# IMAGE COMPOSITE DETECTION USING CUSTOMIZED

Shrishail Math and R.C.Tripathi

Indian Institute of Information Technology,Allahabad
ssm@iiita.ac.in
rctripathi@iiita.ac.in

***ABSTRACT***

*The multimedia applications are rapidly increasing. It is essential to ensure the authenticity of multimedia components. The image is one of the integrated components of the multimedia. In this paper ,we desing a model based on customized filter mask to ensure the authenticity of image that means the image forgery detection based on customized filter mask. We have satisfactory results for our dataset.*

***KEYWORDS***

*Customized Mask, Filter. Image composite, splicing, Image forgery*

## 1. INTRODUCTION

Widespread easy and low cost availability of digital cameras and the prevalence of photo sharing and management websites such as flicker, Picasa and other popular websites provide the photo sharing and management applications in one or other forms. Digital images are playing every important role in our daily life; the digital images are omnipresent right from the cover pages of journals, newspapers, magazines etc. to evidences in court rooms, teaching aids etc. Images are used everywhere either as a personal memory evidences or for official purposes.

Recently, the low cost camera, sophisticated high end image processing, computer graphics software, made editing and manipulated images become easier, hence there is essential to detect the forgeries in the images. There are many types of forgeries such as morphing, copy move, compositing, retouching, etc. The image compositing is more popular one.

## 2. IMAGE COMPOSITE FORGERY

Image compositing is most popular image forgery. The figure 1 shows the creation of image compositing. The photo compositing is the result of cutting and joining a two or more photographs with seamless transition without leaving any visual clues about the joining from other photographs.

DOI : 10.5121/ijcga.2011.1301

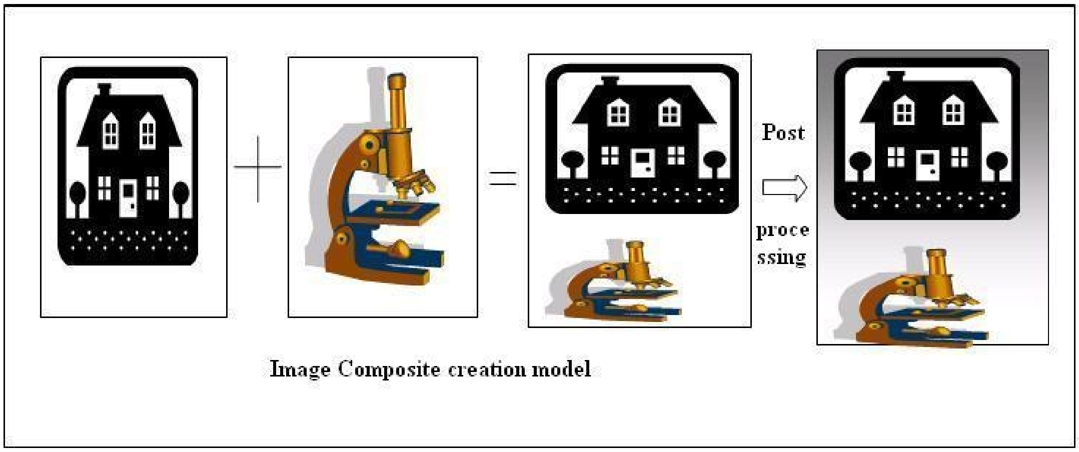

Figure 1: Composite image creation model

## 3. RELATED WORKS

The image compositing is also known as photomontage and image splicing. The image compositing detection assumes that the image scene authenticity properties and conditions such as illuminations, object surface properties, shadow, noise, inter-reflections. Perspective and projective views etc. are rare and difficult match in a composite image. The image composite detection techniques are able to detect the above inconsistent properties in different parts of the same images, the image edges, boundaries and colors, and image qualities may be affected by image compositing.

