ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

*(An ISO 3297: 2007 Certified Organization)*

**Vol. 5, Issue 6, June 2016**

# Forgery Detection of Spliced Images Using Machine Learning Classifiers and color Illumination

Tamana Sharma[1], Er.Mandeep Kaur[2]

M.Tech Student, Dept. of CSE, Sri Guru Granth Sahib World University, Punjab, India[1]

Assistant Professor, Dept. of CSE, Sri Guru Granth Sahib World University, Punjab, India[2]

**ABSTRACT**: Nowadays, the use of Digital images is everywhere, on the magazines, in newspapers, in hospitals, in shopping malls and all over the Internet. As the development in technology is increasing day by day, at the same time the trust in images is decreasing day by day. Most common type of Image forgery is Image composition which is also termed by the name Image Splicing. Combination of two or more images to generate a completely fake image is known as Image composition. It becomes very hard to differentiate between real image and fake image because of the presence of various powerful editing softwares. As a result in most of the cases, there is a need to prove whether the image is real or not. This paper describes a technique for detecting forgery of composite images using machine learning classifiers Support Vector Machine and Least Square Support Vector Machine and Perceptron with the help of color illumination.

**KEYWORDS**: Image Splicing, Machine learning, Image Forgery, Image composition, color illumination**.**

## I. INTRODUCTION

Image Forgery or modification of digital images is not a new concept. It is as old as Photography. But due to the fast development of technology, In Today's time we cannot imagine the exact usage of digital images every day for various purposes [1].It is said that, ―an image tells a thousand words‖. Images are used to explain tough concepts, and inspire us easily in each and every field. With the easily availability of internet, digital cameras and editing software's it is very easy to create a fake image without any training or extra knowledge. The trend of modification in digital images is increasing day by day. In various cases, where the images are used as evidences, the authenticity of images is important to prove in that cases then only the images can be used as a proof. Digital image forgery or we can say that tampering of digital images have become one of the major problems in crimes

There are many ways through which the image can be modified. Combining all those ways the three ways are image retouching forgery, Spliced image forgery, copy move forgery [2]. Image splicing is one of the way of modifying an image that copies a part of an original image and paste it onto another image to create a fake image, and it is mainly followed by post processing techniques such as local/global blurring, compression, and resizing [3].It is also known as image composition. Composite image is an image made by the combination of two or more than two images and is merged to form a single image. An example of image splicing is shownin fig.1. There are mainly five types of image forensic tools techniques. Pixel Based Techniques consists of that tools which helps in detecting anomalies mainly statistical that are to be introduced at the pixel level. Format based Techniques include those tools which helps in grasping the statistical correlations introduced by a specified lossy compression technique. Camera Based techniques include that tools which helps in the proper usage artifacts that are introduced by the camera lens, sensor, or on-chip post-processing. Physically techniques includes that tools which clearly detect issues in the three dimensional interaction

ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

*(An ISO 3297: 2007 Certified Organization)*

**Vol. 5, Issue 6, June 2016**

between physical objects, light, and the camera. Geometric Based techniques include that tools which make exact calculation of objects in the world and their positions relative to the camera [4]. There are basically two approaches of digital imageforgery detection. Active approach consists of Datahiding approach and Digital signature approach. In Data hiding approach, it adds secondary data into an image. Digital watermarking is a common example of this. In this, digital watermark is inserted at source side and verify that at detection side. The limitation of this method is that there is the insertion of watermark at the time of recording, which requires the existence of well-equipped digital camera. In digital signature approach, unique feature of image is extracted and corresponding signature created at the source side. This signature is then used for verification at the detection side .Passiveapproach work on the assumption that although digital forgeries may leave no visual clues that indicate tampering, they may alter the underlying statistics of an image. Any prior information about image is notrequired by this approach. The prior information here means like it does not require any digital signature to be generated or watermark to be inserted in advance. This is the main advantage of passive methods [2].

