



ELSEVIER

Available online at www.sciencedirect.com



August 2014, 21(4): 83–91
www.sciencedirect.com/science/journal/10058885

The Journal of China
Universities of Posts and
Telecommunications

<http://jcupt.xsw.bupt.cn>

Exposing photo manipulation with inconsistent perspective geometry

LI Yan (✉), ZHOU Ya-jian, YUAN Kai-guo, GUO Yu-cui, NIU Xin-xin

Information Security Center, Beijing University of Posts and Telecommunications, Beijing 100876, China

Abstract

Manipulated digital image is got interesting in recent years. Digital images can be manipulated more easily with the aid of powerful image editing software. Forensic techniques for authenticating the integrity of digital images and exposing forgeries are urgently needed. A geometric-based forensic technique which exploits the principle of vanishing points is proposed. By means of edge detection and straight lines extraction, intersection points of the projected parallel lines are computed. The normalized mean value (NMV) and normalized standard deviation (NSD) of the distances between the intersection points are used as evidence for image forensics. The proposed method employs basic rules of linear perspective projection, and makes minimal assumption. The only requirement is that the parallel lines are contained in the image. Unlike other forensic techniques which are based on low-level statistics, this method is less sensitive to image operations that do not alter image content, such as image resampling, color manipulation, and lossy compression. This method is demonstrated with images from York Urban database. It shows that the proposed method has a definite advantage at separating authentic and forged images.

Keywords digital images, forgery detection, image forensics, vanishing points

1 Introduction

Forged images are appearing with growing frequency in tabloid magazines, main stream media outlets, scientific journals, evidence in courtrooms, and so on. With the aid of powerful image editing software such as Adobe Photoshop and some advanced digital cameras, forged images can be created easily by even relatively inexperienced users. Furthermore, the doctored photographs are being generated with growing sophistication. It is even difficult for experts to distinguish authentic images from forgeries relying solely on visual inspection. Therefore, forensic techniques for authenticating the integrity of digital images and exposing forgeries are urgently needed.

With advanced image editing software and proficient skills, forgeries may leave no obvious visual clues, and changes of the images may hardly be found by visual inspection. Nevertheless, some underlying statistical or

geometric changes, which are detectable, may be brought into the images. These detectable changes could be exploited by approaches of image forensics. In recent years, papers concerned on this subject [1], the digital image forensics has become a hot research field of image processing.

Digital image forensics is divided into five categories according to the information which is utilized for detecting forged images [1]. Pixel-level correlation is utilized in Refs. [2–3]. Properties of joint photographic experts group (JPEG) lossy compression were exploited in Refs. [4–5]. The methods proposed in Refs. [6–9] exploit artifacts introduced by camera lens, sensors or on-chip post-processing. Physical rules, such as lighting inconsistencies [10–11] can be used as the evidence of tampering of digital images. Geometric-based technique is also an important and efficient approach to authenticate the integrity of digital images [12–13].

Basic rules of reflective geometry and linear perspective projection were employed in Refs. [12–13]. In Ref. [13], vanishing points formed by the projected parallel lines are utilized. Recently, many articles [14–17] discussed how to

Received date: 27-12-2013

Corresponding author: LI Yan, E-mail: liyanphoto@gmail.com

DOI: 10.1016/S1005-8885(14)60320-4

compute vanishing points in images captured by pinhole camera. Some estimation methods were used to compute a single vanishing point from a set of projected parallel lines which may not intersect at a unique point precisely. The principle of vanishing points is also utilized here to authenticate the integrity of digital images. But no estimation methods are used, i.e., there is no need to compute a single vanishing point, it is just the distances between the intersection points of the projected parallel lines that are used as the evidence for digital image forensics. The concepts of NMV and NSD of the distances between intersection points are proposed for the image forensics. This technique requires no other assumptions, other than that parallel lines are contained in the image. No information of the internal parameters of the camera is required. Fig. 1 is an example of this kind of image. The parallel lines formed by the windows of the building can be utilized to authenticate the image, which will be illustrated in detail later. The underlying methodology is derived from basic rules of three-dimensional geometry and linear perspective projection. If this technique is added to the growing body of forensic analyses [1], creating undetectable forgery will become more difficult.