The image forgery can be identified by the specific patterns relating to image attributes which disturbed by the forgery operations. Particularly image composting is created by the two or more images sources, naturally all the different images are taken from the different devices and at different world view conditions. The host image conditions are expected to reflect in image portions of the altered images. The abrupt and unnatural luminance levels, colors and edges are able to detect the image forgeries. In this paper, we used customized filter masks method to detect the image forgeries.

The image splicing is analyzed in a general way [1, 2, 9], using supervised approaches [2, 9], and using statistical methods [1] as seen in the literature.

The pixel continuity is disturbed due to cut and joining of other images. This feature is exposed to detect the image splicing using support vector machine by Dong et al [9] . He further demonstrates that the correlation and coherency of pixels are not continued at the stitching points.

In [5,7], proposed methods uses the camera response function to determine an image splicing , in [10,11], Yu-Feng Hsu and Shih-FuChang estimates the camera response function using geometric invariants, while [6,7] uses edge based profile.

Zhouchen Lin et al [4] uses the inverse camera response function (CRF) using the analyzing the edges in different patches and verifies the consistency.

Hany Farid and Mary J.Bravo [42] propose the several computational methods for detecting the inconsistencies in shadows and reflections. While Wei Zhang et al [1] detect the image compositing using the geometric and photometric constraints on shadows . Sandeep Gholap and P.K.Bora [12] estimate the illuminant color to expose the image splicing.

MicahK.Johnson and HanyFarid [5] estimated the direction of light from specular highlights that appears on the image eye to detect the image compositing by demonstrating the scene authenticity are differs in composite images.

The researchers used a variety of methods to detect the image forgeries, however very few researchers such as Lukas used image processing methods such a filtering using standard Roberts, sobels and prewitts mask identify the image forgeries, we extend the Lukas concept by designing a customized mask.

# 4. PROPOSED METHOD

## 4.1 Detection of tampering based on customized filtering masks

Several edge detectors based on sobel and prewitts masks are used to detect the image forgery by Lukas[13,14]. Image filtering is used as an effective tool in image analysis and understanding problems. Image filtering is useful in image sharpening, smoothing, noise removal, edge detection and many pre and post processing operations. Filtering can be performed in the spatial domain and frequency domain.

Filtering provides the alternate view of an image and therefore uncovers small anomalies the image tampering creates anomalies. The customization of masks may prove vital information to uncover a forgery or providing further validations.

In the spatial domain, a filter is defined by a mask or the kernel, which is a small array such a 3X3 ,5X5 etc, which is applied to each pixel and their neighbours within an image. The centre of the kernel is aligned with a current pixel and is square with an odd number (3,5,7 etc.) of elements in each dimension , this process is known as a convolution, This way of pixel grouping provides a way to show a trend in an image, such as brightness level across a particular area.

The abstract representation pixel and their eight connected neighbours are shown below.

| | | |
|---|---|---|
| $X_{i-1,j-1}$ | $X_{i-1,j}$ | $X_{i-1,j+1}$ |
| $X_{i,j-1}$ | $X_{i,j}$ | $X_{i,j+1}$ |
| $X_{i+1,j-1}$ | $X_{i+1,j}$ | $X_{i+1,j+1}$ |

Let $X_{i,\ j}$ be pixel at location i. j in image X, the remaining pixels are eight way connected neighbour. The pixel value, which is integer is extracted and manipulated with mask (Kernel)

Let the mask be

$$\begin{pmatrix} k_{11} & k_{12} & k_{13} \\ k_{21} & k_{22} & k_{23} \\ k_{31} & k_{32} & k_{32} \end{pmatrix}$$

The filter's output pixel will be result of Convoluted Image pixels and the mask.

