International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 4 Issue: 11 257 – 260

Image Forensics for Forgery Detection using Contrast Enhancement and 3D Lighting

Ms. Manisha Fegade.
Shivajirao S. Jondhale College Of Engineering,
Dombivli ,India
fegademanisha@gmail.com

Prof. Nilima D. Nikam.
Yadavrao Tasgoankar Institute of Engineering and Technology,
Bhivpuri Rd, India
nilu.nikam@gmail.com

Prof. Vaishali Londhe
Yadavrao Tasgoankar Institute of Engineering and Technology,
Bhivpuri Rd, India.
vaishali.londhe@tasgaonkartech.com

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. Move and paste type of images are Created by malicious person, in which contrast of one source image is enhanced to match the other source 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. 3D lighting environment is an important clue in an image that can be used for image forgery detection. We intend to employ fully automatic face morphing and alignment algorithms.

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, 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 means 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. LITERATURE REVIEW

A wide variety of multimedia editing software, both commercial and open source, are currently available to every computer user. The facility and powerful editing functionality of such software makes digital image manipulation become easy and frequent. So the originality, integrity and even authenticity of digital images may suffer destruction. To recover the human's trust on digital image data, there is an increasing need for developing techniques to detect digital image manipulation in the manner of blind and passive. Image manipulation forensics is just such a technique.

In general, prior works on digital image manipulation forensics can be labeled into two categories. In the first category, forensics methods concentrate on identifying the content-changing image manipulations including image splicing and copy-move which reshape the image content visually and semantically. In the second category, content-preserving image manipulations such as resampling, compression, contrast enhancement, blurring, sharpening and median filtering are detected or estimated passively.

In first survey [4], B.L. Shiva Kumar, Lt. Dr. S. Santhosh Baboo discusses various methods of detecting copy -move image forgery in dig ital images. They compare region duplication detection with scaling and rotation and without scaling and rotation. They also discuss various challenges like tempered region with compression, tampered image with noise, tempered region with rotation.

In [5] Harpreet Kaur, Jyoti saxena and sukhjinder singh compare all the keypoint based copy-move Forgery detection. Keypoint methods like SIFT, SURF, ORB. According to author keypoint based methods are better than block based methods in terms of computational efficiency space complexity and robustness against rotation and scaling. They conclude that SIFT is better than ORB and

SURF in terms of accuracy whereas in terms of time for detection ORB is faster than SURF and SIFT.

In [7],P.M.Panchal, S.R.Panchal, S.K.Shah present the comparison of two keypoint algorithm SIFT (Scale Invariant Feature Transform) & SURF (Speed Up Robust Feature). Both are used to point-out the distinctive invariant features from an image that can be used to compare different angles of image.

Johnson and Farid proposed a method based on the specular highlights that appear on the eye are a powerful cue to shape, color and location of the light source [9]. Inconsistencies in these properties of light can be used as evidence of tampering. It can applicable to arbitrary objects, but this method only determines the direction to the light source within one degree of ambiguity. The inconsistencies in the shape of the specular highlight on the eyes suggest that the people were originally photographed under different lighting conditions. The location of a specular highlight can be used to determine the direction to the light source. Inconsistencies in the estimates from different eyes, as well as differences in the shape and color of the highlights, can be used to reveal traces of digital tampering.

Farid method consider the fact that while creating a digital composite image, the matching of lightning conditions of digital image is very difficult between the individual photographs[10].The differences in lighting can be used as a factor for detecting digital tampering. But the main drawback with this approach is it is not applicable for indoor images.

3. 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 increases the performance of the system. Zero height gap bins, measures are exploited as identifying features. Composition detection algorithm works well for previously Jpeg compressed images.

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. Then both the images are segmented by using SLIC algorithm. Affine transformation and global contrast detection algorithm is used to check contrast of image is checked. If contrast found then we can conclude as image is forged. If image found as original then face detection algorithm will be used for detecting face. If image consist of face then 3D lighting technique is applies to check forgery. Then performance is analysed for effective accuracy.

Perform patch matching process based on the extracted points and detect the forgery portion. Analysis of the performance in terms of precision and recall. The patch based matching helps in locating the forged pixels more exactly in the images. The identification of the most interested points helps in reducing the time in checking each and every pixel of the image. The applications of the affine transformations for the identification of the similarities in the images were capable for the identification of the interested points in the images more effectively. 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. The segmentation based on SLIC method which is the most effective Super pixel segmentation method for the segmentation of the images. The matching process is employed in patch wise manner and hence the complexity in segmentation and matching is much reduced. The extraction of the features based on the affine transformation extracts the most interested points in the images more effectively. 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.

In this proposed system, original image and modified image have been taken as input for detecting forgery portion. Then both the images are segmented by using SLIC algorithm. Affine transformation and global contrast detection algorithm is used to check contrast of image is checked. If contrast found then we can conclude as image is forged. If image found as original then face detection algorithm will be used for detecting face. If image consist of face then 3D lighting technique is applies to check for conclude for forgery. Then performance is analysed for effective accuracy.