Fig. 1 Image containing parallel lines

The rest of this article is organized as follows. In Sect. 2, camera projection and vanishing point are introduced. In Sect. 3, the proposed method is described in detail, which containing four steps: edge detection, straight line extraction, computing intersection points, and image authentication. In Sect. 4, experimental results are presented to demonstrate the efficiency of the proposed method. Sect. 5 concludes this paper.

2 Vanishing point

As described in Ref. [18], the knowledge of camera projection and vanishing point will be reviewed in this section, which will be utilized in the proposed method to detect image manipulation.

In linear perspective projection, the image of an object that stretches off to infinity has finite extent. For example, the image of an infinite scene line is terminating in a vanishing point. The theory of vanishing point can be expressed both in geometric method and in algebraic method.

Geometrically, the vanishing point of the world line is obtained by intersecting the image plane with a ray through the camera center and parallel to the world line. It is the direction of the world line, but not its position, that determines its vanishing point, as illustrated in Fig. 2. Thus, if the world lines are in the same direction, or namely parallel lines, they will have a common vanishing point, as illustrated in Fig. 3. A cuboid, from perspective view, and two sets of parallel lines on it is shown in Fig. 3(a). The lines which are parallel to each other and converge to vanishing point v_1 are the diagonal lines of the cuboid. The lines which are parallel to each other and converge to vanishing point v_2 are the edge lines and mid-point connection lines of the top and bottom surface of the cuboid. Fig. 3(b) shows the cuboid and the parallel lines from the top view.

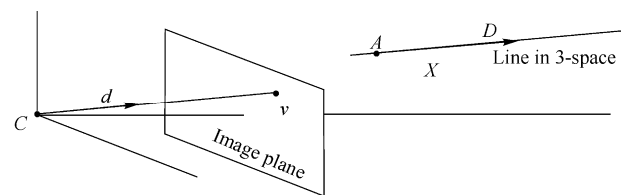
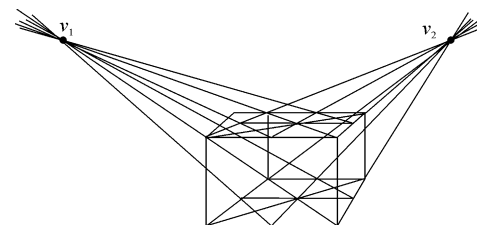
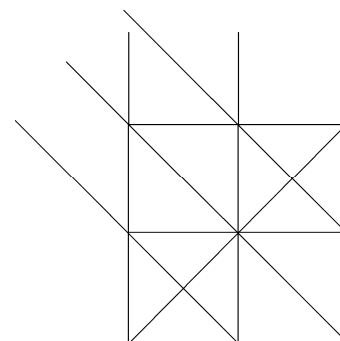


Fig. 2 Way to construct the vanishing point of a line



(a) From perspective view



(b) From the top view

Fig. 3 Vanishing points of two sets of parallel lines on the cuboid

Algebraically, the vanishing point can be obtained as follows. Points on a world line that has direction $\mathbf{D} = (\mathbf{d}^T, 0)^T$ goes through the point \mathbf{A} are written as $\mathbf{X}(\lambda) = \mathbf{A} + \lambda\mathbf{D}$. When λ equals to 0, the point $\mathbf{X}(\lambda)$ is the point \mathbf{A} . As λ varies to ∞ , the point $\mathbf{X}(\lambda)$ varies to infinity point \mathbf{D} . As illustrated in Fig. 2. Let $\mathbf{P} = \mathbf{K}[\mathbf{I} | \mathbf{0}]$ be the camera matrix representing a general projective camera. The general projective camera maps a point in world \mathbf{X} to a point in image \mathbf{x} according to the mapping $\mathbf{x} = \mathbf{P}\mathbf{X}$. So, under the projective camera \mathbf{P} , the point $\mathbf{X}(\lambda)$ is mapped to

$$\mathbf{x}(\lambda) = \mathbf{P}\mathbf{X}(\lambda) = \mathbf{P}\mathbf{A} + \lambda\mathbf{P}\mathbf{D} = \mathbf{a} + \lambda\mathbf{K}\mathbf{d} \quad (1)$$

where \mathbf{a} is the image of \mathbf{A} . As $\lambda \rightarrow \infty$, the vanishing point \mathbf{v} of the line is obtained

$$\mathbf{v} = \lim_{\lambda \rightarrow \infty} \mathbf{x}(\lambda) = \lim_{\lambda \rightarrow \infty} (\mathbf{a} + \lambda\mathbf{K}\mathbf{d}) = \mathbf{K}\mathbf{d} \quad (2)$$

where $\mathbf{v} = \mathbf{K}\mathbf{d}$ means that the vanishing point \mathbf{v} back-projects to a ray with direction \mathbf{d} . So, in the algebraic method, the same conclusion can be drawn as that in the geometric method: the vanishing point \mathbf{v} of a line depends only on the direction of the line, not on its position. In other words, all lines with the same direction intersect in the same vanishing point.