**Fig 1: Example of image Splicing**

Spliced image forgery detection can be done through many ways. Among all those ways, illumination inconsistencies are useful for splicing detection. Two methods of Illumination based forgery Detection are Geometry based methods and color based methods. Geometry based methods helps in detecting irregularities in area of light source between Particular objects and devices. Color based methods helps in detecting irregularities in the interaction between object color and light color [2]. In this paper we used color IL luminance for forgery detection.
In every method manual interaction is must. Nowadays it is difficult to trust images. A human eye cannot differentiate between the real image and fake image. So we develop semi-automatic forgery method for the detection of spliced images that makes use of machine learning classifiers where the decision is taken by classifier. Illuminant color based forgery detection method is developed here. Training and testing strategy is used. Various original and edited images are collected and their texture and gradient features extracted. Then train the system with these features. In final phase, classification is done using a Support Vector Machine (SVM) classifier; Least Square Support Vector machine (LLSVM) and Perceptron classifiers are used.

## II. RELATED WORK

Digital forgery is now an ordeal to individuals because of increasing modifications in real images to form fake images of celebrities, societies that include fake images targeting religion or race, journalism, scientific publication etc. [5]. 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]. To maintain such a large amount of digital data has become critical, complex and challenging. In the past years many forgery detection methods and

ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 6, June 2016

techniques are proposed. The most effective tool for providing image realism and source details is digital watermarking. Image Forgery detection is also solved by these digital watermarks. Various watermarking techniques have been proposed. One method is to use a checksum on the image data that is embedded in the least significant bits of certain pixels [6]. Other methods identify the watermark by computing the spatial cross-correlation function of the sequence and the watermarked image and add a maximum length linear shift register sequence to the pixel data [5]. Invisible watermarks are also designed, which can be blend in with camera or noise. Visible Watermarks also do exist. Weiqi Luo[5] proposed an algorithm that extracts image features with the help of seven characteristics features using statistical analysis of pixels in an image block. It gives less computing complexity and is more robust against many post region duplication image processing graphics operations. Johnson et al. [7] proposed a method that show how composites can be detected with the help of estimating intrinsic parameters of a camera from the image of a person's eyes .In non-tampered images, the principal point lies near the image center. When a person is converted in the image as part of creating a composite image, the principal point is moved proportionally. This process will be hard for low-resolution images. Gholap and Bora et al. [8] proposed a method, that describes color mismatches among objects are considered for forgery detection. This method performs good in images that contains specular highlight. Bo Xu, Guangjie Liu, and Yuewei Dai et al. [3] tried to detect the splicing forgery introduced abnormality using SRM. The experimental results indicate that the proposed method can detect splicing forgeries with much higher accuracy than in luminance channel. Reshma P.D and Arunvinodh et al. [2] proposed a technique of image forgery detection based on color illuminance was described. In this technique an improved forgery detection method was presented that .In this paper Classifier tests the image. The main advantage of this work is that it completely avoids user interaction and provides a crisp Statement on the authenticity of the image.

## III. THE PROPOSED WORK

The techniques used in the proposed forgery detection method are explained in this section. System Framework is shown in Fig2.

