MedCrave
Step into the World of Research
Forensic Research & Criminology International Journal

Mini Review

Open Access

CrossMark

Digital image forensic: a brief review

Abstract

"A picture is worth a thousand words" ancient idiom is more relevant in this era. Digital images are most popular representation of information sharing. This popularity creates an opportunity for the researchers to ensure trustworthiness of images. The forensic analysis of an image is performed using various techniques to ensure its credibility. Several anti-forensic techniques have also been evolved to hide the traces of forgery. This is like virus and antivirus battle.

Volume 5 Issue 4 - 2017

Saurabh Agarwal,[1] Satish Chand[2]
[1]Shri Ram MurtiSmarak College of Engineering & Technology, India
[2]Deptartment of Computer Engineering, Jawaharlal Nehru University, India

Correspondence: Satish Chand, Department of Computer Engineering, Netaji Subhas Institute of Technology, New Delhi, India, Email schand20@gmail.com

Received: July 29, 2017 | **Published:** September 27, 2017

Mini review

In this era of digitalization, everyone is surrounded by digital contents like digital image, digital video through their electronic gadgets. Latest technologies have reduced the cost of camera radically that promote camera-enabled devices like mobile phones, tablets, laptops, etc. People are uploading approximately 24300 images per minute. In most of the cases, these contents are making life easy in some sense. This digital era is also providing high quality image editing applications/softwares that can make changes in images and videos easily. The motivation of these changes may possibly be used to create some rumor, which can influence political, corporate, legal, and personal issues. This demands forensic analysis of images to prove their originality. Previously, when the source is confirmed, the image integrity can be authenticated using digital signature or digital watermark and it is generally called active forensic analysis. Most of the time, the source of an image is unknown, i.e., only the image itself is available to analyze. This type of forensic analysis is called blind or passive. In current scenario, the techniques based on passive forensic analysis are more relevant. In this review article, we emphasis on passive forensic analysis techniques[1–11] and their challenges.

Generally, two types of fake images are created, i.e., using splicing and copy move. In splicing, two or more different images are used to create a fake image and in copy move, some image content of same image is used to create a fake image. While creating realistic looking fake images, various operations are performed like resampling, contrast enhancement, median filtering, etc. Forensic analysis of these operations also helps detecting forgery. In spite of that, various anti-forensics techniques[12–15] have been developed to hide the artifacts of forgery. Image forgery can be detected using various phenomena. The authors in[1,2] have used lighting effects to find the traces of forgery. In[1] the optimized 3-D lighting estimation based on surface reflection model has been discussed to detect splicing of human faces.

The texture operator is the popular choice for detecting forgery.[3]As forged image is created, the internal statistics of the image get disturbed due to boundary modification or different operations. The high discriminative capability of texture operators helps revealing internal statistical properties of the images. Color/illumination map based techniques assume that the external objects illumination is different from the pristine image objects in a fake image. The technique[4] is a hybrid form of illumination map and texture operator. Some techniques exploit hardware limitations like chromatic aberration, CFA artifact, sensor noise, etc to detect forgery. The chromatic aberration is the malfunction to focus light of different wavelengths perfectly of an optical system. This irregularity helps the forensic analysis[16] of images. To reduce cost using single sensor and Color Filter Array (CFA) three basic colors: red, green and blue, are generated. Every model of camera has special CFA pattern and interpolation method, these uniqueness help image forensic analysis.[5,6] Each image has some artifacts due to their capturing device, which is considered as hardware noise. The forged part in an image can be found by Photo-Response Non-Uniformity (PRNU) noise of the camera.[7–9]A variety of PRNU noise confirms image forgery. The JPEG is one of the popular encoding techniques to achieve desired quality in reduced storage need.

The camera manufacturers configure their devices in a way to balance quality and compression. The splicing of two different images generate anomaly in quality that help in forgery detection. Sometimes the image needs be saved two times to create forged image that creates double quantization artifact in the histogram of DCT coefficients and the block synchronization gets disturbed. These artifacts help detecting forgery easily.[10,11] As we have discussed above, various techniques are available for image forensic analysis. These techniques are somehow based on shortcomings of the forged image creation process. To hide the traces of forgery, some methods have been developed that are called anti-forensic methods.[12–15] These methods hide the traces by using noise insertion, resampling, median filtering, etc. on the forged images. To counter anti-forensics, various techniques[17–19]are also available in which the median filtering detection is difficult due to its nonlinear nature. The techniques[18,19] are based on Markov process provide good results. There is lot of challenges in forensic analysis of digital images. As we can see, there is continuous battle between forensic, anti-forensic and counter anti-forensic techniques. New techniques are evolving day-by-day to hide the artifacts of forgery. Latest technology based camera are also making forensic analysis difficult. In spite of that, the forged images are being created using automated content-aware, seam carving type techniques. The wide applications of digital images have compelled the research community to develop universal robust forensic techniques.