In practice, vanishing points can be computed as follows: by extending the image of a set of parallel lines, the intersection is just the vanishing point. Actually, with noise and error, the parallel lines may not intersect at a unique vanishing point, but at some scattered points distributed within a certain range.

3 Proposed method

The theory of vanishing points described in Sect. 2 can be used to detect geometric inconsistencies in forged digital images. Although very infrequent in natural scenes, parallel lines appear frequently in man-made environments. Together with the aid of human understanding of the image content, a set of lines that are parallel with each other will be picked up from the image. In the following pages, it will be shown how this method can be applied to digital image forensics.

There are four steps in the proposed method: edge detection, straight line extraction, computing intersection points, and image authentication.

3.1 Edge detection

Given an image to be verified, the first step is to detect

the edge of the image. The Canny edge detector [19] is used as it has excellent performance and has become the testing standard of edge detection algorithm.

Canny edge detector was developed by John F. Canny in 1986. It consists of four steps: smoothing the raw image with a Gaussian filter, applying directional Gaussian derivative filters, thus obtaining edge gradients and orientations, thinning the edge using non-max suppression and threshold with hysteresis.

3.2 Straight line extraction

After edge detection, a binary image with edge information is obtained, and then, straight lines will be extracted using Hough transform [20]. In image processing, Hough transform, which is widely used, is one of the basic methods to identify the geometric shapes. There are lots of improved algorithms in Hough transform, the most classical Hough transform is used to extract straight lines from binary images.

After the automatic straight line extraction by Hough transform, a set of projected parallel lines which are proper for vanishing point computation are selected. For example, if the line is too short, it is discarded. Or, if the angle between two lines is too small, one of them is discarded.

3.3 Computing intersection points

With the projected parallel lines extracted, the intersection points of these lines can be computed. As illustrated in Fig. 3, a set of parallel lines intersect at vanishing point \mathbf{v}_1 , and the other set of parallel lines which extend to a different direction intersect at vanishing point \mathbf{v}_2 . With the aid of human understanding, the parallel lines with the same direction can be selected.

Ideally, without any image noise and with perfect edge detection and straight line extraction, all parallel world lines with the same direction are imaged as lines which intersect at the same vanishing point. However, in the real situation, noise and distortion exist inevitably in images, so the results of edge detection and straight line extraction are affected more or less. Therefore, the extracted lines will generally not intersect at a unique point.

For this reason, some estimation methods, such as maximum likelihood estimate (MLE) [21–22], are widely used for vanishing point computation [14–17]. In MLE, lines are modified to pass a single point such that sum of

squared orthogonal distances from the endpoints of the measured lines to the modified lines is minimized. Not difficult to understand, MLE is an approximate algorithm, and the vanishing point computed by MLE is not exactly the intersection point of the parallel world lines, but with estimation error. It is the same case for other estimation methods [15–16].

The unique vanishing points need not to be computed in the proposed method, it is only needed to compute the intersection points of the extracted lines. It is just the distances between these intersection points that are used as evidence to authenticate the images. To preserve the evidence, and to avoid approximate error, no estimation method is used in this article. As illustrated in Fig. 4, the three bold lines are extracted from an image to be verified. In methods with estimation, the three bold lines will be modified to intersect at a single point, as illustrated with the fine solid lines. In the proposed method, the directions of lines are not modified, instead, the intersection points of the three bold lines are computed directly, as illustrated with the dotted lines. If there are two lines, there will be one intersection point; if there are three lines, there will be at most three intersection points. It can be deduced, if there are N_1 lines ($N_1 \geq 2$), then:

$$N_p = \frac{N_1(N_1 - 1)}{2} \quad (3)$$

where, N_1 is the number of lines, and N_p is the maximum number of intersection points computed from the N_1 lines. The distances between these intersection points will be utilized in the image authentication step described in the next section.