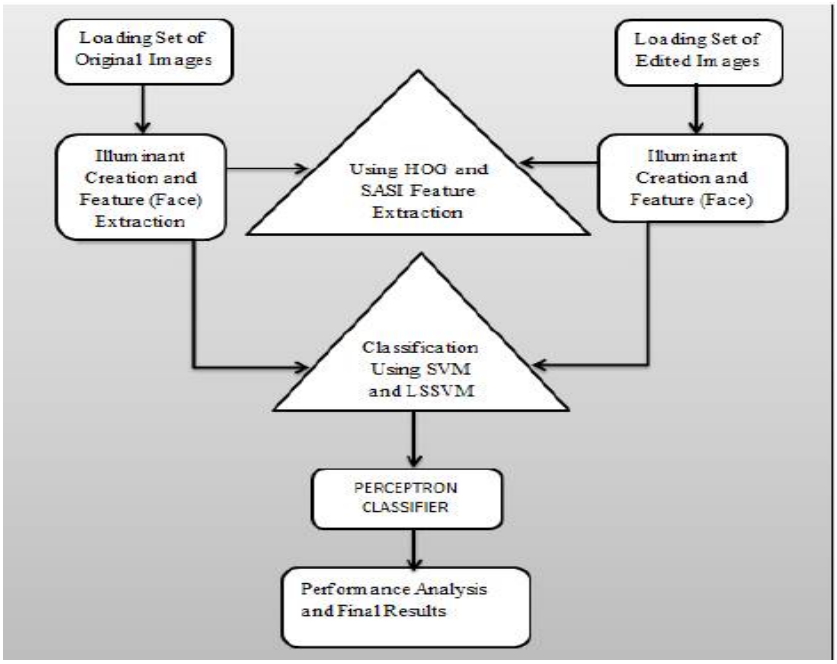


**Fig 2: System Framework**

ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 6, June 2016

Overview of System framework: In this paper, we used the concept illuminant color inconsistency and machine learning classifiers for forgery detection. The method mainly consists of the following steps.

A Estimation of illuminant color: Illuminant color is estimated for input images. Then new images are created i.e. illuminant map for each image that is read.

B Extraction of face: All faces present in one image and corresponding all faces of other individual images are extracted for investigation. Result of Face extraction is shown in Fig 3.

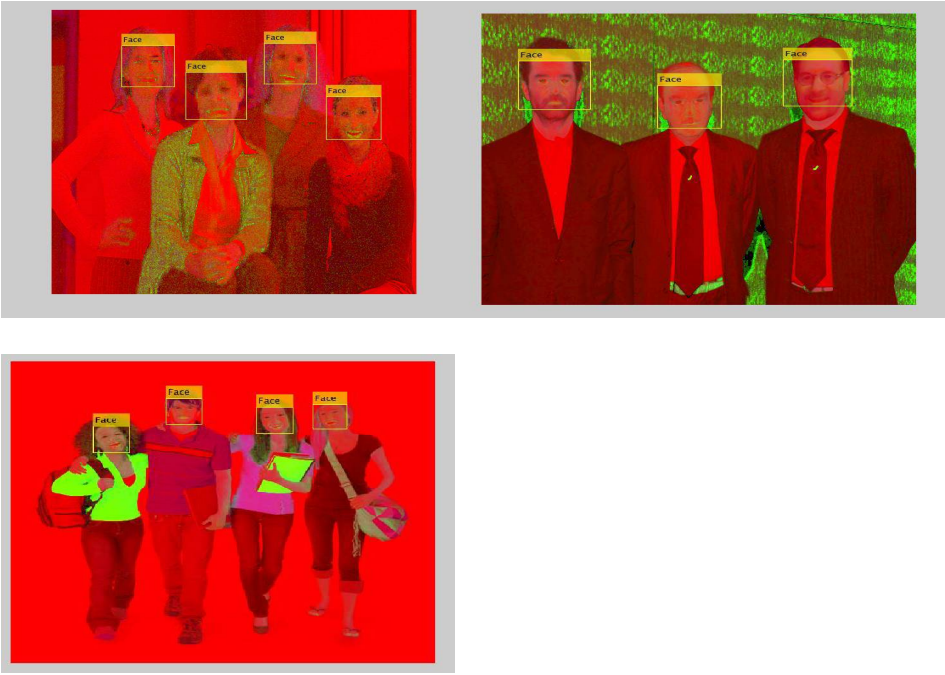


**Fig 3: Results of color illuminance, Feature extraction, and Face extraction of various edited images using SVM and LSSVM**

C Extraction of features: There is a need to extract textural and gradient features. The information regarding spatial arrangement of color in an image is given by Image texture. This helps us to understand content of image clearly. HOG, SASI, features are extracted.

D HOG: Histogram of Oriented Gradients: We used HOG that is an edge descriptor and is used for the purpose of object detection in computer vision and image processing. Histogram of Oriented Gradient descriptors or edge directions mainly 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. HOG directions for the pixels within the cell are computed. Feature descriptor is the combination of these histograms. There may be variations in the extracted HOG features depending on the size and shape of face under construction. So feature vectors of fixed length should be obtained [9].

