IOSR Journal of Electronics and Communication Engineering (IOSR-JECE)
e-ISSN: 2278-2834,p- ISSN: 2278-8735.Volume 14, Issue 1, Ser. II (Jan.-Feb. 2019), PP 38-43
www.iosrjournals.org

Image Forgery Detection Based on SURF and Machine Learning Classifier

P.R. Rothe [1], P. P. Asthankar[2], J. P. Rothe[3]
[1](*Dept. of Electronics Engg, Priyadarshini College of Engineering, Nagpur, India*)
[2]*(Dept. of E &Tc, Priyadarshini College of Engineering, Nagpur, India)*
[3]*(Dept. of Electrical Engg. , St. Vincent Palloti College of Engineering, Nagpur, India)*
Corresponding Author: P.R. Rothe

Abstract: *Today manipulation of digital images has become easy due to availability powerful image editing tools like Adobe Photoshop etc. Detection of a forged image is driven by the need of authenticity and to maintain integrity of the image. The most common type of digital image forgery is known as copy-move forgery wherein a part of image is cut/copied and pasted in another area of the same image. This paper proposed a new image tampering detection method based on Speed-up robust features and Support vector machine (SVM) to detect copy-move forgery in image.*

Date of Submission: 25-02-2019 Date of acceptance:11-03-2019

I. Introduction

In Today's time we cannot imagine the exact usage of digital images every day for various purposes. After the survey, Flickr has some 350 million photographs with more than 1 million added daily (record 2007) and Facebook has more than 50 million cumulative upload of images (record 2010) [1].Currently digital images are the most common and convenient way for expressing and transmitting information. Information expressed in thousands of words can be easily and compactly expressed in a simple image. Pictorial information around us represents nearly 75% of all the information received by human being visual system. With the increasing use of digital images and rapid advent in imaging technology, tampering techniques accordingly became more sophisticated. With the help of powerful image editing software, we can easily modify digital images without leaving any perceptible artifacts. Maliciously tampered images would lead to some potentially serious consequences in our daily life which decreases the credibility of digital images, and their content integrity can no longer be fully trusted.

Different techniques for maintaining the integrity of digital images have been developed. In this project we have used the non intrusive technique to find the tampering. In this project we have used the non intrusive technique that exploit different kinds of intrinsic qualities such as sensor noise of the capturing device or image specific detectable changes for detecting forgery to find the tampering.

II. Digital Image Forgery Types

Alteration of the semantic contents of a digital image may be achieved by removing information from that image, or adding extra information to it for which forgers may use many techniques. Different criteria can be used to classify those techniques, but the most important and widely used techniques are image retouching, image splicing, and image cloning.

Digital images retouching is considered to be the less harmful kind of digital image forgery, since it does not make significant changes to the visual message of an image. Instead it can be used to enhance or reduce digital images features consequently; it is widely used by magazine photo editors.

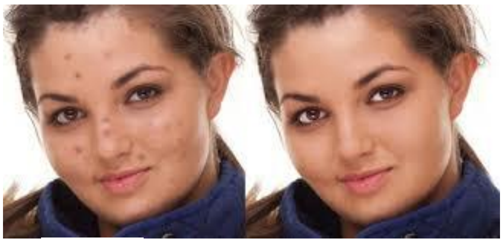


Figure 1 Image retouching technique

In image splicing, fragments from two or more images are combined to create a new image i.e. the part of an image is copied from one image and that part is pasted into another image. This operation is fundamental in digital photo mortaring and in turn is a mechanism for image forgery creation. Consider Figure 2 the LHS image and the RHS image in first row are original whereas the image in second row is spliced that is the bird from the RHS image is copied, flipped and pasted into the LHS image, giving rise to the illusion that the lion is hunting the bird.