Fig. 4 Intersection points of lines

3.4 Image authentication

The estimation method is not used here to minimize any kind of error. It is just the distances between the intersection points of the projected parallel lines that are utilized to authenticate the images.

Firstly, the Euclidean distance between the intersection points is computed as follow:

$$D_{VP} = \sqrt{(x_1 - x_2)^2 + (y_1 - y_2)^2} \quad (4)$$

where, D_{VP} is the Euclidean distance between each pair of intersection points, x_1 and y_1 are the x -coordinate and y -coordinate of one intersection point in the pair, x_2 and y_2 are the coordinates of the other intersection point in the pair, respectively.

Then, to describe the distribution of these intersection points, the mean value and standard deviation of these distances are computed. The mean value of distance D_{mean} is computed as follow:

$$D_{mean} = \frac{1}{n} \sum_{i=1}^n D_{VP}^i \quad (5)$$

where n is the number of these distances, D_{VP}^i is the distance between the i th pair of intersection points. If the number of intersection points is m , then the number of distances between these intersection points will be $n = m(m-1)/2$.

The standard deviation of these distances D_{std} is computed as follow:

$$D_{std} = \sqrt{\frac{1}{n-1} \sum_{i=1}^n (D_{VP}^i - D_{mean})^2} \quad (6)$$

It is found that the values of D_{mean} and D_{std} are not only related to the distances between the intersection points D_{VP} , but also related to the distance between these intersection points and the image. So, the variable D_{CVP-PP} is defined as the distance between the center of the set of intersection points and the principle point of the image, which is assumed as the center of the image.

$$D_{CVP-PP} = \sqrt{(x_{CVP} - x_{PP})^2 + (y_{CVP} - y_{PP})^2} \quad (7)$$

$$x_{CVP} = \frac{1}{m} \sum_{i=1}^m x_{VP}^i \quad (8)$$

$$y_{CVP} = \frac{1}{m} \sum_{i=1}^m y_{VP}^i \quad (9)$$

where (x_{CVP}, y_{CVP}) is the coordinate of the center of the set of intersection points, and (x_{PP}, y_{PP}) is the coordinate of the principle point of the image. x_{VP}^i is the x -coordinate of i th intersection point, y_{VP}^i is the y -coordinate of the i th intersection point, and m is the number of intersection points.

The bigger the value of D_{CVP-PP} is, the bigger the value of the D_{mean} and D_{std} become. i.e., D_{mean} and D_{std} are both in direct proportion to D_{CVP-PP} , as the noise and

error are magnified by the bigger value of D_{CVP-PP} . For the consideration of a normalized D_{mean} and D_{std} , the NMV of the distance between intersection points and the NSD of the distance between intersection points are defined.

$$D_{nmv} = \frac{D_{mean}}{D_{CVP-PP}} \quad (10)$$

$$D_{nsd} = \frac{D_{std}}{D_{CVP-PP}} \quad (11)$$

where, D_{nmv} and D_{nsd} are the NMV and NSD of the distance between intersection points respectively. The value of D_{nmv} and D_{nsd} will be used for image authentication. It needs to be emphasized that both D_{nmv} and D_{nsd} are indispensable, lack of any one of the two will be impractical for image authentication.

In authentic images, the intersection points computed by a set of projected parallel lines should not be far away from each other. So, with the threshold T_{nmv} and T_{nsd} given, the Eq. (12) and (13) should both be satisfied.

$$D_{nmv} \leq T_{nmv} \quad (12)$$

$$D_{nsd} \leq T_{nsd} \quad (13)$$

where T_{nmv} is the threshold set for D_{nmv} , and T_{nsd} is the threshold set for D_{nsd} .

In forged images, Eq. (12) or (13), or neither of the two may not be satisfied. Obviously, if $D_{nmv} > T_{nmv}$ and $D_{nsd} > T_{nsd}$, it is a forged image. If $D_{nmv} \leq T_{nmv}$ and $D_{nsd} > T_{nsd}$, it is the case that most of the intersection points computed converge well, but a few intersection points are far from the converging group. If $D_{nmv} > T_{nmv}$ and $D_{nsd} \leq T_{nsd}$, it is the case that all of the intersection points computed do not converge well, but the distance from each other is almost equal.