 ISSN: 2321-8169
257 – 260

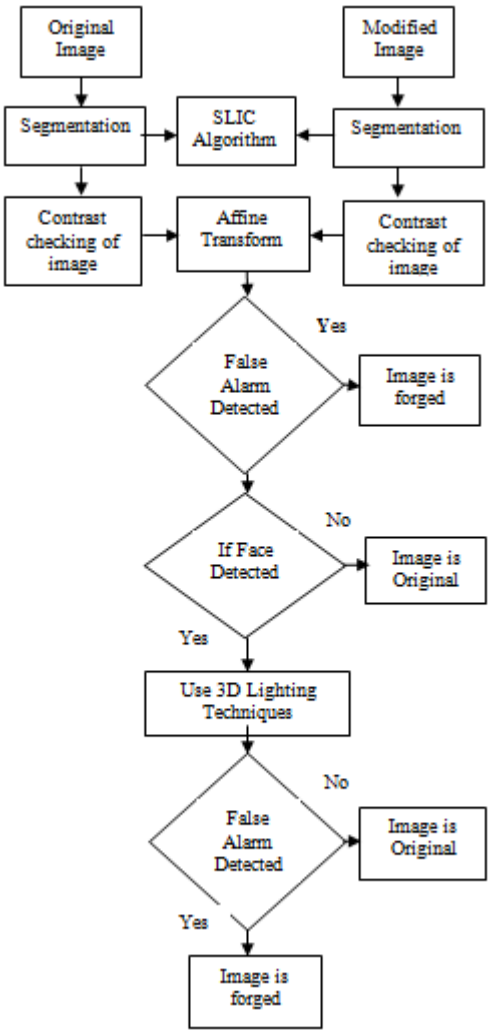

Figure 3.1 Flow Diagram For Proposed System

4. SYSTEM ARCHITECTURE

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.

1. Pre-processing:

In this proposed approach the forensic in the photography mainly copy move changes were analyzed. Initially take the original and modified image for input.

2. Affine Transformation:

Features will be extracted from original and forgery image using affine transformation. An affine transformation or affine map is a function between affine spaces which preserves points, straight lines and planes. Also, sets of parallel lines remain parallel after an affine transformation. An affine transformation does not necessarily preserve angles between lines or distances between points, though it does preserve ratios of distances between points lying on a straight line.

3. Patch Matching Process:

The patch based matching helps in locating the forged pixels more exactly in the images. The identification of the most interested points helps in reducing the time in checking each and every pixel of the image.

4. EM based Matching:

Expectation Maximization (EM) algorithm is used to detect forgery of digital image by computing the interpolated coefficients for the given image.

5. Detection of forgery Image:

After performing different matching as mentioned above post processing includes the result that whether the image is original or not.

6. Performance Analysis:

The calculated performance indicates that the proposed method is capable for the identification of copy move forgery in the images with greater accuracy.

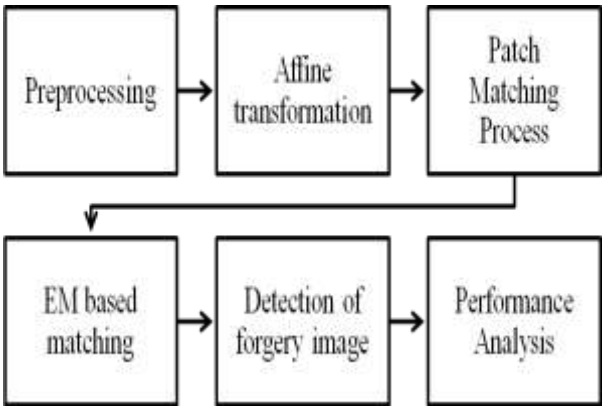

Figure 4.1 System Architecture

5. SECURITY ANALYSIS

To determine whether the digital image is authentic or not is a key purpose of image forensics. There are several different types of tampering attacks. This can be detected by checking various parameters like contrast, brightness, image distortion, shades and shading, lighting effects etc. using this individually forgery detection can be performed. But in proposed system I am using 2-tier for forgery detection. In first tier contrast is checked, if in first tier image doesn't found forged then image will move towards second tier. If image contains human face, then originality of that face is checked by 3D lighting. So the image with equal contrast and different faces can be judge by second tier. So this proposes system will provide better accuracy.

6. APPLICATION

Image forgery detection can be used in various fields involving image processing. Nowadays social media is rapidly evolving. Social media uses much of the data as image. So it is necessary to have original image instead of forged image. Image forgery detection can be used in many applications. Some of them are mentioned below:

- Information security
- News recording
- Military
- Law enforcement
- Crime forensics
- Medical image security
- Photography

7. 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 the proposed system 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.

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 2'nd 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 Comput er science and t echnology, 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-Mu˜noz, Jefersson 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. Ghrera&VipinTyagi :"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 Faridy and Alin C. Popescu, (Feb 2005) "Exposing Digital Forgeries by Detecting Traces of Re-sampling", 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.*