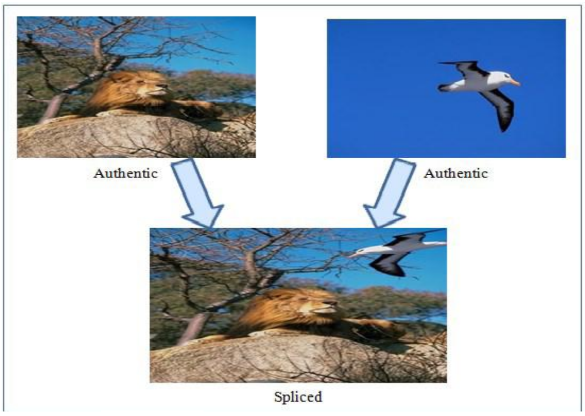


Figure 2 Image splicing technique

In cloning forgery of digital images the tampering occurs within a single image and no need for multiple images. A part of the image is copied and then pasted in a desired location within the same image. It can be considered as a special case of image splicing. In the Fig 3, copy-move forgery is done in case of the tower design. If we see only RHS image in Fig3 image then the forgery cannot be identified with human eyes since the copied part belongs to the same image therefore mostly important properties are congruous with the rest of the image.

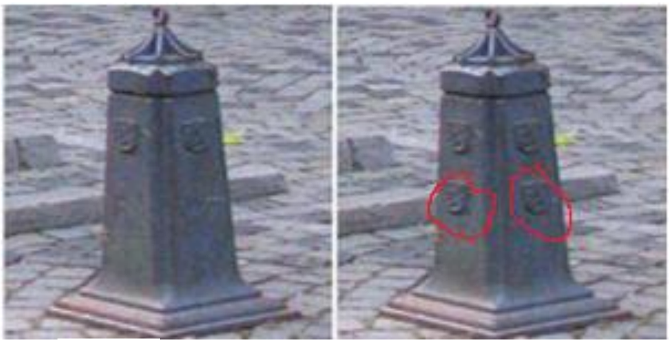


Figure 3 Image Copy-Move (Cloning) Technique

III. Literature Review

Haodong Lee and Weiqi Lou proposed a framework to improve the performance of forgery localization via integrating tampering possibility maps [2]. They first select and improve statistical feature-based detector and copy-move forgery detector forensic approach and then adjust their results to obtain tampering possibility maps. After investigating the properties of possibility maps and comparing various fusion schemes, they propose a strategy to integrate the tampering possibility maps to obtain the final localization results. To design a fusion strategy to integrate the tampering possibility maps, analysis of distributions of values in tampering possibility maps for pristine and fake pixels was done and then an effective decision curve was worked out.

Musaed Alhussein proposed a tampering detection method for splicing and copy-move forgery using local texture descriptor and extreme learning machine (ELM). First, the image is break down into RGB colour components and each component is divided into non-overlapping blocks [3]. Then local binary pattern (LBP) LBP histogram is obtained from each block and the histograms from all the blocks are concatenated to form the feature vector of the image. The features are then fed to an Extreme Learning Machine (ELM) classifier for the decision. The experimentation was performed using CASIA v1.0 and CASIA v2.0 databases. The proposed method achieved 95.67% accuracy in CASIA v1.0 database, and 97.3% in CASIA v2.0 database.

A technique for detecting forgery of composite images using machine learning classifiers was proposed by Tamana Sharma & Mandeep Kaur.Illuminant color is estimated for input images and map for each image is created. All faces present in one image and corresponding all faces of other individual images are extracted for investigation.The textural and gradient features are extracted in the form of HOG (Histogram of Oriented Gradients), SASI(Statistical analysis of structural information)features. HOG describes the shape and appearance of local object within an image. The image is divided into small regions called cells for the purpose of feature extraction and HOG directions for the pixels within the cell are computed. SASI is a generic descriptor that is used to measure the structural properties of textures. SASI extracts the texture information from illuminant map and captures the small granularities and discontinuities in texture pattern. The two features which are computed are given as input to the SVM and LSSVM classifier. The accuracy is found to be 75% with SVM and 100% with LSSVM.

Bo Xu, Guangjie Liu, and Yuewei Dai et al. [4] come up with a technique to detect the splicing forgery introduced abnormality using SRM. The experimental results illustrate that the proposed technique can detect splicing forgeries with much higher accuracy than in luminance channel.

IV. The Proposed Approach

The block diagram of the proposed method is shown in Figure 3. The image is divided into overlapping blocks and the feature of each block is extracted. The features of each block are matched using the Support Vector Machine (SVM). The output obtained is the probability of the matched blocks. Then a threshold value is selected, and all the probabilities greater than the threshold are considered to be tampered.

