
2-Tier Image Forgery Detection using Contrast Enhancement and 3D Lighting

Prof. Manisha Fegade.

Shivajirao S. Jondhale College
Of Engineering,
Dombivli ,India

Prof. Nilima D. Nikam.

Yadavrao Tasgoankar Institute
of Engineering and
Technology, Bhivpuri Rd,
India

Prof. Vaishali Londhe

Yadavrao Tasgoankar Institute
of Engineering and
Technology,
Bhivpuri Rd, India.

Abstract

Nowadays the digital image plays an important role in human life. Due to large growth in the image processing techniques, with the availability of image modification tools any modification in the images can be done. These modifications cannot be recognized by human eyes. So Identification of the image integrity is very important in today's life. Contrast and brightness of digital images can be adjusted by contrast enhancement. Another type of modifications include copy and paste type, in which some part of one image is copied and pasted to another image. Here in this topic contrast enhancement technique is used which aimed at detecting image tampering has grown in different applications area such as law enforcement, surveillance. Also with the contrast enhancement, we propose an improved 3D lighting environment estimation method based on a more general surface reflection model. In this we are dealing with the light direction angle.

Also we intend to use face detection method to detect the face existence and 3D lighting environment estimation to check originality of human faces in the image.

Keywords: Forgery detection, contrast enhancement, light, reflection, copy and move.

1. INTRODUCTION

With the rapid development of digital media editing techniques, digital image manipulation becomes rather convenient and easy. Currently, image forgeries are widespread on the Internet and other security-related applications such as surveillance and recognition that utilize images are therefore

impacted. With the new advancement of technology, availability of fast and powerful computing devices and extremely powerful digital image processing tools such as Adobe Photoshop and Freehand, it is very easy to manipulate, forge or tamper digital image without leaving any obvious clue. An image can be tampered in various ways: deleting or hiding a segment in the image, adding a new object in the image and misrepresentation of image information. To circumvent such a problem, digital forensic techniques have been proposed to blindly verify the integrity and authenticity of digital images.

In our daily life, we see things which are not always what we think they usually look like. It is just because we believe something to be true does not necessarily mean it is true. It is also just because we do not believe something does not mean that it is not true. Authenticity is the basic requirement to believe what we see is that the data, which may be image or video.

2. PROPOSED SCHEME

In existing system, two contrast enhancements based algorithms have been proposed. These algorithms based on histogram bins and peaks analysis. Parallel approach used to increase the performance of the system. Zero height gap bins, measures are exploited as identifying features. Here global contrast enhancement detection algorithm, works well for previously Jpeg compressed images with medium and low quality factor. It means that

image enhancement techniques are applied after the Jpeg compression strategy. Prior works for composition detection fails to identify which type of manipulation was enforced. But composite detection method identifies the manipulation using the similarity values. Splicing attack more or less similar to move and- paste attack. Both techniques modify the certain region of image. But move-and-paste attack uses portion of the original image as its source image. i.e. the source and destination of the modified image originated from the same image. This algorithm also identifies the splicing attack.

Disadvantage: The process can detect smaller forgeries and the process needed to improve for spatial resolution. There is need of improvement for facial images since in face images the similarities were difficult to identify since the face skin tones and the textures were similar.

In this proposed system, original image and modified image have been taken as input for detecting forgery portion. Histogram is one of the most important parameter to check contrast of an image. So, histogram of both the images is calculated. Both the histograms are compared. If the difference between both histogram is zero then we can conclude that the image is original or else it is forged. In second tier of the system we will use face detection algorithm for detecting face. If image consist of face then 3D lighting technique is applies to check forgery. Then performance is analysed for effective accuracy. The calculated performances indicate that the proposed method is capable for the identification of copy move forgery in the images with greater accuracy.

Advantages

The process can be able to identify the copy move regions in the images more effectively due to the two stages matching of the images. As the input image is verified twice in two tier for forgery detection, it can achieve more accurate results. Also the system can work for other type of image forgeries. Even if the modified image is not of copy and paste type then also our system can detect originality of image.