4 Experiments

In order to verify the effectiveness of the method proposed in the paper, the algorithm is implemented in MATLAB R2012 with the York Urban database [23]. This database is a compilation of 102 indoor and outdoor images of urban environments on the campus of York University and in downtown Toronto, Canada. The images are 640×480 in size and have been taken with a Panasonic Lumix DMC-LC80 digital camera. The 102 images in the York Urban database are all authentic ones. To get forged images, the authentic images are spliced to

create the forgeries.

The authentic and forged images are being tested. True positive rate (TPR) and false positive rate (FPR) are calculated with the threshold of D_{nmv} and D_{nsd} set to different values, as illustrated in Table 1. Where, TPR represents the fraction of forged images that are correctly classified by the algorithm, and FPR represents the fraction of authentic images that are incorrectly classified as forgeries. As shown in Table 1, with the decrease of T_{nmv} and T_{nsd} , more forged images are identified to be forgeries, so the value of TPR increases. On the other hand, more authentic images are also identified to be forgeries, so the value of FPR also increases. To get the TPR of 100%, the threshold of D_{nmv} is set to $T_{nmv} = 0.0701$, and the threshold of D_{nsd} is set to $T_{nsd} = 0.0496$, corresponding to the FPR of 1.7241%, as shown in the fourth row of Table 1.

Table 1 TPR and FPR calculated by different thresholds

TPR/%	FPR/%	T_{nmv}	T_{nsd}
90.4412	0.0000	0.1269	0.1169
93.3824	0.5747	0.1080	0.0842
95.5882	0.5747	0.1051	0.0718
97.0588	1.1494	0.0915	0.0626
98.5294	1.7241	0.0783	0.0526
100.0000	1.7241	0.0701	0.0496
100.0000	2.8736	0.0680	0.0418

Next, some images will be selected to show the experiment steps and efficiency of the proposed method. The authentic images are selected from York Urban database, and the forged images are created by splicing the authentic images.

4.1 Authentic images

Four images from the database are selected, as illustrated in Fig 5. The names of the four images in database are P1020833, P1020867, P1080106 and P1080100, respectively.



(a) P1020833



(b) P1020867



(c) P1080106



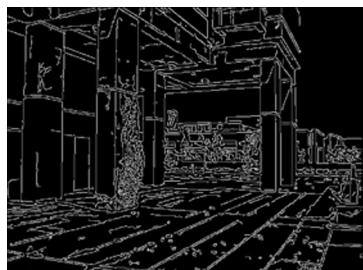
(d) P1080100

Fig. 5 Authentic images

The images after edge detection are illustrated in Fig 6.



(a) P1020833



(b) P1020867



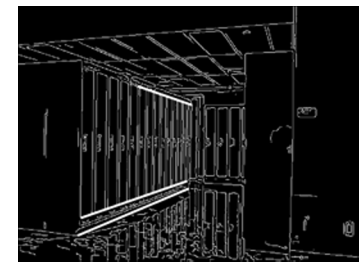
(c) P1080106



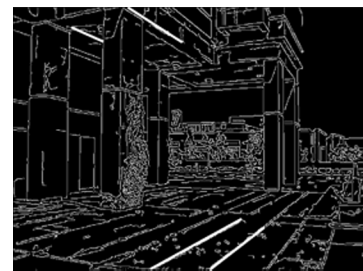
(d) P1080100

Fig. 6 Authentic images after edge detection

The images after straight line extraction are illustrated in Fig. 7.



(a) P1020833



(b) P1020867



(c) P1080106



(d) P1080100

Fig. 7 Authentic images after straight line extraction

The intersection points are computed from the selected lines, as illustrated in Fig. 8. The D_{nmv} and D_{nsd} of the intersection points in the four images calculated by Eqs. (10) and (11) are illustrated in Table 2. Compared with the threshold $T_{nmv} = 0.0701$ and $T_{nsd} = 0.0496$, it is clear that the four images are all authentic ones.



(a) P1020833



(b) P1020867



(c) P1080106



(d) P1080100

Fig. 8 Intersection points of authentic images

Table 2 D_{nmv} and D_{nsd} of authentic images

	D_{nmv}	D_{nsd}
Fig. 8(a)	0.0373	0.0276
Fig. 8(b)	0.0094	0.0070
Fig. 8(c)	0.0246	0.0183
Fig. 8(d)	0.0217	0.0162

4.2 Forged images

In this section, two forgeries are selected from the spliced images which are created, as illustrated in Fig. 9. The faked area is highlighted with the circles. Where, the cabinet in Fig. 5(a) was copied and pasted into Fig. 5(b) to create Fig. 9(a), and the gray building in Fig. 5(c) was copied and pasted into Fig. 5(d) to create Fig. 9(b). It is difficult for most viewers to determine that the two images have been manipulated. However, the proposed method could expose the forgeries easily, which will be shown in the following.



