An Efficient technique for Image Forgery Detection Using Local Binary Pattern (Hessian and Center Symmetric) and Transformation Method

Mohanad Fadhil Jwaid
Department of Information Technology
Maharashtra Institute of Technology
Pune, India
mohanada02jwaid@gmail.com

Trupti Baraskar
Department of Information Technology
Maharashtra Institute of Technology
Pune, India
trupti.baraskar@mitpune.edu.in

Abstract: In today's world image tampering or digital image forgery are very common with different tools and software available, which many time leads to digital crime and has an adverse effect on business and technology sector. A digital image provides a compact and authentic way to convey various secure information. To provide more authenticity to it, here a new passive image forgery detection technique is served and implemented. This proposed method is based on Hessian and Center Symmetric Local Binary Pattern, Principle Component Analysis and Discrete Wave Transform. This feature extraction method is applied on the forge input image which is applicable for identifying forge image using copy-move and splicing approach. The proposed method consists of following steps: firstly preprocessing, and second is feature extraction using Local interest point of each object based on Hessian method and extraction Center-Symmetric local binary pattern features. Thirdly Discrete Wavelet Transform has applied for simulations analysis of low-frequency sub-band and removing noise from the image. Fourthly Principle Component Analysis is applied to feature vectors to reduce its dimension while the efficiency well results. Last step using machine learning technique which requires training and testing phases, for a non-linear problem, as kernel function is used that projects the data to a higher dimensional space where it becomes linearly separable. Expected result of the proposed method will be standard metrics that evaluated the localization performance, the True Positive Rate and True Negative Rate are calculated.

Keywords: ***Image forgery, Local Binary pattern (LBP), Discrete Wavelet Transform (DWT), Principle Component Analysis (PCA), TPR, TNR***

I. Introduction

Image processing is a technique of converting an image into its digital format and performing manipulation on it for enhancing its quality or to extract some important information. Nowadays digital images are part of daily scenario because it squeezes a lot of information and is easily transferable. Most importantly no expertises are required for editing a digital image due to user interactive applications. Tampering of images and spreading negative propaganda is common nowadays which can be essential in criminal investigation scientific discovery etc. There are two methods; Active and Inactive to identify a digital forgery [2].

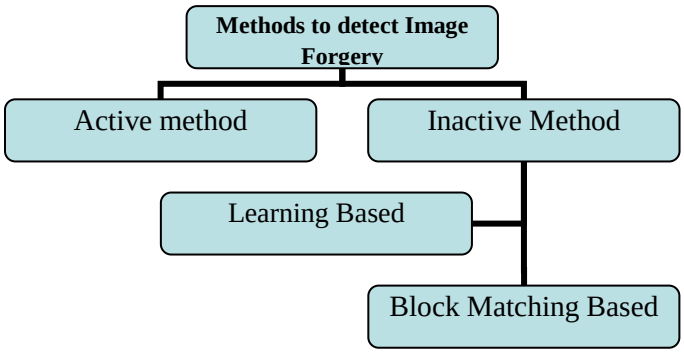

Fig.1. Methods of Image Forgery Detection

Active method has it shortcoming as it depends on the integrity of the signature which is not embedded in most of the cameras. Inactive method is divided in two categories learning based and block matching based methods; block matching based methods are those in which forgery is detected by the localization of the region of image which is useful for evidence in front of jury, due to its time consuming nature it

cannot be used for verifying the forged images uploaded everyday on social media [4].

In the proposed method, learning based passive technique is used to detect copy-move forgeries and picture splicing forgeries. This technique is inspired based on Local binary pattern and principle component analysis which will transformed with the help of DWT.The technique of creating duplicate picture has been tremendously easy with the introduction of new and powerful computer graphic editing software which are free of cost available as Photoshop, GIMP, and Corel Paint Shop. Today, this powerful picture processing software's allowed people to change pictures and pictures conveniently. Nowadays it creates a big challenge to authenticate the pictures. Sometimes it is difficult to identify the edited region from the original picture. The identification of a forged picture is driven by the need of authenticity and to keep up integrity of the unique picture.

II. Related Work

In today's Era, Image Orginality and authenticity has becomes a major threat in may real time applications like banking, legal documents, crime investigation etc.[1] Image Cloning Forgery is one of the most risk full method of image forgery, here the user can copy paste the original image and manipulate information in the authenticated part [2]. Additionally, as copying is done from the same image, its color palette, noise factors, flexible range and other image characteristics becomes similar with the regions of the original image which is difficult to identify the forgery [3].

