FORGERY IMAGE DETECTION BASED ON ILLUMINATION COLOR CLASSIFICATION WITH ADVANCED SKIN COLOR AND EDGES

Dinesh Kumar C. Dr . D.Surendran M.E.,(Ph.D)

,

***Abstract*—In recent days, photographs have been used as evidence in courts. Photographers are able to create composites of analog pictures, this process is very time consuming and requires expert knowledge. Today, Powerful digital image editing software makes image modifications straightforward. This undermines our trust in photographs. In this paper, one of the most common forms of photographic manipulation, known as image composition or splicing is analysed .A forgery detection method that exploits subtle inconsistencies in the color of the illumination of images. The proposed approach is machine-learning based and requires minimal user interaction. The technique is applicable to images containing two or more people and requires no expert interaction for the tampering decision. Here, the existing work can be extended by using advanced face detection method using skin tone information and edges . A lighting insensitive face detection method based upon the edge and skin tone information of the input color image is proposed. From these illuminant estimates, we extract texture- and edge-based features which are then provided to a machine-learning approach for automatic decision-making.**

***Index Terms*—Color constancy, illuminant color, image forensics, machine learning, spliced image detection, texture and edge descriptors.**

1 INTRODUCTION

Image processing is a wide concept and in basically here ,the digital image processing is discussed.On analysing this,one of the most common forms of photographic manipulation known as image composition or splicing is found.A image is forgered by splicing the original image that are called as analog pictures[1].So that the forgered image plays as a vital role in courts for evidence.By having the forgered image many rumours has been arised.

- *C.Dinesh Kumar is currently pursuing masters of engineering in computer science and engineering in Sri krishna college of engineering and technology ,coimbatore, PH-9788410501. E-mail: dineshkumarit06@gmail.com*
- *D.Surandran is currently working as a Associate Professor in computerscience and engineering from sri krishna college of engineering and technogy,coimbatore, PH-9865020489*

The forgery image is not viewed be different from the original image.To differentiate both the images a SVM classifier is used.Fig. 1. How can one assure the authenticity of a photograph? Example of a spliced image involving people.

There are two process which are used to detect the images whether it is forgered or real one. A trained examples are stored in the database and are put into SVM classifier[5]. The images in the support vector machine is used to classify the real image and forgered image .So by *following* all the steps which are described in the list of the modules, a forgered image is detected. A brief explanation is given in every segment for which they are used and demonstrate how the forgery picture is detected[8].

Image composition (or splicing) is one of the most common image manipulation operations. One such example is shown in Fig. 1,is a modified image in which there are group of boys .The person who is 2nd and 3rd from right is inserted. Although this image shows a harmless manipulation case, several more controversial cases have been reported, e.g., the 2011 Benetton Un- Hate advertising campaign1 or the diplomatically delicate case in which an Egyptian state-run newspaper published a manipulated photograph of Egypt's former president, Hosni Mubarak, at the front, rather

than the back, of a group of leaders meeting for peace talks.

1.1 FORGERED IMAGE

Digital images in the modern world play very important role in areas like forensic investigation, insurance processing, surveillance systems, intelligence services, medical imaging and journalism. But the basic requirement to believe what we see is that the images should be authentic. With the advancement of technology and availability of fast computing resources, it is not very difficult to manipulate or forge the digital images. The availability of some software tools makes the problem more menacing. Despite this there is no method available to detect all types of tampering with accuracy. Before coming to the discussion of forgery detection techniques; it is necessary to know about the different types of tampering done with digital images. There are many ways to categorize the image tampering based on different points of view (for a categorization .Generally, we can say that the most oftenly performed operations in image tampering are:

- Deleting or hiding a region in the image.
- Adding a new object into the image.
- Misrepresenting the image information.

Copy move image tampering is one of the frequently used techniques to hide or manipulate the content of the image. Some part of the same image or some other image is pasted on another part of image. To detect the region of some other image statistical methods may work but if the region pasted belongs to the same image then it's quite difficult to detect this forgery[6]. Many methods have been suggested to detect this type of forgery.

The art of making an image forgery is almost as old as photography itself Photo manipulation has become more common in the age of digital cameras and image editing software. Gathered below are examples of some of the notable instances of photo manipulation in history. so based on the examples this work focus on the instances that have been most controversial or notorious, or ones that raise the most interesting ethical questions . The photographers have also experimented with composition.

Fig .2. The Examples of original and modified image are shown.

In this photo by famed photographer Mathew Brady, General Sherman is seen posing with his Generals. General Francis P. Blair (far right) was added to the original photograph. The photo on the left is another image from the same sitting, at which General Blair was not in attendance.