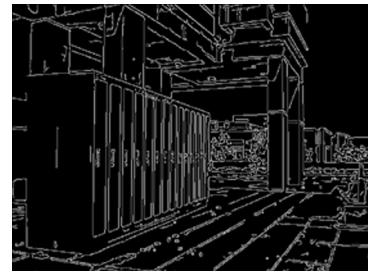
(a) Spliced by P1020833 and P1020867



(b) Spliced by P1080106 and P1080100

Fig. 9 Two spliced images

The spliced images after edge detection are illustrated in Fig. 10.



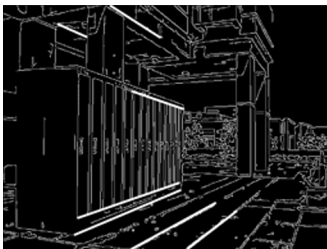
(a) Spliced by P1020833 and P1020867



(b) Spliced by P1080106 and P1080100

Fig. 10 Spliced images after edge detection

The spliced images after straight line extraction are illustrated in Fig. 11.



(a) Spliced by P1020833 and P1020867



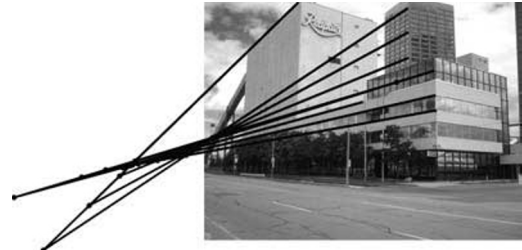
(b) Spliced by P1080106 and P1080100

Fig. 11 Spliced images after straight line extraction

The intersection points are computed from the selected lines, as illustrated in Fig. 12. The D_{nmv} and D_{nsd} of the intersection points in the two spliced images calculated by Eqs. (10) and (11) are illustrated in Table 3. Compared with the threshold, the value in the table are much greater than $T_{nmv} = 0.0701$ and $T_{nsd} = 0.0496$. It shows that the two images are forgeries.



(a) Spliced by P1020833 and P1020867



(b) Spliced by P1080106 and P1080100

Fig. 12 Intersection points of spliced images

Table 3 D_{nmv} and D_{nsd} of spliced images

	D_{nmv}	D_{nsd}
Fig. 12(a)	0.3194	0.2848
Fig. 12(b)	0.2270	0.1807

4.3 Algorithm comparison

The receiver operating characteristic (ROC) curve of the proposed method is illustrated in Fig. 13 in bold line. The x -coordinate of ROC curve is TPR, and the y -coordinate of ROC curve is FPR. ROC quantifies the algorithms discriminatory ability. It can be seen from the ROC curve that the proposed method can get a very high TPR with very low FPR. When the threshold of D_{nmv} is set to $T_{nmv} = 0.0701$, and the threshold of D_{nsd} is set to $T_{nsd} = 0.0496$, the TPR will reach 100% and the FPR of 1.7241%.

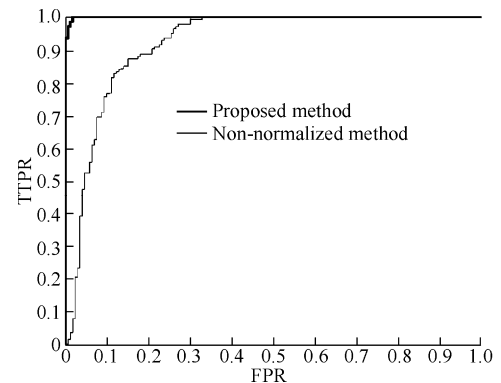


Fig. 13 ROC curve of the proposed method and non-normalized method

As D_{nmv} and D_{nsd} are the normalized value of D_{mean} and D_{std} respectively, the method in which the value of D_{mean} and D_{std} are used for image authentication will be called non-normalized method for short. For comparison, the ROC curve of the experiment results of the non-normalized method is plotted with fine line in Fig. 13. Intuitively, the fine line is not as much closed to the left and top edges of the bold line. It shows that under the

equal TPR, the FPR of the non-normalized method is much higher than the proposed method. In order to get the balance, in the non-normalized method the TPR of 93.382 4% is with the FPR of 16.092%. It shows the advantage of the proposed method.

