Identifying Photo Forgery using Lighting Elements

Manoj Kumar and Sangeet Srivastava*

1Department of Computer Science and Engineering, The NorthCap University, Gurugram - 122017, Haryana, India; wss.manojkumar@gmail.com
2Department of Applied Sciences, The NorthCap University, Gurugram - 122017, Haryana, India; sangeetsrivastava@ncuindia.edu

Abstract

Nowadays digital media manipulation has become a common trend. Digital media, especially images, being one of the primary modes of communication, can be easily manipulated. Current research trends in digital image forensics focus on validating the authenticity of the image. **Objectives:** Objective of the present study is to authenticate objects in an image using light sources and their properties. **Method:** By locating the direction of the light source, forgery in the images can be easily detected. Inconsistencies between different light sources in the image highlight image tampering. This paper focuses on detection of image forgery using lighting inconsistencies. The proposed technique measures the lighting properties from different objects or surfaces present in the image. **Finding:** The model for digital forensics identifies the lighting discrepancies in the objects of an image and provides results indicating difference between real and fake images. **Improvement:** The proposed technique is an objective based method and identifies digital image forgery based on physics of the environment. Results are promising and reproducible making the technique an important tool for image forgery detection.

**Keywords:** Authenticity, Image Forensics, Image Tampering Detection, Lighting

1. Introduction

Digital data, including image, audio and video, are major information carriers in this digital period. This digital data is massively shared and distributed over the internet and due to this, data is prone to manipulations. Digital images are present everywhere as a proof of truthfulness, but due to the availability of cheap and high technical editing software this truthfulness is no longer reliable. Image processing experts can easily manipulate images and therefore its meaning without leaving any detectable traces1. This results in modification of image for malicious or unauthorized purpose. Image forensics is the branch of multimedia security which helps to locate the image manipulations based on various traces available in the image data.

Figure 1 and Figure 2 shows some of the image forgeries reported recently. In Figure 1 car is intentionally copied from one part of the original image (Left) and pasted to form a new image (Right). Figure 2 shows forgery by manipulating men’s face in the image.

Image forgeries are classified into copy move, Image splicing, image retouching and lighting condition.

![Figure 1](image1.png)

**Figure 1:** Left part is original while the right is fake2

One of the most common techniques is copy move where some part of the original image is used to perform forgery. Image splicing can be done by composing two different images in a single image. Image retouching
Identifying Photo Forgery using Lighting Elements

can be done by modifying or enhancing image features. Sometimes an image splicing is performed in such a way that the manipulation is visually impossible to identify lighting conditions in a composite image. In such cases light source are estimated to detect the forgeries.

**Figure 2:** Forged Image where Wong Su from DAP-China forged a photograph receiving knighthood from Queen Elizabeth-II.

There exist many approaches in the literature for identifying tampering in the digital images. All the existing techniques change some kind image data that is related to statistical, geometrical and physical properties. Pixel based forgeries are performed by changing pixel data during the compression or by changing wavelet coefficients for image objects. Authors in described a forensic approach using DWT. They applied DWT to the input image to produce a reduced dimension representation. After this they compressed the overlapping blocks and from this duplicated blocks are identified by using Phase correlation. Their technique is robust to detect copy move forgeries. In they calculated image features using HAAR and Biorthogonal wavelets for image compression in a more efficient manner. Their technique can also be used to improve the pixel based image forgery detection. The paper extracted the feature vectors from the image blocks. They decomposed the image using DWT wavelet decomposition and later applied SVD to detect the forgery. Pixel based techniques identifies the low level correlations between pixels and locates the tampering traces. Sensor based techniques detect inconsistencies in the chromatic aberrations, colour filter array interpolation by using sensor noise. Recent work related to these techniques can be studied from.

Cryptography and encryption schemes can be applied to protect the images against pixel based tampering. Techniques which can make image forgery difficult and helps in counter forensics can be extended the work done by.