Table .1. Active and Passive Approach

type	advantage	disadvantage	techniques	Author name
active	1.Computational cost less. 2.Simple knowledge about original image is require.	1. It require some human intervention. 2. Extract bandwidth is needed for transmission of signature.	1. Digital watermarking. 2. Digital signature.	Rani Suzan, IEEE[3]
passive	Preexisting digital images and data cannot gain any profit using Active approach, Passive approach overcomes this disadvantage.	It is based on the assumption that digital forgeries may leave no visual clues that indicate tampering, so they require different statistics of an image. Thus it is complex.	1. Pixel based techniques. 2. Format based techniques. 3. Camera based techniques.	Charmil Netin, IEEE[4]

III. Proposed work

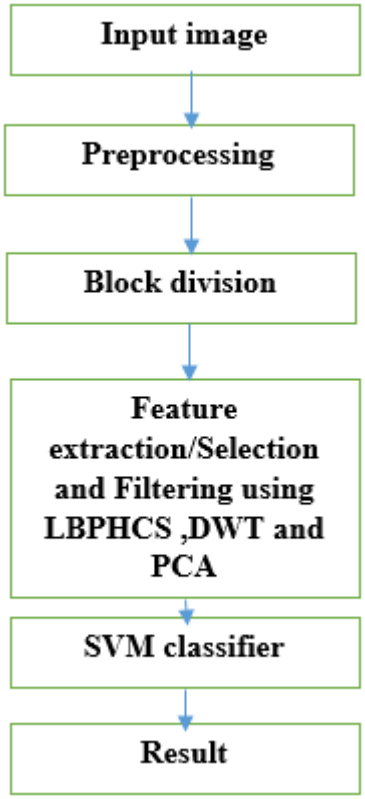

Figure .1. Proposed Model

Proposed system identifies the picture manipulation i.e. to detect the picture forgery and image splicing in given input picture. In our system firstly the algorithm changes the input RGB picture into YCbCr color channel; afterwards chrominance component is divided into non-overlapping blocks. Second Local Binary Pattern (LBP) is performed by using Hessian and Center Symmetric، and discrete wavelet transform is applied in all squares. Finally Principle Component Analysis (PCA) is utilized for all squares and the output is fed to Support vector Machine (SVM) classifier as features. So the final result is given that the forgeries is find or not.

In today's visual world, digital images have become an integral part of our everyday life due to their ability to convey a wide range of information in a compact way and the availability of digital image acquisition tools. It has become easy to use digital images for nefarious designs and negative propaganda on social and electronic media, and hiding the facts, which can be crucial for criminal investigation, medical imaging, scientific discoveries, etc. As such, the authenticity of digital images cannot be taken for granted. So our work can be solving this problem. A digital image is a very rich source of information and can capture any event perfectly, but because of this reason, its authenticity is questionable. So our work can overcome this problem successfully. This work can used to detect the copy move data in various important fields like social media, courts, insurance etc.

IV. Proposed Methodology

Pre-processing:

First step is pre-processing which convert an input image from R G B color to YCbCr, there are two types of YCbCr (Y-Component also called Luminance) and (Cb and Cr Components also called Chrominance). An image forgery detection based on second type because the human eyes are less sensitive to chrominance than luminance. The transform from RGB to YCbCr is given as:

Y=0.299R+0.587G+0.114B …… (1)

Cr=0.701R−0.587G−0.114B …….. (2)

Cb=−0.299R−0.587G+0.886B..... (3)

Block Division:

The input image is divided into square blocks or circle blocks. Features are extracted using LBPHCS, DWT and PCA. Block-based methods are suitable for detecting uniform regions. These regions generally represent image textures, such as sky, ocean, and grass, in minimal detail. The common assumption regarding these methods is that the forged duplicate regions have not been subject to geometric transformation, such as scaling and rotation, or post processing operations, such as illumination changes and blurring.

Feature Extraction:

A local pattern, which in LBP operators is identified in a pixel neighborhood and expressed using the relations between the pixel p, and its N neighborhood pixels located on a circle of radius R, which constitutes a circularly symmetric-neighbor group. The definition of LBP operator represents local patterns with binary-code, which are computed by thresholding the grayscale values of the neighborhood pixels relative to the grayscale value of the middle pixel where zeros are represented by black

circles and ones by white circles.