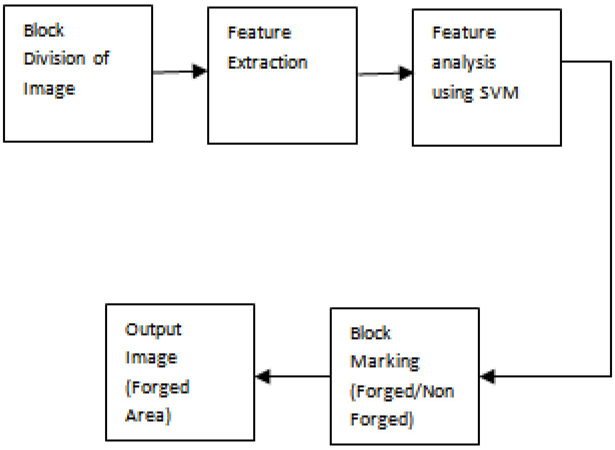

Block Division of Image
Feature Extraction
Feature analysis using SVM
Output Image (Forged Area)
Block Marking (Forged/Non Forged)

Figure 3 Block Diagram of Proposed Method

The image is divided into overlapping blocks and the feature of each block is extracted. The features of each block are matched using the Support Vector Machine (SVM). The output obtained is the probability of the matched blocks. Then a threshold value is selected, and all the probabilities greater than the threshold are considered to be tampered.

An image is partitioned into overlapping blocks by sliding a predefined window by one pixel throughout the whole image. To assure detection of area of all sizes the size of the window used is 8×8. The total number of blocks generated by dividing NxM image into blocks of size bxb is given by the following equation

$$N_b = (N - b +1) \text{ x } (M - b +1)$$

Every individual block will be compared with every other block formed within the image, using a threshold value between 0 to 1.

Two types of features are extracted namely Morphological features and SURF (Speed-Up Robust Features) features. Morphological feature extraction is block based and SURF extraction is key-point based therefore we are combining the best of two methods. Morphological image processing is a collection of non-linear operations related to the shape or morphology of features in an image. The morphological features used are mean value and standard deviation.

The SURF detector focuses its attention on blob like structures in the image. Object Recognition using SURF consist of three steps - feature extraction, feature description, and feature matching. The function used for feature extraction accepts the input image and return an array of extracted interest points. These interest points are depicted over the input image as shown in a Figure 5. SURF encompasses a feature detector based on a Gaussian second derivative mask, and a feature descriptor that bank on local Haar wavelet responses.

The SURF detector algorithm consists of the following steps:

1. Form the scale-space response by convolving the source image using DoH filters with different σ.
2. Search for local maxima across neighboring pixels and adjacent scales within different octaves.
3. Interpolate the location of each local maxima found.
4. For each point of interest, return x, y, σ, the DoH magnitude, and the Laplacian's sign.

For feature description, SURF summarizes the pixel information in a local neighborhood. It determines an orientation for each feature, by convolving pixels in its neighborhood with the horizontal and the vertical Haar wavelet filters. These filters can consider as block based methods to compute directional derivatives of the image's intensity. By using intensity changes to characterize orientation, this descriptor is able to describe features in the same manner regardless of the specific orientation of objects or of the camera.

The features obtained with the feature extraction methods are matched in this step. That is each block is compared with other blocks and blocks having similar features are considered to be tampered. In this project we have used Support Vector Machine algorithm for feature matching.

It is a state-of-the-art classification method introduced in 1992 by Boser, Guyon, and Vapnik [5] & belong to the general category of kernel methods [6, 7]. In this case the dot product can be replaced by a kernel function that computes a dot product in high dimensional feature space. The goal of SVM is to separate the data with hyper plane and extend this to non-linear boundaries using kernel trick [8] [9].