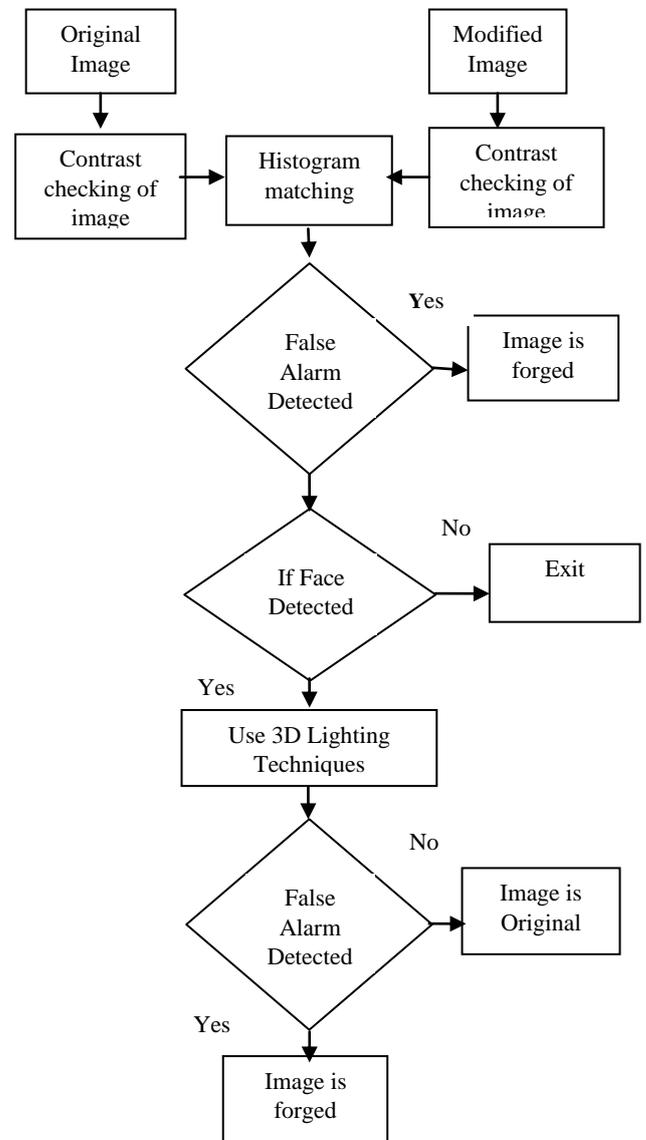


Figure 2.1 Flow Diagram For Proposed System

3. RESULTS

In this I propose a system for detecting originality of image that is to check whether the input image is forged or original. This can be achieved by matching contrast and 3D lighting effect of an image.

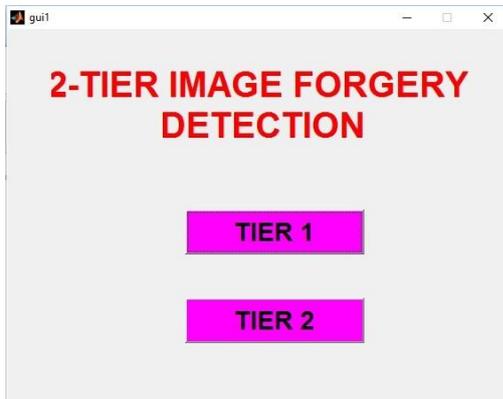


Figure 3.1 : Basic GUI of the System



Figure 3.2: Input Image (a)



Figure 3.2: Input Image (b)

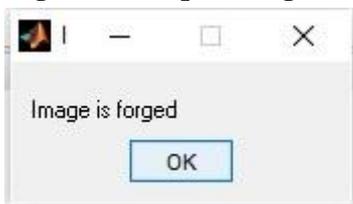


Figure 3.3: Results of Tier 1

In figure 3.2 (a) and (b) input image and its reference image is considered. Then it is checked for contrast enhancement. As seen in figure the

brightness is changed so image is modified. So, result shows image is forged.



Figure 3.4: GUI for Tier 2

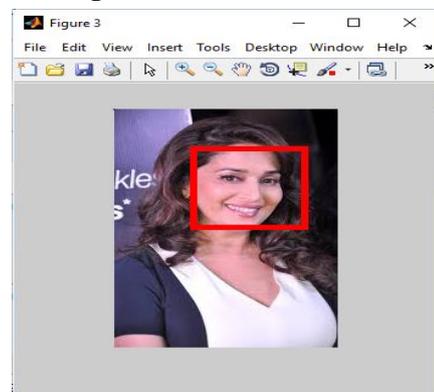


Figure 3.5: Face Detection

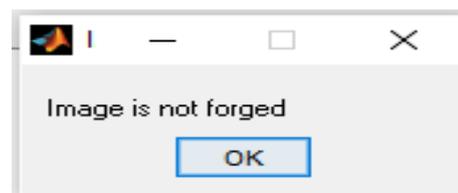


Figure 3.6: Result for Tier 2

As shown in figure 3.4 we will input image and will check it for face detection as shown in figure 3.5. this face is checked for lighting direction and other background part is also checked for lighting direction. As it is same conclusion is image is not forged.

4. CONCLUSION

Images are effective means of natural communication for humans due to their immediacy as well as the easy way of understanding the image content. The contrast enhancement technique is

typically used to adjust the global brightness and also the contrast of digital images. Malicious users may perform contrast enhancement locally for creating composite image which looks like real image. Thus, it is important to detect contrast enhancement for verifying the originality and even the authenticity of the digital images.