The Filter's result will be mathematically represented as

$$\mathit{Output\ pixel}\ x_{i,j} = [\ (\ x_{i-1,j-1}(k_{11}) + x_{i-1,j}(k_{12}) + x_{i-1,j+1}(k_{13}) + x_{i,j-1}(k_{21}) +$$

$$x_{i,j}(k_{22}) + x_{i,j+1}(k_{23}) + x_{i+1,j-1}(k_{31}) + x_{i+1,j}(k_{32}) + x_{i+1,j+1}(k_{33})\ \ )$$

The result of the above operation emphasizes the trends in the image, particularly, abrupt pixel variability in the edges, more importantly at tampered regions. This is due to the averaged eight connected neighbor pixels that are used to determine new pixel value. To see more effective results an image is divided into blocks and convolution is performed on block bases. The smaller the block size will give better results.

## 5. EXPERIMENT AND RESULTS

Lukas analyzed the forgery detection based on filters [13]. He used the standard mask such as Sobel. Robert, Prewitt and Marr masks. These methods has a limited application and ability of forgery detection, However these masks provide the foundation for image filtering. We are extending the concept of filtering based on customized mask to tailor the filtering that is resulting in a better revelation of forgery traces. The concept of the kernel or filter mask and convolution are explained in section 4

We designed the customized masks by empirically, for example the first customized mask is

$$\begin{pmatrix} -1 & -2 & -2 \\ -2 & 14 & -2 \\ -2 & -2 & -1 \end{pmatrix}$$

Customized Mask

The Customized Mask is designed in such a way that the sum of all connected neighbours weight is equal to the centres pixels weight. This mask effectively filters out statistically similar areas in the image and only shows dissimilar regions or areas. These different dissimilar results are aroused from prominent edges or maybe from the forged regions of an image. The results provide the alternate way of viewing results on screen or in printouts.

The results are dark, sometimes inverted results reveals the abnormalities. First we convert the image to grey scale image so that the statistical data of the original authentic image doesn’t affect by convolution with a customized mask.

The given figure 2 shows the test image and its result from customized mask figure 3 and the inverted result of customized result shown in figure 4. The inverted result clearly shows the traces of forgery.