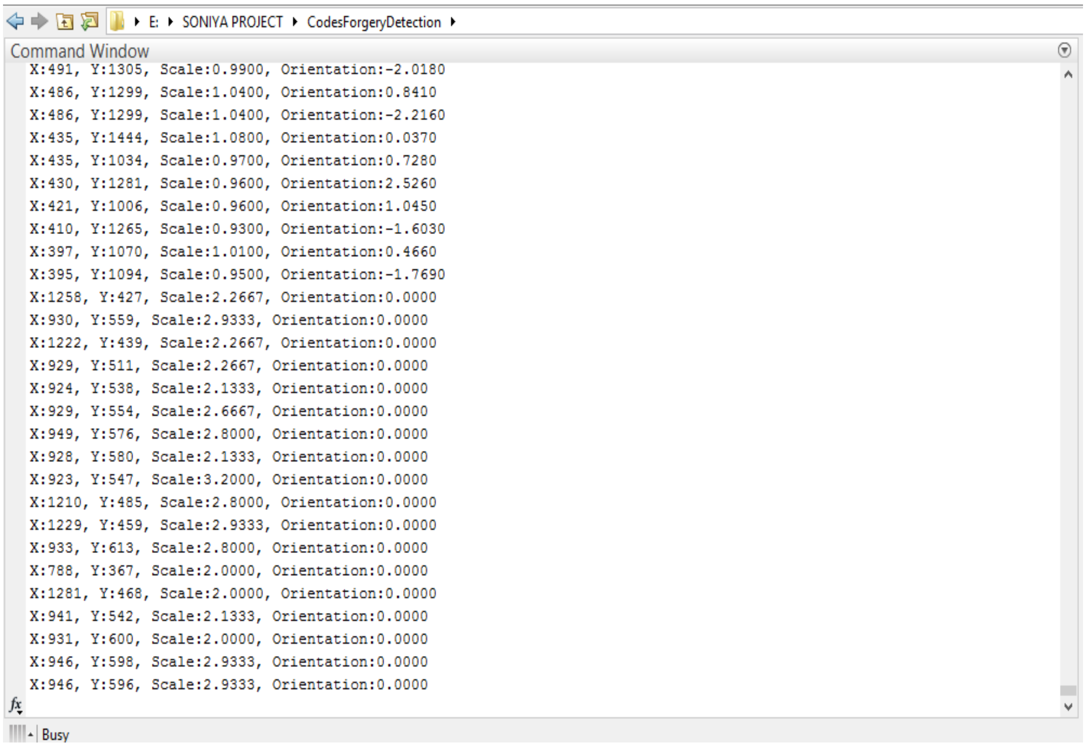
Next a threshold value is selected which ranges between 0 to 1. The blocks having probability less than the threshold will be ignored and the blocks having probability above the threshold will be termed as tampered image.

For the image DWT is applied to get four components (a,h,v,d).The SURF features of the key points in these four parts are obtained. The SURF features obtained are (x,y positions, radius r for the size and orientation ϴ). With these surf features the SVM is trained to tag Forged and Nonforged parts of image.

V. Results

The sample of extracted Speed Up Robust Features (x,y,r,& theta) of the key locations are shown in Figure 4. The key points are indicated by small drop or spots on the image in Figure 5. In Figure 6 the Original image shown has the field and small part of the field as the forged part while Nonforged part is the sky. The tamper map shows the forged portion as white part. In the detected image the fake parts of the image are shown, the pristine part is shown by Black background.

