Abstract

Digital Photo images are everywhere around us in journals, on walls, and over the Internet. However we have to be conscious that seeing does not always imply reality. Photo images become a rich subject of manipulations due to the advanced digital cameras as well as photo editing software. Accordingly, image forgery is becoming much easier using the existing tools in terms of time and accuracy, and thus the forensics of detecting an image forgery case is becoming difficult and needs more and more time and techniques to prove the image originality especially as crime evidences and court related cases. In this paper, a framework with associated algorithms and methodologies is proposed to ensure the authenticity of the image and the integrity of the content in addition to protecting the photo image against forgery suspects. The framework depends on developing new generation of certified digital cameras that could produce authenticated and forgery-proof photos. The proposed methodology generates an irreversible hash integrity code from the image content based on color matrix calculations and steganography algorithms. The simulation results proved the capability of the proposed technique to detect image forgery cases in more than 16 scenarios of manipulation.
A Novel Watermarking Approach for Protecting Image Integrity based on a Hybrid Security Technique

References

1. A. Cheddad, J. Condell, K. Curran, and P. Mc Kevitt, “Digital image steganography: Survey and analysis of current methods,” Signal processing, vol. 90, no. 3, pp. 727–752, (2010).

2. H Farid, A survey of image forgery detection. IEEE Signal Process. Mag. 2(26), pp. 16–25, (2009).

3. B Mahdian, S Saic, A bibliography on blind methods for identifying image forgery. Signal Process. Image Commun. 25(6), pp. 389–399, (2010).

4. I. Cox, M. Miller, J. Bloom, J. Fridrich, and T. Kalker, Digital watermarking and steganography. Morgan Kaufmann, 2007.

5. JG Han, TH Park, YH Moon, IK Eom, Efficient Markov feature extraction method for image splicing detection using maximization and threshold expansion. J. Electron. Imaging. 25(2), pp. 23-31 (2016).

6. WC Hu, WH Chen, DY Huang, CY Yang, Effective image forgery detection of tampered foreground or background image based on image watermarking and alpha mattes. Multimed. Tools Appl. 75(6), pp. 3495–3516, (2017).

7. CH Choi, HY Lee, HK Lee, Estimation of color modification in digital images by CFA pattern changes. Forensic Sci. Int. 226, pp. 94 –105, (2013).

8. P Ferrara, T Bianchi, A De Rosa, A Piva, Image forgery localization via finegrained analysis of CFA artifacts. IEEE Trans. Inf. Forensics Secur. 7(5), pp. 1566– 1577, (2012).

9. Che-Yen, Wen, and Yang Kun-ta. "Image authentication for digital image evidence." Forensic Science Journal, 2006: 1-11.

10. Scientific Working Group on Imaging Technology (SWGIT) , Draft Recommendations and Guidelines for the Use of Digital Image Processing in the Criminal Justice System, Version 1.1 , February 2001.

11. J Luk’a’s, J Fridrich, M Goljan, Digital Camera Identification from Sensor Pattern Noise. IEEE. T. INF. Foren. Sec. 1(2), pp. 205- 214, (2006).

12. I Amerini, L Ballan, R Caldelli, A Del Bimbo, G Serra, ASIFT-based forensic method for copy move attack and transformation recovery. IEEE. Trans. Inf. Forensics Secur.6 (3), pp. 1099–1110, (2011).

13. S Bayram, HT Sencar, N Memon, Classification of digital camera-models based on demosaicing artifacts. Digit. Invest. 5, pp. 49 –59, (2008).

14. H Cao, AC Kot, Accurate detection of demosaicing regularity for digital image forensics. IEEE Trans. Inf. Forensics Secur. 4(4), pp. 899–910, (2009).

15. AC Gallagher, TH Chen, Image authentication by detecting traces of demosaicing. Proceedings of IEEE Computer Society Conference on Computer Vision and Pattern Recognition Workshops, pp. 1–8, (2008).

16. D. R. Stinson, Cryptography: theory and practice. CRC press, 2005.

17. D. B. A. M. D. E. I. M. Yousif Elfathiz Yousif, "Review on Comparative Study of Various Cryptography Algorithm," International Journal of Advanced Research in Computer Science and Software Engineering(IJARCSSE), vol. 5, no. 4, pp. 51-55, 2015.

18. Suresh Kumar, Ganesh Singh, Tarun Kumar(2013), “Hiding the Text Messages of Variable Size using Encryption and Decryption Algorithms in Image Steganography”, International Journal of Computer Applications (0975 – 8887) Volume 61– No.6, January 2013.

19. M.RAJKAMAL and B.S.E. ZORAIDA, (2014) “Image and Text Hiding using RSA &
Blowfish Algorithms with Hash-Lsb Technique”, International Journal of Innovative Science, Engineering & Technology, Vol. 1 Issue 6, August 2014.

20. G.R.Manjula and AjitDanti, (2015) “A NOVEL HASH BASED LEAST SIGNIFICANT BIT (2-3-3) IMAGE STEGANOGRAPHY IN SPATIAL DOMAIN”, International Journal of Security, Privacy and Trust Management, Vol 4, No 1, February 2015.

21. Z Lin, J He, X Tang, CK Tang, Fast, automatic and fine-grained tampered JPEG image detection via DCT coefficient analysis. Pattern Recognition 42(11), pp. 2492–2501, (2009)

Index Terms

Computer Science

Security

Keywords

Image Forgery Detection, Image Quality Assessment, Integrity Protection.