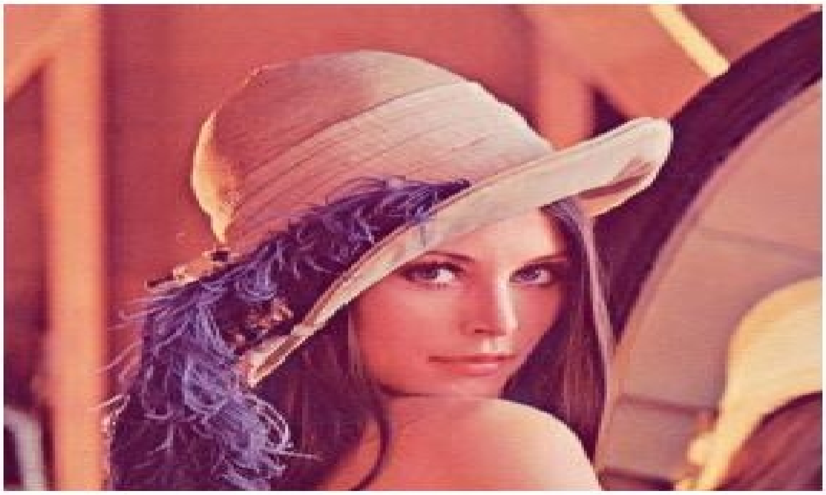

Figure 2: Test image

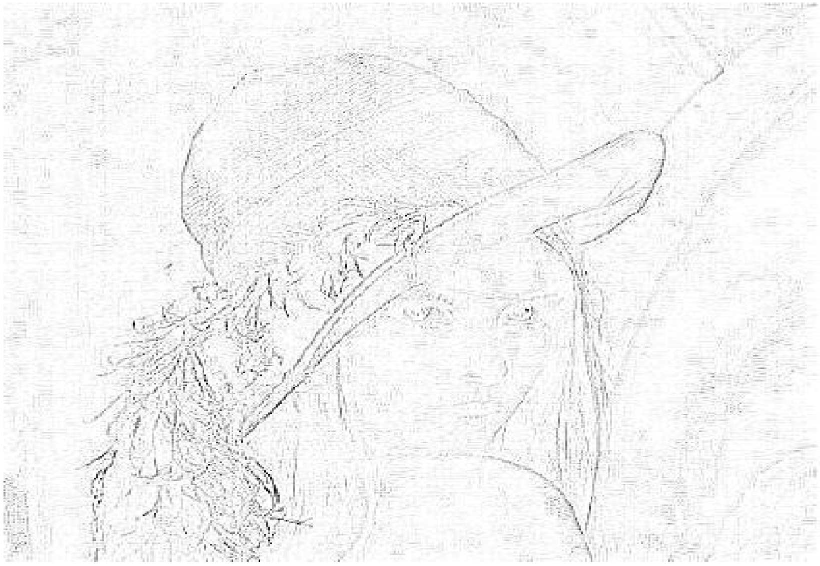

Figure 3: Result of customized filter mask

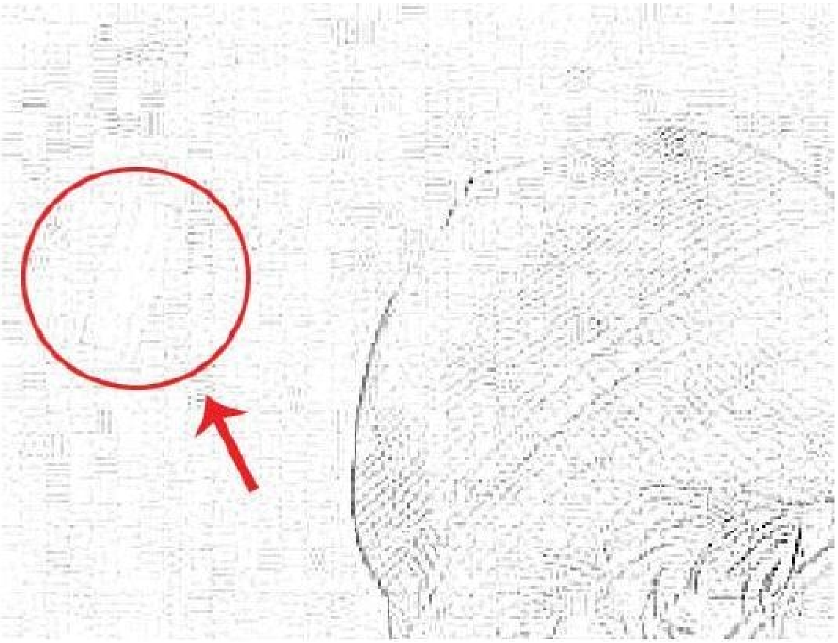

Figure 4: inverted result of customized mask result

Table 1: summary of forgery detection methods and image formats used

| Forgery detection method | Grey Scale image | BMP | RGB | PNG | JPEG |
|---|---|---|---|---|---|
| Customized Filter Mask | X | X | X | X | X |

We tabulate the results of customized filter tests on ten forged images at different levels of forgeries and the results and interpretation of results. The test image and their attributes

Table 2: Summary of Customized filter results

| Forgery | Inconclusive Signs of Tampering | Possible Signs of Tampering (further tests or analysis is required) | Definitive Signs of Tampering |
|---|---|---|---|
| Test image 1 |  | X |  |
| Test image 2 | X |  |  |
| Test image 3 |  |  | X |
|  |  |  |  |
| Test image 5 |  | X |  |
| Test image 6 | X |  |  |

| | | | |
|---|---|---|---|
| Test image 7 | | X | |
| Test image 9 | | X | |
| | | X | |

We are summarizing the results of all the three methods on both unforged and forged images. We used the 25 unforged images and 20 forged images. The results are tabulated as below.

