Journal of Mathematics and Informatics
Vol. 1, 2013-14, 94-99
ISSN: 2349-0632 (P), 2349-0640 (online)
Published 1 October 2014
www.researchmathsci.org

Journal of
Mathematics and
Informatics

A Mathematical Approach to Detect Tampered Images

Xiao-qiang Zhou[1] **,** ***Hai-yan Zeng***[1] **and** ***Man-jia Hu***[1]

[1]College of Mathematics, Hunan Institute of Science and Technology, Yueyang, 414006, P.R.China, E.mail: zxq0923@163.com

Received 21 June 2014; accepted 16 July 2014

Abstract. Detecting tampered image is a challenging work due to the high volume of image database and the accurate definition of tampering. We propose a novel algorithm based on standard deviation which could detect the tampered automatically, furthermore, localization and extraction process is conducted to optimize the proposed method. Color reduction technique , intensity based method for edge detection and horizontal based localization approach are applied here to fulfill the algorithm. The core idea of the paper is that normally tampered regions process high standard deviation while compared with non-tampered areas. As the result, the output of our algorithm are tampered regions. By presenting promising experience, the performance of proposed method is analyzed. Further application and possible optimization are discussed.

Keywords**:** Mathematical Model, Machine Learning, Tampered Images, Deviation

1. Introduction

Despite the availability of extremely powerful technologies in both generating and processing digital images, there is a severe lack of techniques and methodologies for validating the authenticity of digital images. Due to this asymmetry, digital images appear to be the source of a new set of legal disputes and problems rather than being a solution. Furthermore, combined with the ease with which image processing tools can be obtained and used to modify images in indistinguishable ways, verifying the integrity of digital images proves to be a challenging task. This in turn undermines the credibility of digital images presented as news items, as evidence in a court of law, as part of a medical record or as financial documents since it may no longer be possible to distinguish whether an introduced image can be considered as the original, or a (maliciously) modified version. Recognizing the complexity of the problem, various digital watermarking techniques have been proposed as a means for authenticating images that are most likely to undergo various types of processing. In this approach to problem, a fragile watermark is embedded into the original image to create a marked image which is later extracted to determine if marked images has been tampered and to give the localization information as to which part of the image has been tampered, e.g., [1][2][3].

While this approach enables detector to establish the degree of authenticity and integrity of a digital object, it practically requires that the watermark was embedded during the creation of the digital object. This limits watermarking to applications where the digital object generation mechanisms have built-in watermarking capabilities, and therefore it cannot be offered as a general solution to the problem of authentication. Consequently, alternative approaches, that do not require much prior knowledge or

processing of the original image, needed to be considered. Another approach to verify integrity of digital images is inspired from the use of cryptographic hash functions for data authentication. The crux of this class of techniques is in the design of a, so called, robust perceptual hash function. Since digital media content might have many different digital representations, robust hash functions are designed to produce the same hash value as long as the input has not been perceptually modified. Mihcak and Venkatesan [4] proposed such function based on iterative geometric filtering. Another method is proposed by Fridrich [5] wherein a robust hash is generated by first dividing an image into blocks, projecting each block onto pseudo-randomly generated smooth basis functions and then appropriately quantizing the resulting values. In [6], Venkatesan et al. proposed another robust image hashing scheme based on random quantization of the statistics of wavelet coefficients. However, Coskun and Memon [7] showed that, these robust hash functions do not have satisfactory diffusion capabilities meaning that the hash value remains similar as the perceptual information is slowly changed. Another promising class of techniques that aim at detecting image tampering is based on the assumption that although image tampering might cause no visual artifacts or anomalies, it will nevertheless affect the underlying statistics of the image. Furthermore, one may safely assume that the process of image manipulation will very often involve a sequence of processing steps to avoid the appearance of illicit human intervention. Typically, a tampered image (or parts of it) would have undergone some common image processing operations, like scaling, rotation, brightness adjustment, compression, etc., to produce visually consistent images. To detect such anomalies, Bayram et al. [8] compiled more than 100 features that are sensitive to various common image processing operations and constructed classifiers to detect images that have undergone such processing. Similarly, Ng and Chang examined bicoherence characteristics of images to detect photomontages. Fridrich et al. in [9], based on correlation procedures, proposed method for detecting forgeries created by copying and pasting parts of an image over other parts. Based on the observation that image resizing operation introduced pixel-wise correlations in an image Popescu et al. [10] proposed a procedure to detect image resizing. Later, Johnson et al. [11] proposed a method based on inspecting inconsistencies in lighting conditions and Assuming the camera (or a number of images taken by the camera) is available, Lukas et al. in [12] proposed a technique to detect and localize tampering by analyzing the inconsistencies in the sensor pattern noise extracted from an image. Along the same direction, Swaminathan et al.[13] used inconsistencies in color filter array interpolation to detect tampered parts of an image. The above results show that none of the above techniques can offer a definitive solution by themselves.