Digital images offer many attributes for tamper detection algorithm to take advantage of - specifically the color and brightness of individual pixels as well as an image's resolution and format. These properties allow for analysis and comparison between the fundamentals of digital forgeries in an effort to develop an algorithm for detecting image tampering. This paper focuses on images saved in the JPEG format. Therefore a research work on basis of compression scheme is discussed to determine what information can be gathered about a digital forgery saved in this format.

1.2 OBJECTIVE

With regard to providing confidentiality for images, the project work helps to determine the orginality of the images. In this project, a advanced face detection method using skin tone information and edges. The skin tone color constancy is extracted from every image and the comparision is done between different images.The comparision is done with the images already stored in the database which are trained one.The trained images are compared with the testing images .Finally, by having the features of the training and testing images ,the forgered images is detected if it mismatch eachother.

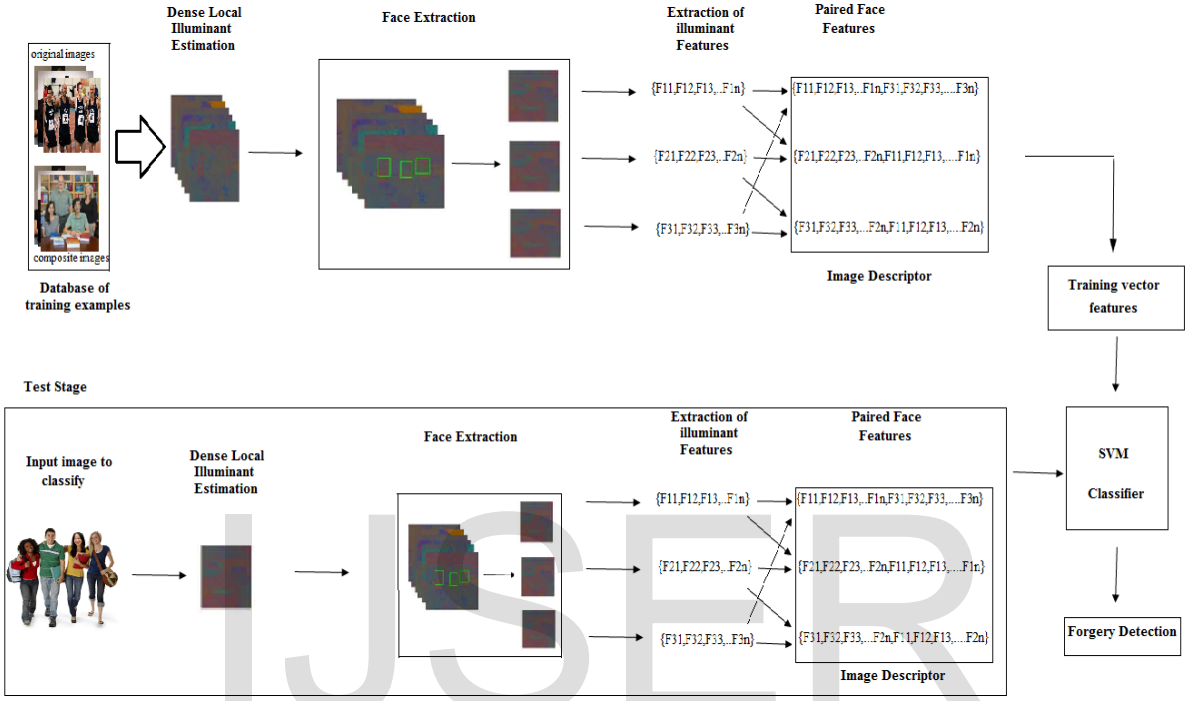

Fig .3.Overview of proposed system

2 EXISTING SYSTEM

In existing, many methods has been proposed for detecting the forged images.Tiago jose de carvalho proposed in [1] that illumination-based methods for forgery detection are either geometry-based or color-based [6] [7] [8] has been used . Geometry-based methods focus at detecting inconsistencies in light source positions between specific objects in the scene has been used . Color-based methods search for inconsistencies in the interactions between object color and light color [2] has been used .

An early approach of multi-illuminant estimation has been done.In this smoothly blending illuminants used a diffusion process to recover the illumination distribution.By exploring with this pixelwise illuminant estimator is used . It allows to segment an image into regions illuminated by distinct illuminants. Differently illuminated regions can have crisp transitions, for instance between sunlit and shadow areas. The issues of the existing system are it oversmooths the illuminant boundaries.And it donot scale well on smaller image regions.A single illuminant estimator always fails.

3 PROPOSED SYSTEM

In the proposed system,an important step towards minimizing user interaction for an illuminant-based
tampering decision-making [3] was made. A new semiautomatic method that is also significantly more reliable than earlier approaches has been proposed. Quantitative evaluation showed that the existing method achieved a detection rate of 86%, . The exploitation of the fact can be done

that local illuminant estimates are most discriminating when comparing objects of the same (or similar) material. Thus, the automated comparison of human skin, and more specifically faces, to classify the illumination on a pair of faces as either consistent or inconsistent has been made. User interaction is limited to marking bounding boxes around the faces in an image. The main advantages of this work are it requires only minimum amount of human interaction and it gives good result for achieving over internet images and also under cross-database training/testing. More than that robust security has been also achieved.