In this system of forgery detection will be performed in 2-tiers. In first tier contrast of an original and forged image is checked. Based on the contrast matching image is judged for forgery. If image has human face, then in the second tier human face is checked for forgery that whether the face is original or forged. This will be achieved by using 3D lighting effects. This 2-tier forgery detection will be capable for the identification of copy move forgery in the images with greater accuracy. Even this system will work for other type of foregeries like smoothing, sharpening of image, colour change of image etc.

REFERENCES

- [1] Ms.S.T Suryakanthi Sornalatha, Ms.S.Devi Mahalakshmi, Dr. k. Vijayalaxmi, "Detecting Contrast Enhancement based Image forgeries by Parallel Approach", IEEE sponsored 2nd international conference on electronics and communication systems (ICECS '2015), 978-1-4244-xxxx-x/09.
- [2] Bo Peng, Wei Wang, Jing Dong and Tieniu Tan, "Improved 3D Lighting Environment Estimation for Image Forgery Detection", 2015 IEEE International Workshop on Information Forensics and Security (WIFS)- 978-1-4673-6802-5/15.
- [3] Hany Farid "2009, Image Forgery Detection A Survey", IEEE Signal processing Magazine.
- [4] B.I. Shivakumar, Lt. Dr. S.Santhosh Baboo. "detecting copy - move forgery in digital images: A survey and analysis of current methods", Global journal of Computer science and technology, vol. 10, pp. 61 - 65, 2010.
- [5] Harpreet Kaur, Jyoti Saxena and Sukhjinder Singh, "Key -point based copy-move forgery detection and their Hybrid methods", Journal of the International Association of Advanced Technology and science, Vol. 16, June 2015.
- [6] Anselmo Ferreira, Siovani C. Felipussi, Carlos Alfaro, Pablo Fonseca, John E. Vargas-Muñoz, Jeferson A. dos Santos, and Anderson Rocha, "Behavior Knowledge Space-Based Fusion for Copy-Move Forgery Detection", TRANSACTIONS ON IMAGE PROCESSING 2016.
- [7] P.M. Panchal, S .R. Panchal and S.K, Shah, "A comparison of SIFT and SURF", International journal of innovative Research in computer and communication engineering " Vol. 1, April 2013.
- [8] Mohd Dilshad Ansari, S. P. Ghreera & Vipin Tyagi : "Pixel-Based Image Forgery Detection: A Review" IETE Journal of Education, 40-46(Aug 2014).
- [9] Johnson and Hany, (2005) "Exposing digital forgeries by detecting inconsistencies in lighting", in Proc. ACM Workshop on Multimedia and Security, New York, NY, USA, pp. 1–10.
- [10] Hany Farid and Alin C. Popescu, (Feb 2005) "Exposing Digital Forgeries by Detecting Traces of Resampling", Signal Processing, IEEE Transactions on (Volume:53 , Issue: 2).
- [11] Nikhilkumar P. Joglekar, Dr. P. N. Chatur "A Compressive Survey on Active and Passive Methods for Image Forgery Detection" International Journal Of Engineering And Computer Science ISSN:2319-7242 , Volume 4 , Page No. 10187-10190, 1 January 2015.
- [12] E. Kee and H. Farid, "Exposing digital forgeries from 3-d lighting environments," in *Information Forensics and Security (WIFS), 2010 IEEE International Workshop on.* IEEE, Conference Proceedings, pp. 1–6.
- [13] F. Wei, W. Kai, F. Cayre, and X. Zhang, "3d lighting-based image forgery detection using shape-from-shading," in *Signal Processing Conference (EUSIPCO), 2012 Proceedings of the 20th European,* Conference Proceedings, pp. 1777–1781.
- [14] T. Carvalho, H. Farid, and E. Kee, "Exposing photo manipulation from user-guided 3d lighting analysis," in *IS&T/SPIE Electronic Imaging.* , International Society for Optics and Photonics, 2015, pp. 940 902–940 902.
- [15] Gang Cao, Yao Zhao, Rongrong Ni and Xuelong Li, "Contrast Enhancement-Based Forensics in Digital Images", IEEE Trans. Information forensics and security, vol. 9, No. 3 April 2013.
- [16] A. C. Popescu and H. Farid, "Exposing digital forgeries by detecting traces of resampling," *IEEE Trans. Signal Process.*, vol. 53, no. 2, pp. 758–767, Feb. 2005.
- [17] M. Stamm and K. J. R. Liu, "Blind forensics of contrast enhancement in digital images," in International Conf. on Image Processing, San Diego, 2008.
- [18] M. Stamm and K. J. R. Liu, "Forensic detection of image tampering using intrinsic statistical fingerprints in histograms," in Proc. APSIPA Annual Summit and Conference, Sapporo, 2009.
- [19] M. C. Stamm and K. J. R. Liu, "Forensic estimation and reconstruction of a contrast enhancement mapping," in *Proc. IEEE Int. Conf. Acoust., Speech Signal, Dallas, TX, USA, Mar. 2010, pp. 1698–1701.*