In Figure 6 the input image is shown as 'Original image', the part of the image in which tampering is done is shown in the Tamper map by white portion and the forged part of the image is shown as Detected image. The Black portion in the Detected image shows the pristine image. Figure 7 shows the final result of the given image with time required for detection.



```
X:491, Y:1305, Scale:0.9900, Orientation:-2.0180
X:486, Y:1299, Scale:1.0400, Orientation:0.8410
X:486, Y:1299, Scale:1.0400, Orientation:-2.2160
X:435, Y:1444, Scale:1.0800, Orientation:0.0370
X:435, Y:1034, Scale:0.9700, Orientation:0.7280
X:430, Y:1281, Scale:0.9600, Orientation:2.5260
X:421, Y:1006, Scale:0.9600, Orientation:1.0450
X:410, Y:1265, Scale:0.9300, Orientation:-1.6030
X:397, Y:1070, Scale:1.0100, Orientation:0.4660
X:395, Y:1094, Scale:0.9500, Orientation:-1.7690
X:1258, Y:427, Scale:2.2667, Orientation:0.0000
X:930, Y:559, Scale:2.9333, Orientation:0.0000
X:1222, Y:439, Scale:2.2667, Orientation:0.0000
X:929, Y:511, Scale:2.2667, Orientation:0.0000
X:924, Y:538, Scale:2.1333, Orientation:0.0000
X:929, Y:554, Scale:2.6667, Orientation:0.0000
X:949, Y:576, Scale:2.8000, Orientation:0.0000
X:928, Y:580, Scale:2.1333, Orientation:0.0000
X:923, Y:547, Scale:3.2000, Orientation:0.0000
X:1210, Y:485, Scale:2.8000, Orientation:0.0000
X:1229, Y:459, Scale:2.9333, Orientation:0.0000
X:933, Y:613, Scale:2.8000, Orientation:0.0000
X:788, Y:367, Scale:2.0000, Orientation:0.0000
X:1281, Y:468, Scale:2.0000, Orientation:0.0000
X:941, Y:542, Scale:2.1333, Orientation:0.0000
X:931, Y:600, Scale:2.0000, Orientation:0.0000
X:946, Y:598, Scale:2.9333, Orientation:0.0000
X:946, Y:596, Scale:2.9333, Orientation:0.0000
```

Figure 4 SURF Features

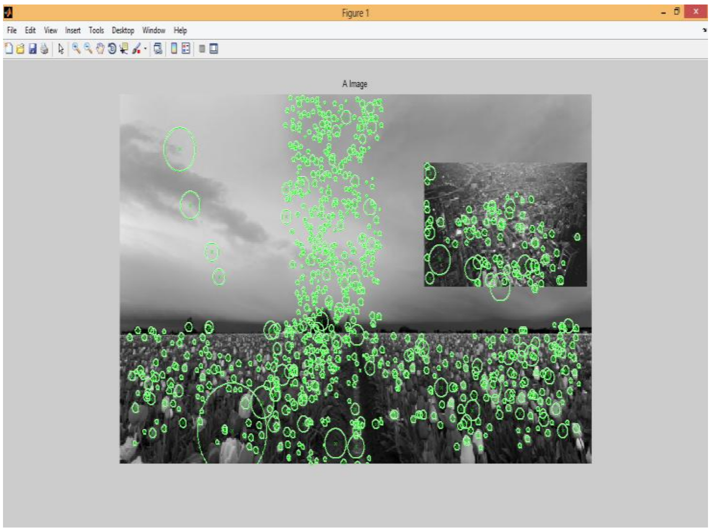


Figure 5 Approximate Component of the Image, showing Image in Enhanced but Compressed form

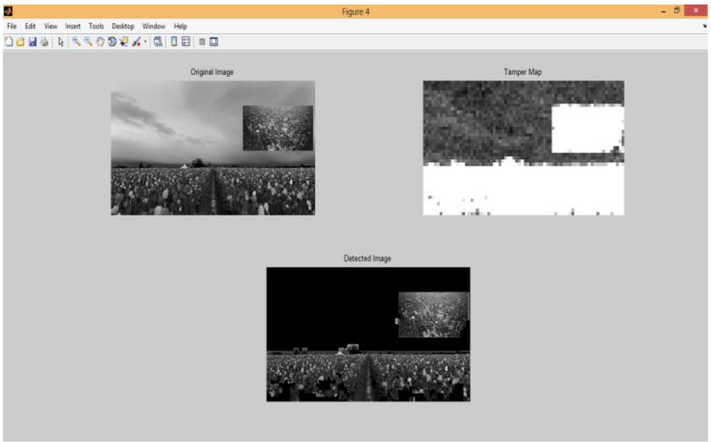
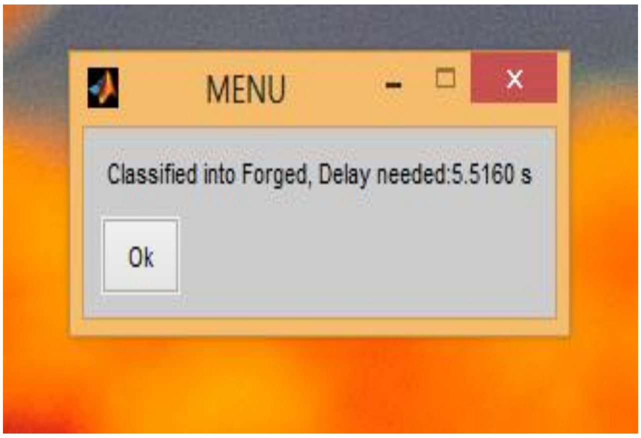


Figure 6 Final Output showing Image under observation, Tamper Map and Detected Image



Classified into Forged, Delay needed:5.5160 s

Figure 7 Final Conclusion (Forged/Non Forged) along with Delay in seconds.