5 Conclusions

In this article, the techniques for exposing forged images are studied. A geometric-based approach for image forensics is proposed. The principle of vanishing points formed by the linear perspective projection is leveraged for the purpose of forged image detection. By means of edge detection and straight lines extraction, intersection points of the projected parallel lines are computed. The distances between the intersection points are used as the evidence for image authentication. In order to preserve the evidence, any estimation approach is not used in the proposed method. As it is not the single vanishing point but the NMV and NSD of the distances between intersection points that are used as evidence. Compared with the non-normalized mean value and standard deviation, the proposed NMV and NSD method is of definite advantages at separating authentic and forged images. The proposed method requires some human understanding in selecting parallel lines contained in the image. To compute the intersection points of a set of parallel lines, the parallel lines with the same direction should be selected. For the images containing more than one vanishing point, the parallel lines with the same direction should be selected at one time, and parallel lines with another direction should be selected the next time.

Two experiments show that with human visual system it is almost impossible to detect planar perspective distortions raised from photo composition. Meanwhile, the proposed method shows that it can be applied to detect inconsistent intersection points. The critical step of this technique is straight line extraction. Success of this step can lead to precise intersection point computation, which can then present evidence to authenticate the images.

Like other geometric-based forensic techniques, it is less sensitive to image operations that do not alter image content, such as image resampling, color manipulation, and lossy compression.

The proposed method makes minimal assumption, and the only requirement is that parallel lines are contained in the image. Although somewhat narrowly applicable,

man-made environments often contain plenty of parallel lines such as buildings, roads, railways, stairs, windows, and so on. By adding this forensic technique to the growing body of forensic analyses, it will be increasingly difficult to create undetectable forgery.

As with any forensic technique, an informed forger could attempt to circumvent the forensic analysis. However, based on the experiments, even with the aid of Adobe Photoshop, a powerful and professional image editing software, it is still hard to do the image composition with strict consistence of perspective geometry. It suggests that an image which looks plausible is not always authentic.

The potential area of future research is to develop similar methods which can be applied to images containing curved lines. This is for the consideration that straight lines may not be contained in the image.

Acknowledgements

This work was supported by the General Administration of Press and Publication of the People's Republic of China (GXTC-CZ-1015004/15-1).

References

1. FARID H. Image forgery detection -- A survey. *Signal Processing Magazine, IEEE*, 2009, 26(2): 16–25
2. POPESCU A C, FARID H. Exposing digital forgeries by detecting duplicated image regions. *Dept Comput Sci, Dartmouth College, Tech Rep TR2004-515*, 2004, 11p
3. POPESCU A C, FARID H. Exposing digital forgeries by detecting traces of resampling. *Signal Processing, IEEE Transactions on*, 2005, 53(2): 758–767
4. LUK Š J, FRIDRICH J. Estimation of primary quantization matrix in double compressed JPEG images. *proceedings of the Proc Digital Forensic Research Workshop, F*, 2003, 17p
5. PEVNY T, FRIDRICH J. Detection of double-compression in JPEG images for applications in steganography. *Information Forensics and Security, IEEE Transactions on*, 2008, 3(2): 247–258
6. GLOE T, BOROWKA K, WINKLER A. Efficient estimation and large-scale evaluation of lateral chromatic aberration for digital image forensics. *proceedings of the IS&T/SPIE Electronic Imaging, International Society for Optics and Photonics*, 2010: 754107/1-13
7. KIRCHNER M. Efficient estimation of CFA pattern configuration in digital camera images. *proceedings of the IS&T/SPIE Electronic Imaging, International Society for Optics and Photonics*, 2010: 754111/1-12
8. HSU Y-F, CHANG S-F. Image splicing detection using camera response function consistency and automatic segmentation. *proceedings of the Multimedia and Expo, IEEE International Conference on*, 2007: 28–31