Detecting Lighting inconsistencies is another well-known technique for forgery detection. Lighting inconsistencies can be detected using 2D, 3D surface information and radiance information from an image. Recent work by explored the lighting inconsistencies using specular highlights in the eyes. They showed that how the direction of light source can be estimated from the specular highlights from eyes. Author in proposed a tampering detection method based on shadows, geometrical and optical properties of image. They implemented their approach based on the planer homology phenomenon between shadows from a light source. If the homology constraint for all the objects in an image is not consistent then it means image is doctored one. In a similar approach by proposed a method of shading and shadows on the projected light source direction. They solved the problem by making it as a linear programming problem. They formulated the shading of object constraint of 3D light source and projected into 2D image. This technique is robust to detect the light source direction for forgery detection. Author in proposed a 3D lighting analysis based digital image forensics technique. They showed that an expert can postulate 3D shape and from this 3D light can be easily estimated. A perturbation analysis is further performed to produce a probabilistic measure for the location of the light. In this paper, we tried to minimize certain assumptions as in. This paper uses the concept of different illumination patterns for calculating object surface features which are described in the following sections of this paper. To make optics based technique more robust an approach is suggested in can be implemented. They carried out a study of optical image encryption in the Fresnel transform domain, using a Random Phase Mask (RPM) in the input plane and a phase mask based on Devil’s Vortex Toroidal Lens (DVTL) in the frequency plane. Even though their scheme is valid for grayscale and binary images but it is robust against occlusion and noise attacks. In authors designed a new geometrical approach for identifying fake and real images. The applied segmentation techniques on image are to find the forgery. With geometrical representation they applied Top-Hat filtering and grey scale reconstruction for identifying forgery with curved surface reflection. Their results show the robustness of their technique. The proposed paper finds the inconsistencies using the lighting properties in an image. Our scheme validates whether an image is fake or real based on light inconsistencies.
The proposed paper is divided into four Sections. The Methodology of this paper is discussed in Section 2 followed by experimental outcomes in Section 3. Section 4 concludes the proposed methodology and suggests future improvements in this work.

2. Proposed Methodology

In this paper, 3D light is estimated from user provided data. A user has to select 3D shape in the image by defining probes for estimation of lighting. By knowing certain factors such as shading, shadows and slant angle the estimation of 3D shape can be easily obtained. Even, it is very difficult to estimate the 3D shape of surfaces, but by knowing above mentioned factors this can be achieved. To remove the uncertainties and error optimization the least square optimization is performed in this work.

A user can locate 3D shape in the image by adjusting the probe orientation w.r.t z axis and by providing corresponding slant angle $\sigma$. A probe consists of a circular base and a small vector orthogonal to the base of the probe. The user has to select this probe on the image surface such that the vector seems to be orthogonal to the object surface. To obtain the 3D shape of the image surface, we require a point $p$ and slant angle which coincide with the direction of viewer to surface. Slant angle is provided by manually estimating the direction of the surface normal onto the image. Figure 3 shows the image plane and local coordinate system to obtain the probe. Here, a user also specifies the start point and end point on the object surface which helps to estimate the orientation of the probe which is stored in a vector $v$. In the proposed work the length of this vector is limited to 10 pixels. If any unknown user selects vector length greater than 10 pixels, then the proposed algorithm automatically truncates the extra pixels.

The 3D probe is constructed using following orthogonal vectors $A1, B1$ and $C1$ as shown in Equation (1). In this $p$ is the location of the probe, $f$ is focal length, which is a mid-range value in this experiment and $c$ is principal point.

\[
A1 = \begin{bmatrix} 1 \\ f \\ p \\ 1 \end{bmatrix} \quad C1 = \begin{bmatrix} 1 \\ \frac{1}{f} \\ \frac{f}{p} \\ 1 \end{bmatrix} \quad B1 = A1 \times C1
\]

Probe’s base lies in the $B1$ and $C1$ plane. This user selected probe is parameterized by slant $\sigma$ and tilt $\tau$. To obtain both these parameters we use following rules as defined in Equation (2).

\[
\sigma = \sin^{-1}\left(\frac{1}{f} \right), \quad \tau = \tan^{-1}\left(\frac{\nu_1}{\nu_2}\right)
\]

The 3D shape construction requires both $f$ and $c$. The value of $c$ is w.r.t orthogonal projection is considered as zero. In the next step of the proposed method, using the obtained 3D shape and surface normal the calculation for light estimations is processed.

