) forgery image

Fig 1.3 Original vs Forged image

Tampering perecentage:4.5856

No of original image	*No of forged image*	*TP*	*TN*	*FP*	*FN*
25	*25*	*24*	*22*	*1*	*3*

Table 1:Proposed System confusion matrix

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

Accuracy = 86%

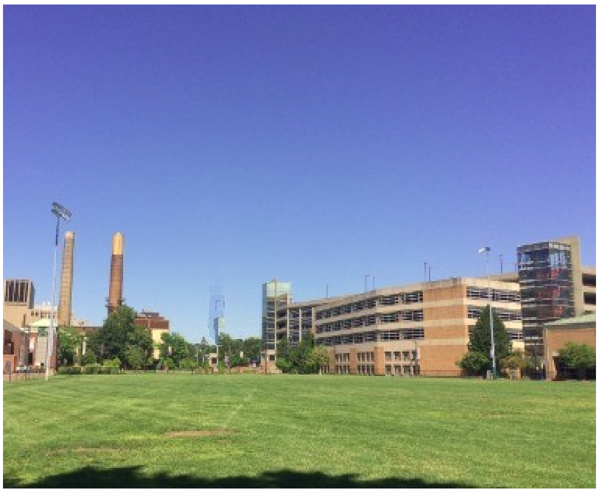


Fig 1.4 Forged image

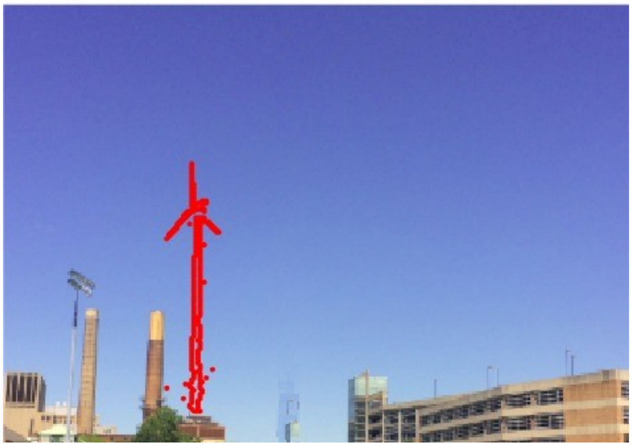


Fig 1.5 Tampering found in the image

V. CONCLUSION:

Here primarily the SIFT algorithm is used. This algorithm is used to divide the original image into number of different blocks. Using this we can be able to identify the proper initial size of the block which helps to upgrade the accuracy and also decreases the expenses. Therefore, Scale Invariant Feature Transform (SIFT) has a keyrole to play in the image forgery detection.

VI. FUTURE SCOPE:

The utilization of the proposed system can be elongated into many fields of applications in the future by adjusting it according the requisite. For example the proposed system can be updating by integrating required features and utilized in many other implementations like detecting counterfeit products, which can avail the users to find the product of the pristine brand. It can be utilized by the E-commerce platform users to verify if the product is pristine or fake by detecting whether the logo is forged or not. The scope can be elongated in the field of art for determining the distinction between the pristine and the forged artwork.

VI. REFERENCES:

[1] Aditya R Hambarde, Avinash G Keskar,”Copy-move Forgery Detection Using DWT and SIFT Features”, proceeding Department of Electronics Engineering Visvesvaraya National Institute of Technology, Nagpur, India 78699.

[2] Mr.Arun Anup M,”Image forgery And Its Detection: A survey (2015)”, Department of computer engg and science, MES college of Engineering.

[3] Salam A.Thajeel, Ghazali Sulong,”A Survey Of Copy-Move Forgery Detection Techniques”, Journal of Theoretical and Applied Information Technology, 10th December 2014.

[4] Vincent Christlein, ” An Evaluation Of Popular Copy-Move Forgery Detection Approaches”, Student member IEEE,vol.07.no 6 December 2012.

[5] Jessica Fridich, David Soukal,”Detection of Copy Move Forgery in Digital Image”, Department of computer Science, NY 13902-6000.

[6] Hwei-Jen Lin, Chun-Wei Wang, Yang-Ta Kao, ’’Fast Copy-Move Forgery Detection”, WSEAS Transactions On Signal Processing, Issue 5, Volume 5, May 2009.

[7] Matthew C. Stamm,, “Forensic Detection of Image Manipulation Using Statistical Intrinsic Fingerprints”, IEEE Transactions On Information Forensics And Security, Vol. 5, No. 3, September 2010.

[8] Rani Mariya Joseph, Chithra A.S.,“Literature Survey on Image Manipulation Detection” ,International Research Journal of Engineering and Technology (IRJET) ,Volume: 02 Issue: 04,July-2015.

[9] S. Bayram, H. T. Sencar and N. Memon, “An efficient and robust method for detecting copy-move forgery”, Proceedings of the IEEE International Conference on the Acoustics, Speech and Signal Processing, (2009) April 19-24.

[10] L. Li, S. Li and J. Wang, ”Copy-Move forgery detection based on PHT”, Proceedings of the World congress on the Information and Communication Technologies, (2012).

[11] O. Al-Qershi, B. Khoo,”Passive detection of copy-move forgery in digital images: state-of-the-art”,Forensic Sci Int, 231 (2013)

[12] W. Li, N. Yu, Rotation robust detection of copy-move forgery,in: Proc. of IEEE ICIP, Hong Kong, China, 2010

[13] V. Christlein, C. Riess, E. Angelopoulou, On rotation invariancein copy-move forgery detection, in: Proc. of IEEE WIFS, Seat-tle, WA, USA, 2010.

[14]I. Amerini, L. Ballan, R. Caldelli, A. Bimbo, G. Serra,“ A SIFT-based forensic method for copy-move attack detection and transformation recovery”,IEEE Trans Inf Forensics Secur, 6 (3) (2011)

[15] A. Dada, R.V. Dharaskarb, V.M. Thakarec,”A Survey on keypoint based copy-paste forgery detection techniques”,Sci Direct Comput Sci, 78 (2016)