- the 32nd Chinese Control Conference (CCC'13), Jul 26–28, 2013, Xi'an, China. Piscataway, NJ, USA: IEEE, 2013: 208–212
26. Xu X R, Zhang Y Q, Hong Y G. Matrix approach to stabilizability of deterministic finite automata. Proceedings of the American Control Conference (ACC'13), Jun 17–19, 2013, Washington, DC, USA. Piscataway, NJ, USA: IEEE, 2013: 3242–3247
 27. Xu X R, Hong Y G. Observability analysis and observer design for finite automata via matrix approach. IET Control Theory & Applications, 2013, 7(12): 1609–1615
 28. Xu X R, Hong Y G. Matrix expression and reachability analysis of finite automata. Journal of Control Theory and Applications, 2012, 10(2): 210–215
 29. Zhang G. Automata, Boolean matrices, and ultimate periodicity. Information and Computation, 1999, 152(1): 138–154
 30. Dogruel M, Ozguner U. Controllability, reachability, stabilizability and state reduction in automata. Proceedings of the 1992 IEEE International Symposium on Intelligent Control (ISIC'92), Aug 11–13, 1992, Glasgow, UK. Piscataway, NJ, USA: IEEE, 1992: 192–197
 31. Seshu S, Miller R, Metzger G. Transition matrices of sequential machines. IRE Transactions on Circuit Theory, 1959, 6(1): 5–12
 32. Zhang Y Q, Xu X R, Hong Y G. Bi-decomposition analysis and algorithm of automata based on semi-tensor product. Proceedings of the 31st Chinese Control Conference (CCC'12), Jul 25–27, 2012, Hefei, China. Piscataway, NJ, USA: IEEE, 2012: 2151–2156

(Editor: ADA Lai Ti)

From p. 91

9. LI C T. Source camera identification using enhanced sensor pattern noise. Information Forensics and Security, IEEE Transactions on, 2010, 5(2): 280–287
10. JOHNSON M K, FARID H. Exposing digital forgeries in complex lighting environments. IEEE Transactions on Information Forensics and Security, 2007, 2(3): 450–461
11. KEE E, FARID H. Exposing digital forgeries from 3-D lighting environments. proceedings of the Information Forensics and Security (WIFS), IEEE International Workshop on, 2010: 1–6
12. FARID H, BRAVO M. Image forensic analyses that elude the human visual system. proceedings of the SPIE Symposium on Electronic Imaging, F, 2010: 754106-754106-10
13. O'BRIEN J F, FARID H. Exposing Photo Manipulation with Inconsistent Reflections. ACM Trans Graph, 2012, 31(1): 1–11
14. MENG X Z, NIU S Z, YAN R, et al. Detecting photographic cropping based on vanishing points. Chinese Journal of Electronics, 2013, 22(2): 369–372
15. XU Y, OH S, HOOGS A. A minimum error vanishing point detection approach for uncalibrated monocular images of man-made environments. proceedings of the Computer Vision and Pattern Recognition (CVPR), IEEE Conference on, 2013: 23–28
16. BAZIN J C, YONGDUEK S, DEMONCEAUX C, et al. Globally optimal line clustering and vanishing point estimation in Manhattan world. proceedings of the Computer Vision and Pattern Recognition (CVPR), IEEE Conference on, 2012: 16–21
17. YAO H, WANG S Z, ZHAO Y, et al. Detecting image forgery using perspective constraints. Signal Processing Letters, IEEE, 2012, 19(3): 123–126
18. HARTLEY R, ZISSERMAN A. Multiple view geometry in computer vision. Cambridge Univ Press, 2004
19. CANNY J. A computational approach to edge detection. Pattern Analysis and Machine Intelligence, IEEE Transactions on, 1986, (6): 679–698
20. BALLARD D H. Generalizing the Hough transform to detect arbitrary shapes. Pattern Recognition, 1981, 13(2): 111–122
21. LIEBOWITZ D, ZISSERMAN A. Metric rectification for perspective images of planes. proceedings of the Computer Vision and Pattern Recognition, 1998 Proceedings, IEEE Computer Society Conference on, 1998: 482–488
22. GAVIN H. The Levenberg-Marquardt method for nonlinear least squares curve-fitting problems. Environmental Engineering, 2010: 1–15
23. DENIS P, ELDER J H, ESTRADA F J. Efficient edge-based methods for estimating manhattan frames in urban imagery. Berlin Heidelberg: Springer, 2008: 197–210

(Editor: ADA Lai Ti)