The purpose of local interest points is to make an efficient match between uniform duplicate regions .The local interest points of forgery objects are identified based on the Hessian matrix that exhibits strong derivatives in two orthogonal directions. Given point $x= (x, y)$ in the interest region in image I, Hessian matrix $H(x,\sigma)$ in x at scale σ is described as follows:

$$H(X, \sigma) = \begin{bmatrix} Ixx(X,\sigma) & Ixy(X,\sigma) \\ Ix,y(X,\sigma) & Iy,y(X,\sigma) \end{bmatrix} \quad \ldots\ldots (4)$$

Where Ixx, Ixy, and Iyy are the second derivatives for each point x in the image [3].Center-Symmetric is provides details of analyzing the patterns of interest regions of segments for copy-move forgery detection. The descriptors for each segment is calculated, which combines the strength of Hessian features and of CSLBP texture analysis .The CSLBP can be defined as a modified version of the local binary pattern (LBP). The main formula of CSLBP is:

$$CSLBP(Xc.Yc) = \sum_{n=0}^{n=3} S(\mathrm{Gn} - \mathrm{Gn}_{+4})2^n \quad .(5)$$

Where Gn represents eight neighboring pixels [3].

After that applying the transformation techniques that are used for detect forgery in images. First technique is Discrete Wavelet Transform, it is allow the simultaneous analysis of both frequency and time. DWT is used to removing noise from images, the other use of DWT is reduce the size of an image at each level. Wavelet coefficients are extracted from the sub bands after discrete wavelet transform. First applying multi-resolution wavelet decomposition to small fixed-sized image blocks. This transform decomposes an image with an overall scale factor of 4 providing, at each level, one low-resolution sub-image (LL) and three wavelet Coefficients sub-images (HL,LH,HH). For image forgery detection 2 level wavelet decomposition is used for calculating wavelet coefficients for each block. These wavelet coefficients are then stacked into a vector for each block .This feature vectors are used for further processing.

Then apply Principle Component Analysis (PCA) technique, where the PCA is a great useful filter in image processing. It is the most common and popular linear dimension reduction approach. It has been used for years because of it is conceptual simplicity and computation efficiency. PCA is employed for feature extraction and also decrement of data dimension while the efficiency is well preserved.

SVM Classifier:

Last step is classification where Support Vector Machines (SVM) is employed for tampered image detection that is a two-class problem. SVM which is a machine learning technique involves training and testing stage, so the features are fed in SVM for classification, it uses kernel functions to map the samples to a higher dimension space where the classes become linearly separable. SVM should be detect whether an image is fake or original. Next figure will show these steps. For the validation of our approach, it is important that we thoroughly compare our method with existing method; we implemented this method using both grayscale and Cr channel. Our implementation achieved similar results compared with that of the original paper when grayscale images were used (89.93%). When we tested this method using Cr channel, we found that the detection performance is better than that of the grayscale (91.38%). A comparison between the results of our method and existing method using Cr channel is depicted. It can be observed that our method achieved a higher detection performance. To check whether this achievement is statistically significant, the t-test with 95% condense level was applied and significant difference was found. It presents a comparison between the proposed method and stat-of-the-art forgery detection methods, which use SVM and the same datasets. It can be observed that the proposed method outperforms the existing techniques. The proposed system involves two parameters in pre-processing, feature extraction and classification steps. These parameters are:

True Positive Rate (TPR)

True Positive Rate (TPR), also known as Sensitivity or Recall, measures the percentage of actual tampered images (positives) that are correctly classified as such. It is calculated as:

TPR = TP / (TP + FN) ……. (6)

True Negative Rate (TNR)

True Negative Rate (TNR), also known as Specificity, measures the percentage of actual authentic images (negatives) that are correctly classified as such. It is computed using the following formula

TNR = TN / (TN + FP) ……. (7)

Where:

TP (True Positive) is the number of tampered images, which are classified as tampered; FN (False Negative) is the number of tampered images, which are classified as authentic;

TN (True Negative) is the number of authentic images, which are classified as authentic.