Acknowledgments

None.

Funding

None.

Conflicts of interest

Author declares that there is no conflict of interest.

References

1. Peng B, Wang W, Dong J, et al. Optimized 3D Lighting Environment Estimation for Image Forgery Detection. *IEEE Trans Inf Forensics Secur.* 2017;12:479−494.
2. Lv Y, Shen X, Chen H. An improved image blind identification based on inconsistency in light source direction. *J Supercomput.* 2011;58(1):50−67.
3. Saleh SQ, Hussain M, Muhammad G, et al. Evaluation of Image Forgery Detection Using Multi-scale Weber Local Descriptors. *International Symposium on Visual Computing.* 2013;416−424.
4. Carvalho T, Faria FA, Pedrini H, et al. Illuminant-based transformed spaces for image forensics. *IEEE Trans Inf Forensics Secur.* 2016;11(4):720−733.
5. Li L, Xue J, Wang X, et al. A robust approach to detect digital forgeries by exploring correlation patterns. *Pattern Anal Appl.* 2013;18(2):1−15.
6. Ferrara P, Bianchi T, De Rosa A, et al. Image forgery localization via fine-grained analysis of CFA artifacts. *IEEE Trans Inf Forensics Secur.* 2012;7(5):1566−1577.
7. Chierchia G, Cozzolino D, Poggi G, et al. Guided filtering for PRNU-based localization of small-size image forgeries. *ICASSP, IEEE Int Conf Acoust Speech Signal Process Proc.* 2014;6231−6235.
8. Gaborini L, Bestagini P, Milani S, et al. Multi-clue image tampering localization. *2014 IEEE Int Work Inf Forensics Secur WIFS.* 2015;125−130.
9. Chierchia G, Poggi G, Sansone C, et al. A bayesian-MRF approach for PRNU-based image forgery detection. *IEEE Trans Inf Forensics Secur.* 2014;9(4):554−567.
10. Yu L, Han Q, Niu X, et al. An improved parameter estimation scheme for image modification detection based on DCT coefficient analysis. *Forensic Sci Int.* 2016;259:200−209.
11. Bianchi T, Piva A. Analysis of non-aligned double JPEG artifacts for the localization of image forgeries. *IEEE Int Work Inf Forensics Secur WIFS.* 2011.
12. Kaimal AB, Manimurugan S, Anitha J. A modified anti-forensic technique for removing detectable traces from digital images. *Int Conf Comput Commun Informatics IEEE.* 2013;1−4.
13. Cao G, Zhao Y, Ni R, et al. Anti-Forensics of Contrast Enhancement in Digital Images. *ACM Multimed Secur Work.* 2010;25−34.
14. Fan W, Wang K, Cayre F, et al. JPEG anti-forensics with improved tradeoff between forensic undetectability and image quality. *IEEE Trans Inf Forensics Secur.* 2014;9(8):1211−1226.
15. Fan W, Wang K, Cayre F, et al. JPEG anti-forensics using non-parametric DCT quantization noise estimation and natural image statistics. *Proc first ACM Work Inf hiding Multimed Secur-IH&MMSec.* 2013;13:117−122.
16. Fang Z, Wang S, Zhang X. Image splicing detection using camera characteristic inconsistency. *Multimed Inf Netw Secur MINES.* 2009;1:20−24.
17. Jiang Y, Zeng H, Kang X, et al. The game of countering JPEG anti-forensics based on the noise level estimation. *2013 Asia-Pacific Signal Inf Process. Assoc Annu Summit Conf IEEE.* 2013. p. 1−9.
18. Kirchner M, Fridrich J. On detection of median filtering in digital images. USA: Media Forensics Secur II, 2010. p. 1−39.
19. Agarwal S, Chand S, Skarbnik N. SPAM revisited for median filtering detection using higher-order difference. *Secur Commun Networks.* 2016;9(17):4089−4102.