2. Our proposed method

In our proposed algorithm, a robust and efficient system is developed to detect tampered images automatically. Edge detection with standard deviation performs well to detect edges in all directions. The flow of our methodology could be separated into three steps: Image pre-processing, edge detection and tampering localization.

2.1 Image pre-processing

In this step, we pay special on image de-noising and transformation. It is admitted that there exists a great deal of noise leading factors while getting an image, therefore, image

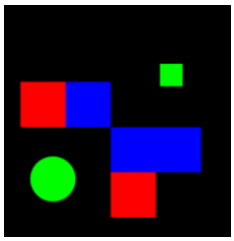
de-noising is eagerly needed. Dai Li[14] et al proposed a adaptive CBM3D algorithm for de-noising, which is one of the state-of-art algorithms. If the image data is not represented in YUV color space, it is converted to this color space by means of appropriate transformations. Our method only uses the intensity data (V channel of YUV) during further processing. Here V channel represents the intensity of image. Literatures indicated that V channel performs well when analyzing watermarking issues. The figure 1. And figure 2. well present the two presentation method, respectively.

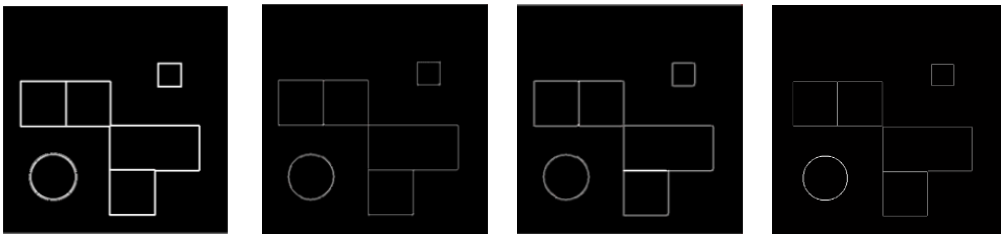
Figure 1. Tampered Image

Figure 2. V Channel

2.2 Edge detection algorithm selection

There are some well-performed edge detection algorithms such as Canny, Boolean, and Color Canny. In the order to select the best approach, we conduct a survey at the following figures and make our decision later according to the overall performance.





Marr.Hilddreth Canny Color Canny Boolean

Conclusion could be made from the above experimental result that Canny edge detector gains better performance. Moreover, in Figure 3. we use the Canny to our scene with good result.

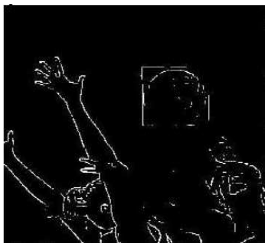


Figure 3. Edge Image

2.3 Localization of tampered region

There are a great deal of localization method such as SURF[15], SIFT[16], etc. In our proposed methodology Horizontal and Vertical projections are calculated and with the help of horizontal and vertical thresholds other directional edges are removed. Horizontal and Vertical edges images are combined together and feature map is generated.

$$H.Threshold = Mean(Horizontal) \tag{1}$$

$$V.Threshold = Mean(Vertical) \tag{2}$$

Figure 4. Horizonal

Figure 5. Vertical

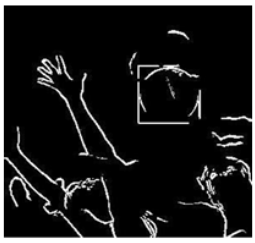


Figure 6. Combined

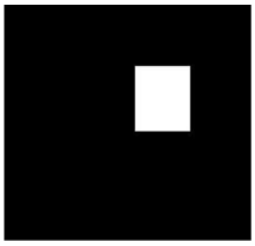


Figure 7. Feature Map

To gain a better visibility, we propose a mark method to observe the tampered region saliently. In the marked map, tampered is set the red color, literatures has shown that red color may catch people' intention most compared with other colors.