E SASI: Statistical analysis of structural information**:** We used SASI that is a Texture Descriptor. It extracts the texture information from illuminant map and captures the small granularities and discontinuities in texture pattern. SASI is a generic descriptor that is used to measure the structural properties of textures. It is based on the autocorrelation of horizontal, vertical and diagonal pixel lines over an image at different scales [9]. ROC's of HOG and SASI of edited images are shown in Fig.4.

ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

*(An ISO 3297: 2007 Certified Organization)*

**Vol. 5, Issue 6, June 2016**

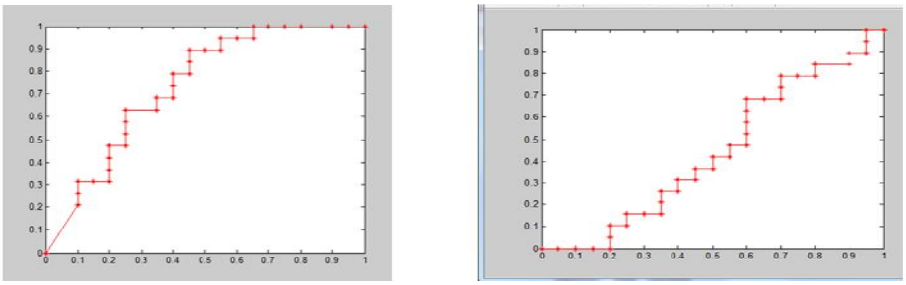

**Fig 4: ROC's of set of edited images using HOG and SASI**

F Classification: The two features which are computed in previous step are given as input to the classifier. Then classifier classifies the image either original or edited with the help of SVM and LSSVM classifier. LSSVM Is added to selected folders to improve accuracy as compared to SVM. Then the perceptron classifier is used to compute the class of an image.

G Support Vector Machines (SVM): We used SVM as it is a machine learning classifier and is powerful methodology for solving problems in nonlinear classification, function estimation and density estimation which has also led to many other recent developments in kernel based methods in general.

H Least squares support vector machines (LS-SVM) are least squares versions of support vector machines (SVM), which are a set of related supervised learning methods that analyze data and recognize patterns, and which are used for classification and regression analysis. In this version we finds the solution by solving a set of linear equations instead of a convex quadratic programming (QP) problem for classical SVMs. Least squares support vector machines (LS-SVM) is a version of SVM that involves equality constraints and works with a least squares cost function [9].

I Perceptron Classifier**:** In machine learning, the perceptron is an algorithm for supervised learning of binary classifiers: functions that can decide whether an input (represented by a vector of numbers) belongs to one class or another. It is a type of linear classifier, i.e. a classification algorithm that makes its predictions based on a linear predictor function combining a set of weights with the feature vector. The algorithm allows for online learning, in that it processes elements in the training set one at a time. We used this classifier for the prediction of edited images. Results of Classification are shown in fig 5.