In the proposed work, we assume that the illumination on the surface of the scene is constant around all the directions and is illuminated by a single point light source. This assumption gives us a basic terminology related to the radiance of the scene which is given by $r = n.s + a$. In this $n$ is surface normal obtained by $n^T = (n_x, n_y, n_z)$, $s$ is light source direction, obtained by $s^T = (s_x, s_y, s_z)$ and $a$ approximates the indirect illumination i.e. light term. In $r$, there are four unknown parameters which are $s_x, s_y, s_z$ and $a$. So to obtain the lighting coefficients for 3D light estimation, we need at least four surface patches (k) on the image surface with same intensity values. By combining $r$ and $n$, we attained following linear system as shown in Equation (3).

\[
\begin{pmatrix}
n_i^T \\
\vdots \\
n_k^T
\end{pmatrix}
\begin{pmatrix}
1 \\
\vdots \\
1
\end{pmatrix}
= 
\begin{pmatrix}
r_i \\
\vdots \\
r_k
\end{pmatrix}
\]

In terms of lighting parameters this linear system in Equation (3) can be written as $Ne = r$. Further, to optimize the errors in lighting parameters a least square optimization is applied by applying $e = (N^T N)^{-1} N^T r$. In the proposed work, forgery is identified in terms of azimuth $\Phi = -\tan^{-1}(s_y/s_x)$ and elevation $\theta = \sin^{-1}(s_z/||s||)$ w.r.t image plane. Obtained results of the proposed work show that this technique is able to identify lighting inconsistencies. The difference between $\Phi$ and $\theta$ for various image
patches (fake and real) identifies the tampering with the image. In this work, the range of azimuth and elevation values lies from $(-\pi \text{ to } \pi)$ and $(-\pi/2 \text{ to } \pi/2)$ correspondingly.

### 3. Experimental Outcomes

The results of the proposed technique are carried out using some existing images which are taken from and some are captured by our cameras. For all images, this technique shows its robustness and works on user provided data and detects forgery in image objects based on estimation of light source. Figure 4 shows the doctored image in which user selects probes on different patches. In this image football is fake with respect to the entire scene. The obtained results in Table 1 show that football is inconsistent with estimated light source compared to other objects in the image. For every patch user selected 7 to 10 probes in this work. The value of $\Phi$ lies from $-100^\circ$ to $-95^\circ$ while for $\theta$ the values varies from $-15^\circ$ to $-25^\circ$. First four values in Table 1 are consistent while the values obtained from football are inconsistent w.r.t. first four values.

| Selected Patch        | $\Phi$ | $\theta$ |
|-----------------------|--------|----------|
| Dark Boy Face         | -100   | -15      |
| Dark Boy Elbow        | -95    | -25      |
| Fair Boy Elbow        | -120   | -18      |
| Fair Boy Face         | -95    | -18      |
| Football              | 90     | 25       |

In Figure 5, a dog is intentionally inserted to check the performance of the proposed work. Figure 6 demonstrates results for measured $\Phi$ and $\theta$ for Figure 5. In this, user select probes on two different corners of image grass and one from the dog face. Experimental results as indicated in Figure 6 show that lighting on dog face is inconsistent while rest patches are consistent with the scene.

### 4. Conclusion

In the proposed paper, we presented a digital image forensic technique based on assessment of the light source(s) for an image. This technique is able to estimate the lighting properties and hence detects the forgeries for various objects present in the image. Lighting directions are estimated by using azimuth and elevation/orientation parameters. The errors may appear in results depending on the user choice for selecting the probes. This can be overcome by implementing the automatic selection of probes. The proposed approach generates the 3D shape which is further used to detect the 3D lighting in the image for various objects. Finally, least square optimization is used to improve the accuracy of this technique. In future, this technique can be designed for more than one light source environments and can also be improved for different illumination intensities where probes are chosen on uneven intensities simultaneously.
5. References