3. The experiment

The proposed approach has been evaluated using datasets containing different types of tampered images. The whole test data consists of 50 images. The precision and recall rates (Equations (3) and (4)), have been computed based on the number of correctly

detected tampered parts in an image in order to further evaluated the efficiency and robustness.The precision rate is defined as the ration of correctly detected parts to the sum of correctly detected parts plus false positive. False positive are those regions in the image, which are actually not tampered parts, but have detected by the algorithm as tampered parts.

$$\text{Precision Rate} = \frac{\text{Correctly Detected Parts}}{\text{Correctly} + \text{False Positive Parts}} \times 100\% \quad (3)$$

The Recall rate is defined as the ratio of correctly detected parts to the sum of correctly detected parts plus false negatives. False negatives are those regions in the image, which are actually tampered parts, but have been not detected by the algorithm.

$$\text{Recall Rate} = \frac{\text{Correctly Detected Parts}}{\text{Correctly} + \text{False Negative Parts}} \times 100\% \quad (4)$$

Figure 8. Test Image

Figure 9. Tampered Image

Figure 10. Feature Map

Figure 11. Marked Image

Table 1: Results on Tampered images

Test Data	**No of Images**	**Precision Rate**	**Recall Rate**
Using Paint	50	92.2	90.6
Using Photo Shop	50	45.4	35.7
Total	Total	68.8	63.2

4. Conclusion

In this paper, simple standard deviation based Tampering Detection is proposed. Preliminary results show that when the devised method is applied to different tampered mages, it can successfully estimate the degree of blur ness and detected the tampered regions effectively.

REFERENCES

1. Fridrich J., Image watermarking for tamper detection, Proc. ICIP, *International Conference on Image Processing*, 2 (1998) 404–408.

2. Huang J., Hu J., Huang D., and Shi Y.Q., Improve security of fragile watermarking via parameterized wavelet, Proc. ICIP, *International Conference on Image Processing*, 2 (2004) 721– 724.
3. Watanabe J., Hasegawa M., and Kato S., A study on a watermarking method for both copyright protection and tamper detection, Proc.ICIP, *International Conference on Image Processing,* 4 (2004) 2155–2158.
4. Mihcak M.K. and Venkatesan R., New iterative geometric methods for robust perceptual image hashing, Proc. of the *Digital Rights Management Workshop*, November 2001.
5. Fridrich J., Robust bit extraction from images, ICMCS 99, Florence, Italy, June 1999.
6. Venkatesan R., Koon S., Jakubowski M., and Moulin P., Robust image hashing, Proc. *IEEE Int. Conf. on Image Processing*, 2000.
7. Coskun B. and Memon N., Confusion/diffusion capabilities of some robust hash functions, Proc. *CISS, Conf. on Information Sciences and Systems*, March 2006.
8. B. Sankur S. Bayram, I. Avcibas and N. Memon, Image manipulation detection, *Journal of Electronic Imaging*, 15(4) (2006).
9. J. Fridrich, D. Soukal, and J. Luk, Detection of copy-move forgery in digital images, Proc. *Digital Forensic Research Workshop, Cleveland, OH*, August 2003.
10. A.C. Popescu and H. Farid, Exposing digital forgeries by detecting traces of resampling, *IEEE Transactions on Signal Processing*, 53(2) (2005) 758–767.
11. M.K. Johnson and H. Farid, Exposing digital forgeries by detecting inconsistencies in lighting, Proc. *ACM Multimedia and SecurityWorkshop*, New York, pp. 1–9, 2005.
12. Luk J., Fridrich J., and Goljan M., Detecting digital image forgeries using sensor pattern noise, Proc. of *SPIE Electronic Imaging, Photonics West*, January 2006.
13. M. Wu A. Swaminathan and K. J. Ray Liu, Image tampering identification using blind deconvolution, Proc. *IEEE ICIP*, 2006.
14. Dai, L., Zhang, Y., Li, Y., and Wang, H. (2014, April). MMW and THz images denoising based on adaptive CBM3D. In *Sixth International Conference on Digital Image Processing* (pp. 915906-915906). International Society for Optics and Photonics.
15. Fan, Youchen, Huayan Sun, and Haoxiang Wang. Application in casting defect lossless examination based on surf. 2013-*Fifth International Symposium on Photoelectronic Detection and Imaging. International Society for Optics and Photonics*, 2013.
16. Ng, P. C., and Henikoff, S., SIFT: Predicting amino acid changes that affect protein function. *Nucleic Acids Research*, 31(13) (2003) 3812-3814.