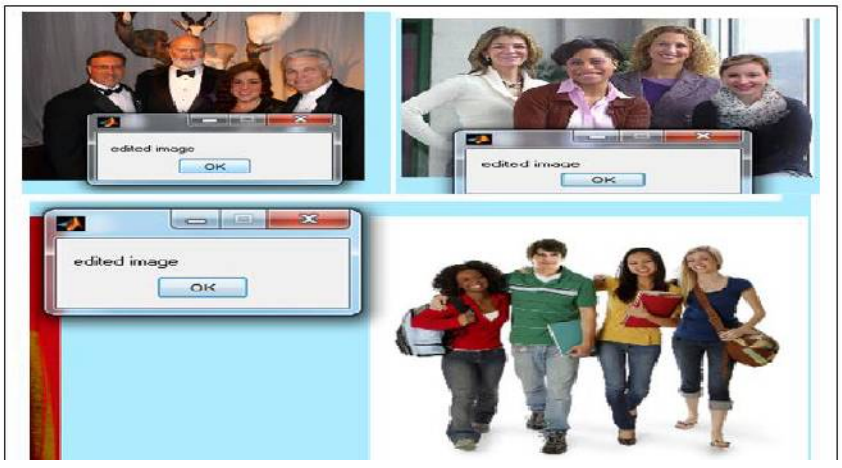


**Fig 5: Results of perceptron Classifier**

ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

*(An ISO 3297: 2007 Certified Organization)*

**Vol. 5, Issue 6, June 2016**

## IV. GRAPHICAL REPRESENTATION

Graphs are plotted between the old SVM and Modified SVM using LSSVM. Comparison is based upon the accuracy between the old SVM and Modified SVM. More is the accuracy, better are the Results. Fig 6 shows the graphical representation in the form of bar graphs.

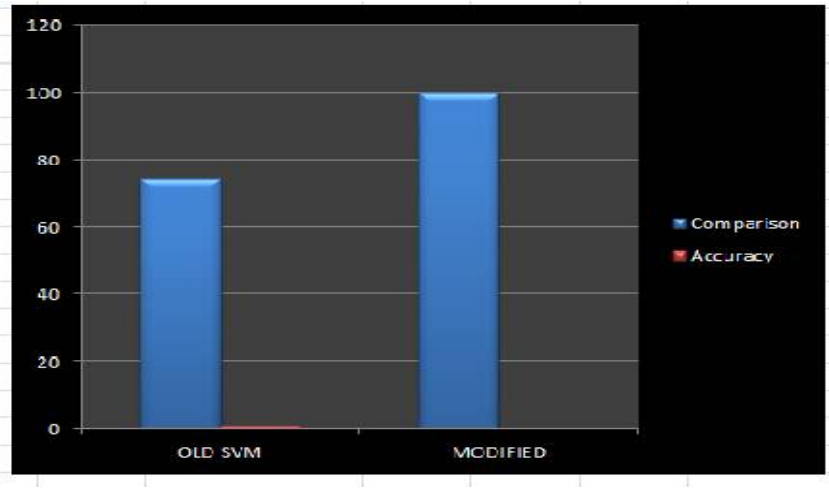


**Fig 6: Graphical Representation**

## V. CONCLUSION

The overall work is implemented by the use of many machine learning classifiers SVM, LSSVM, Perceptron and color illumination by extracting features in MATLAB platform. The advantage of proposed work is that user interaction is completely removed and is capable of detecting many different forged images. In this work, an improved forgery detection method .This work is only capable of detecting spliced images.

## REFERENCES

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

[2] Arunvinodh C and M.F, Reshma P.D, "Image Forgery Detection Using Svm Classifier," IEEE Sponsored 2nd International Conference on Innovations in Information Embedded and Communication Systems", 2015.

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

[4] Luo, Weiqi, Jiwu Huang, and Guoping Qiu, "Robust detection of region-duplication forgery in digital imagel, Pattern Recognition", ICPR 18th International Conference on. Vol. 4. IEEE, 2006.

[5] B. L. Shiva Kumar and Lt. Dr.Santosh, "Detecting Copy Move Forgery in Digital Images: A Survey and analysis of current methods", Global Journal of Computer Science and Technology, vol.10, 2010.

[6] M. K. Johnson and H. Farid,"Detecting photographic composites of people", in Proc. 6th Int. Workshop on Digital Watermarking, Guangzhou, China,2007.

[7] P. K. Bora and Sandeep Gholap,"Illuminant Colour Based Image Forensics", Proc. IEEE Region 10 Conf, pp. 1-5, 2008.

[8] S.L.Jothilakshmi and V.G.Ranjith,"Automatic Machine Learning Forgery Detection Based On SVM Classifier", (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (3), 2014, 3384-3388, 2014.

[9] J.A.K. Suykens J. De Bra banter, L. Lukas and J. Vandewalle,"Weighted least squares support vector machines: robustness and sparse approximation", Elsevier, Neurocomputing 48 85–105, 2002.