## 6. CONCLUSION AND DISCUSSIONS

It is well known fact that there is no single technique to determine all the type of forgeries. This chapter introduced three simple and effective methods for detecting the image forgery, specifically for image compositing type of forgery. Each method focused on the image attributes, which are changed by the forgeries. For testing, we had small image dataset, however overall results were found satisfactory. It was realized that user of our technique will have to decide on his/her own discretion which method will suit which type of case. Need was also felt to extend the work for using technique of “fusion” to obtain most optimum results utilizing all the three methods to complement each other.

## REFERENCES

[1] W.Zhang,,X.Cao,J.Zhang,J.Zhu,P.Wang, “Detecting photographic composites using shadows ,in: IEEE International Conference on Multimedia and Expo,2009,pp.1042–1045.

[2] W.Wang,J.Dong,T.Tan, “Effective image splicing detection based on image chroma“,in: IEEE International Conference on Image Processing,2009.

[3] J.Lukas,”Digital image authentication using image filtering techniques”, in: Proceedings of ALGORITMY 2000, Conference on Scientific Computing,Podbanske,Slovakia,September2000, pp. 236–244.

[4] Z.Lin,,J.He,X.Tang,C.K.Tang, “Fast, automatic and fine-grained tampered jpeg image detection via dct coefficient analysis ,Pattern Recognition 42(11)(2009)2492–2501.

[5] M.Johnson.H.Farid” ,Exposing digital forgeries through specular highlights on the eye”, in: 9th International Workshop on Information Hiding,SaintMalo,France,2007.

[6] Y.F.Hsu, S.-F.Chang, “Detecting image splicing using geometry invariants and camera characteristics consistency “, in: ICME,2006, pp. 549–552.

[7] Y.F.Hsu, S.-F.Chang, “Image splicing detections using camera response function consistency and automatics estimation “, in: ICME, 2007, pp.28–31.

[8] H.Farid.M.Bravo,” Image forensic analyses that elude the human visual system “,in: SPIE Symposium on Electronic Imaging , SanJose, CA, 2010.

[9] J.Dong,W.Wang,T.Tan,Y.Shi,“Run-length and edge statistics based approach for image splicing detection”, in: Digital Water- marking, 7th International Work shop, IWDW2008, Busan, Korea, November 10 -12, 2008, pp.76–87.

[10] E.S.Gopi, N.Lakshmanan, T.Gokul, S.Kumara Ganesh, P.R.Shah, “Digital image forgery detection using artificial neural network and auto regressive coefficients”,in: CCECE,2006, pp.194–197.

[11] H.A.Gou.Swaminathan, M.Wu, "Noise features for image tampering detection and steganalysis ", in :ICIP(6), IEEE, San Antonio, USA,2007,pp.97–100.

[12] S.Gholap, P.K.Bora , "Illuminant colour based image forensics ", in: TENCON 2008,TENCON 2008. IEEE Region10 Conference, IEEE Computer Society, Hyderabad, India, November 2008, pp.1–5.

[13] J.Lukas,"Digital image authentication using image filtering techniques", in: Proceedings of ALGORITMY 2000, Conference on Scientific Computing, Podbanske, Slovakia,September2000, pp. 236–244.

[14] J.Lukas, J.Fridrich, M.Goljan," Detecting digital image forgeries using sensor pattern noise", In SPIE Electronic Imaging, Photonics West 2006.

## Authors

### Short Biography

Shrishail Math received his BE(Electronics and Communication Engineering), M.Tech( Computer Science and Engineering) from University of Mysore and Manipal University in year 1996 and 2001 respectively . currently,Doctroal student at Indian Institute of Information Technolgy,Allahabad, his research interests are information assurance and security and multimedia forensics.

R.C.Tripathi is Dean Student affair , Worked as senior director Ministry of Communication and Information Technology(MCIT),Govt.of India. He published three books and 70 research articles and papers in international and national journals. He worked as a co-chairman of 1st International conference on Intelligent Interactive Multimedia (IITM 2010 sponspored by ACM.