1. Redi JA, Taktak W, Dugelay J-L. Digital image forensics: a booklet for beginners. Multimedia Tools and Applications. 2011; 133–62.
2. Farid MKJAH. Exposing digital forgeries by detecting inconsistencies in lighting. ACM Multimedia and Security Workshop; 2005.
3. Khan ES, Kulkarni EA. An efficient method for detection of copy-move forgery using discrete wavelet transform. International Journal on Computer Science and Engineering. 2010; 2(5):1801–6.
4. Chaudhary MP, Lalit G. Lifting scheme using HAAR and biorthogonal wavelets for image compression. International Journal of Engineering Research and Applications. 2013; 3(4):474–8.
5. Dan QT, Li SS, Wu G. A sorted neighborhood approach for detecting duplicated regions in image forgeries based on DWT and SVD. ICME; 2007.
6. Kee E, Johnson M, Farid H. Digital image authentication from JPEG headers. IEEE Transactions on Information Forensics and Security. 2011 Sep; 6:1066–75.
7. Pan X, Lyu S. Region duplication detection using image feature matching. IEEE Transactions on Information Forensics and Security. 2010; 5(4):857–67.
8. Popescu A, Farid H. Exposing digital forgeries in color filter array interpolated images. IEEE Transactions on Signal Processing. 2005; 53(10):3948–59.
9. Kirchner M. Efficient estimation of CFA pattern configuration in digital camera Images. Society of Photo-Optical Instrumentation Engineers (SPIE); 2010.
10. Fridrich J. Digital image forensic using sensor noise. IEEE Signal Processing Magazine. 2009; 26(2):26–37.
11. Kaur N, Mahajan N. Image forgery detection using SIFT and PCA classifiers for panchromatic images. Indian Journal of Science and Technology. 2016 Sep; 9(35):1–6.
12. Elwin GJKGR. Image forgery detection using multidimensional spectral hashing based polar cosine transform. Indian Journal of Science and Technology. 2015 May; 8(9):28–39.
13. Vashisth S, Singh H, Yadav AK, Singh K. Devil’s vortex phase structure as frequency plane mask for image encryption using the fractional mellin transform. International Journal of Optics. 2014; 1–9.
14. Vashisth S, Singh H, Yadav AK, Singh K. Image encryption using fractional Mellin transform, structured phase filters, and phase retrieval. Optik - International Journal for Light and Electron Optics. 2014 Sep; 125(18).
15. Jeyakumar K. Image compression and fusion based technology using wavelet transform. Indian Journal of Science and Technology. 2015 Nov; 8(32):1–8.
16. Johnson M, Farid H. Exposing digital forgeries through specular highlights on the eye. 9th International Workshop on Information Hiding; Saint Malo, France. 2007.
17. Zhang W, Cao JZX, Zhu J, Wang P. Detecting photographic composites using shadows. IEEE International Conference on Multimedia and Expo; 2009. p. 1042–5.
18. Kee E, O’Brien JF, Farid H. Exposing photo manipulation from shading and shadows. ACM Transactions on Graphics. 2014; 33(5):1–21.
19. Carvalho T, Farid H, Kee E. Exposing photo manipulation from user guided 3D lighting analysis. SPIE Symposium on Electronic Imaging; San Francisco, CA. 2015.
20. Singh H, Yadav AK, Vashisth S, Singh K. Optical image encryption using devil’s vortex toroidal lens in the fresnel transform domain. International Journal of Optics. 2015; 1–20.
21. Cristin VCRR. Exposing image manipulation with curved surface reflection. Indian Journal of Science and Technology. 2016 Oct; 9(38):1–9.
22. Stevens KA. Surface tilt (the direction of slant): A neglected psychophysical variable. Perception and Psychophysics. 1983; 33(3):241–50.
23. Belkasoft. Forgery Detection Plugin. Belkasoft forensics made easier. Available from: https://belkasoft.com/forgery-detection.
24. Kumar G, Gaharwar S, Nath VV, Gaharwar R. Neuro-fuzzy based first responder for image forgery identification. Orient Journal of Computer Science and Technology. 2016 Apr; 9(1):12–6.