This section investigates the effect of using four commonly used color systems: RGB, Grayscale and YCbCr

V. Implementation and Expected Result

The developed application has done registration for login and user can access stored image data base. First step: According to develop application, access authentication has implemented and testing is also done. Accordingly have to do authentication that has implemented and tested. Now user give the input parameters like (name, password, email and phone number)

Second step: After authentication of the user, original image is classified into RGB images.

Third step: Now classify image is converted into YCbCr image.

Below table number (2) shows the types of image format and size of each image taken for testing purpose.

Table 2: image format and size

Image type	Size
jpg	384*256 256*384
jpeg	384*256 256*384
tif	757*568 1152*768
bmp	757*568 1152*768

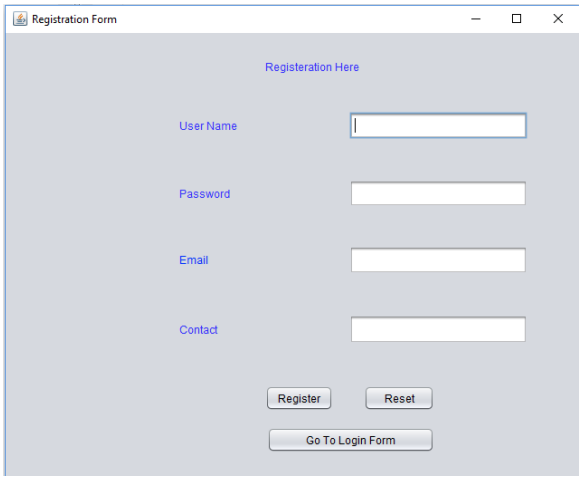

Fig .3. Registration form for login

Fig .4. RGB image classification

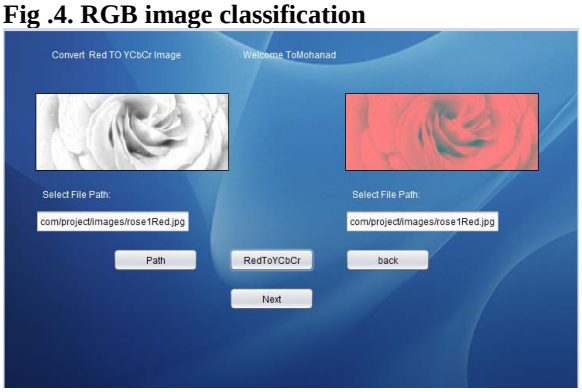

Fig .5. Conversion of RGB to YCbCr

VI. Conclusion

Now the proposed work is conclude that input image authentication and pre-processing has been done.

This application will be applicable for detecting image forgery. It would be efficient technique for forgery detection using LBPHCS, DWT, PCA and SVM classifier.

References

[1] Fahime Hakimi, Mahdi Hariri, Farhad GharehBaghi, “Image Splicing Forgery Detection using Local Binary Pattern and Discrete Wavelet Transform”, 2nd international conference on Knowledge-Based Engineering and Innovation (KBEI), Tehran , Iran IEEE 2015 .

[2] Amani Alahmadi, Muhammad Hussain, Hatim Aboalsamh, Ghulam Muhammad, George Bebis, Hassan Mathkour, “Passive Detection of Image Forgery using DCT and Local Binary Pattern”, Signal Image and Video Processing · 2013 IEEE Global Conference on Signal and Information Processing.

[3] Rani Susan Oommen, Jayamohan M., Sruthy S., “A Survey of Copy-Move Forgery Detection Techniques for Digital Images”, International Journal of Innovations in Engineering and technology. April 2015,

[4] Charmil Nitin Bharti, Purvi Tandel, “A Survey of Image Forgery Detection Techniques”, 2016 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET), IEEE, 2016

[5] Diaa M. Uliyan, Hamid A. Jalab, Ainuddin W. Abdul Wahab, “Copy Move Image Forgery Detection Using Hessian and Center Symmetric Local Binary Pattern”, 2015 IEEE Conference on Open Systems (ICOS), August 24-26, 2015, Melaka, Malaysia

[6] Texture Operator Based Image Splicing Detection Hybrid Technique Saurabh Agarwal; Satish Chand 2016 Second International Conference on Computational Intelligence & Communication Technology (CICT)

[7] Region duplication forgery detection in digital images using 2D-DWT and SVD Varsha Karbhari Sanap; Vanita Manikrao Mane 2015 International Conference on Applied and Theoretical Computing and Communication Technology (iCATccT).