VI. Conclusion

Tampering detection is a hard problem to solve as it involves different methodologies and abilities. We have proposed a framework for image forgery detection. The extensive results have shown the effectiveness of the proposed frame-work. This way, it is impossible that just one image tampering detection approach reveals perfectly an image manipulation. The performance of the used approach has been significantly improved by carefully selecting features, designing the training samples and adjusting the SVM parameters.

References

[1]. Christian Riess and Tiago Jose de arvalho,"Exposing Digital Image Forgeries by Illumination Color Classification", IEEE Transactions On Information Forensics And Security, vol. 8,2013.

[2]. Haodong Li, Weiqi Luo, Xiaoqing Qiu,and Jiwu Huang, "Image Forgery Localization via Integrating Tampering Possibility Maps", IEEE Transactions on Information Forensics and Security, Vol. 12, pp. 1240-1251, May 2017.

[3]. Musaed Alhussein, "Image Tampering Detection Based on Local Texture Descriptor and Extreme Learning Machine", UK Sim-AMSS 18th International Conference on Computer Modelling and Simulation, IEEE, pp. 196-199, April2016.

[4]. Tamana Sharma, Mandeep Kaur, "Forgery Detection of Spliced Images Using Machine Learning Classifiers and Colour Illumination",International Journal of Innovative Research in Science, Engineering and Technology, Vol.5, Issue 6, 2016.

[5]. Boser, B.E., Guyon, I.M., and Vapnik,V.N., "A training algorithm for optimal margin classifiers", 5th Annual ACM Workshop on COLT, pp.144–152, Pittsburgh, PA. 1992.

[6]. Shawe-Taylor, J. and Cristianini, N., "Kernel Methods for Pattern Analysis", Cambridge University Press, Cambridge, MA. 2004.

[7]. Scholkopf, B. and Smola, A., "Learning with Kernels", MIT Press, Cambridge, MA. 2002.

[8]. Nello Cristianini and John Shawe- Taylor, "An introduction to Support Vector Machines and other Kernel-based Learning Methods", Cambridge University Press, 2000.

[9]. Tom Mitchell, Machine Learning, McGraw-Hill, Computer science series, 1997.

[10]. Bo Xu, Guangjie Liu, and Yuewei Dai , "Detecting Image Splicing Using Merged Features in Chroma Space‖, the Scientific World Journal",2014.

[11]. Xunyu Pan and Siwei Lyu, "*Detecting image region duplication using sift features*", In Acoustics Speech and Signal Processing ICASSP-2010, pages 1706– 1709, IEEE, 2010.

[12]. Yanjun Cao, Tiegang Gao, Li Fan, and Qunting Yan "*A robust detection algorithm for copy-move forgery in digital images*", Forensic science international, 214(1):33–43, 2012.

[13]. Li Kang, Xiao-pin Cheng, K Li, and C Xiao-ping," *Copy-move forgery detection in digital image*", In Proc of the 3rd International Congress on Image and Signal Processing.[S. l.]: IEEE Computer Society, pages 2419–2421, 2010.

[14]. Mohammad Farukh Hashmi, Vijay Anand, and Avinas G Keskar," *Copy-move image forgery detection using an efficient and robust method combining un-decimated wavelet transform and scale invariant feature transform*", AASRI Procedia, 9:84–91, 2014.

IOSR Journal of Electronics and Communication Engineering (IOSR-JECE) is UGC approved Journal with Sl. No. 5016, Journal no. 49082.

P.R. Rothe. " Image Forgery Detection Based on SURF and Machine Learning Classifier." IOSR Journal of Electronics and Communication Engineering (IOSR-JECE) 14.1 (2019): 38-43.