A advanced face detection method using skin tone information and edges. The skin tone color constancy is extracted from every image and the comparision is done between different images.The comparision is done with the images already stored in the database which are trained one.The trained images are compared with the testing images .Finally, by having the features of the training and testing images ,the forgered images is detected if it mismatch eachother.

The Fig.4 shows the overview of the proposed method.It gives the complete knowledge of the work done in the project.Initially the images are taken and it is splited into orginal and edited image.The images are splited for the purpose of comparision of detection of forged and orginal image.Here it describes two types of process. One is test stage while the other one is training process.In both the process, the steps involved will resembles each other. First the dense illuminant estimation is extracted from the images of the training examples.The illuminant is found for all the image in the database.Then the face extraction is done where here the faces is cropped by using a rectangle boxes.And the images is splited to extract the illuminant features.These features are extracted using SASI and HOGedge algorithm.The features are then paired to give a combination of features which is used to detect the forgery image for future use.These process are done in the training database.

The test stage also follows the same steps done in the training set,but the only change is that a individual image is taken for the process. At the last the SVM(Support Vector Machine) is used to classify the images which are from training feature vector and test stage.In the classification steps ,the forgered image is detected if any of the features mismatch eachother.so that image is called as forged image.

4 EXPECTED RESULTS

The standard images have been taken for the analysis of the project. The expected results are from both the original and edited images.In the process, it gives the accuracy of 80% of the images are real images.

5 CONCLUSIONS

In this work, new method for detecting forged images of people using the illuminant color has been discussed. The illuminant color using a statistical gray edge method and a physics-based method which exploits the inverse intensity chromaticity color space has been estimated.These illuminant maps are treated as texture maps.An information on the distribution of edges on these maps are extracted.

In order to describe the edge information, a new algorithm based on edge-points and the HOG descriptor, called HOGedge is proposed. We combine these complementary cues (texture- and edge-baed) using machine learning late fusion.The results are encouraging, yielding an AUC of over 86% correct classification. Good results are also achieved over internet images and under cross-database training/testing. Although the proposed method is custom-tailored to detect splicing on images containing faces, there is no principal hindrance in applying it to other, problem-specific materials in the scene. The proposed method requires only a minimum amount of human interaction and provides a crisp statement on the authenticity of the image. Additionally, it is a significant advancement in the exploitation of illuminant color as a forensic cue. Prior color-based work either assumes complex user interaction or imposes very limiting assumptions.

6 REFERENCES

[1].Tiago Jose de Carvalho,Christian Riess,Elli Angelopoulou and Helio Pedrini "Exposing Digital Image Forgeries By Illumination Color Classification" *IEEE Trans. Inf. Forensics Security* ,Vol. 8, no. 7, pp. 1182 - 1194, July 2013.

[2]. R. Kawakami, K. Ikeuchi, and R. T. Tan, "Consistent surface color for texturing large objects in outdoor scenes," in *Proc. IEEE Int. Conf. Comput. Vision*, 2005, pp. 1200–1207.

[3]. S. Gholap and P. K. Bora, "Illuminant colour based image forensics," in *Proc. IEEE Region 10 Conf.*, 2008, pp. 1–5.

[4]. J. F. O'Brien and H. Farid, "Exposing photo manipulation with inconsistent reflections," *ACM Trans. Graphics*, vol. 31, no. 1, pp. 1–11, Jan. 2012.

[5]. J. Lukas, J. Fridrich, andM.Goljan, "Digital camera identification from sensor pattern noise," *IEEE Trans. Inf. Forensics Security*, vol. 1, no.2, pp. 205–214, Jun. 2006.

[6] M. Johnson and H. Farid, "Exposing digital forgeries by detecting inconsistencies in lighting," in Proc. ACM Workshop on Multimedia and Security, New York, NY, USA, 2005, pp. 1–10.

[7] Y. Ostrovsky, P. Cavanagh, and P. Sinha, "Perceiving illumination inconsistencies in scenes," Perception, vol. 34, no. 11, pp. 1301–1314, 2005.

[8]. S. Bianco and R. Schettini, "Color constancy using faces," in *Proc. IEEE Comput. Vision and Pattern Recognition*, Providence, RI, USA, Jun. 2012.

[9]. W. Fan, K. Wang, F. Cayre, and Z. Xiong, "3D lighting-based image forgery detection using shape-from-shading," in *Proc. Eur. Signal Processing Conf. (EUSIPCO)*, Aug. 2012, pp. 1777–1781.