C28 Hands-On Digital Image Authentication Techniques

Oliver Giudice, PhD, Roma 00044, ITALY; Antonino Paratore, MS, ICTLab S.R.l. Spinoff of Università di Catania, Catania 95125, ITALY; Sebastiano Battiato, PhD*, Università di Catania, Catania 95125, ITALY; Luca Guarnera, MS, Università di Catania, Catania 95125, ITALY*

Learning Overview: After attending this presentation, attendees will be familiar with various techniques for image authentication based on double quantization detection analysis and first quantization step estimation of a digital image. Due to the widespread digital image forensics technique, this presentation will attempt to make a uniformness among all the existing solutions by presenting a simple but schematic view. All techniques will be presented organized in categories and the pros and cons exposed with regard to practical application scenarios.

Impact on the Forensic Science Community: This presentation will impact the forensic science community by raising awareness of a wide range of solutions and the forensics community will be able to select the most accurate technique for a specific investigation case.

The widespread diffusion of digital image technology over the past decades has increased the interest in image integrity verification, thus becoming one of the main goals in multimedia forensics. Understanding if a certain image was previously compressed, together with any information related to past processing, is an extremely powerful tool for forensic examinations. Some of the retrievable information, such as the first quantization step used by JPEG algorithms at image acquisition time, represents one of the fundamental parameters for both image tampering detection and source camera identification. In this presentation, after presenting the fundamentals of JPEG compression and the traces left on digital images, the most significant state-of-the-art techniques for integrity verification by making use of first quantization step estimation will be illustrated and critically compared.

Every day millions of people safely store and share many moments of their lives through social networks. All that data is digitally stored in multimedia content through their digital devices, such as mobile smart phones. Thus, forensic investigations can take advantage of that data through evidence collection of the images and videos and reconstruct a specific crime event. To check the originality of these digital clues, a new domain was recently created called image forensics, whose goal is to leverage the knowledge of image processing to answer questions that arise in an investigative scenario.[1,2]

In this complex environment, since JPEG has emerged as the most popular compression standard for digital images, data related to the image processing pipeline have been deeply analyzed by research communities in order to identify the traces left by the compression algorithm on an image.[3-5] To this end, one part of the algorithm most examined was the Discrete Cosine Transform (DCT), a mathematical tool applied on images to shift from spatial domain to a domain of frequency.

Throughout the years, research papers that provided an overview on state-of-the-art methods in image forensics did not perform an in-depth exploration of each aspect of DCT analysis, probably due to the difficulty of joining insights from several methods.[6-16] The purpose of this presentation is to fill this gap, which has never been covered as a stand-alone topic. The most important methods that try to model the behavior of DCT coefficients when a JPEG image is decompressed after the shoot, edited, and then compressed again, or stored in uncompressed format, will be described with pros, cons, and application scenarios.

Reference(s):

1. B. Zhu Bin, M.D. Swanson, and T.A.H. When Seeing Isn't Believing (Multimedia Authentication Technologies). *IEEE Signal Processing Magazine*, vol. 21, no. 2, pp. 40–49, 2004.
2. https://www.fbi.gov/about-us/lab/ forensic-science-communications/fsc/oct2005/standards/.
3. G.K. Wallace. The JPEG Still Picture Compression Standard. *Communications of the ACM*, vol. 34, no. 4, pp. 30–44, 1991.
4. *JPEG Survey*. http://w3techs.com/technologies/overview/ images format/all.
5. S. Battiato, A.R. Bruna, G. Messina, and G. Puglisi. Image Processing for Embedded Devices. *Applied Digital Imaging*, vol. 1, 2010.
6. N. Allan, L. Pan, and A. Xiang Y. Novel Method for Detecting Double Compressed Facebook JPEG Images. *Applications and Techniques in Information Security*, pp. 191–198, 2014.
7. E. Kee, M.K. Johnson, and F.H. Digital Image Authentication From JPEG Headers. *IEEE Transactions on Information Forensics and Security*, vol. 6, no. 3, pp. 1066–1075, 2011.
8. W. Luo, Z. Qu, F. Pan, and A. Huang J. Survey of Passive Technology for Digital Image Forensics. *Frontiers of Computer Science in China*, vol. 1, no. 2, pp. 166–179, 2007.
9. H. Farid. *Image Forgery Detection and IEEE Signal Processing Magazine*," vol. 2, pp. 16–25, 2009.
10. J.A. Redi, W. Taktak, and D.J.L.D. Image Forensics: A Booklet for Beginners. *Multimedia Tools and Applications*, vol. 51, no. 1, pp. 133–162, 2011.
11. A. Piva. An Overview on Image Forensics. *ISRN Signal Processing* 2013.
12. M.C. Stamm, M. Wu, and K.R. Liu. Information Forensics: An Overview of the First Decade. *IEEE Access*, vol. 1, pp. 167– 200, 2013.
13. G. Birajdar and M.V.H. Digital Image Forgery Detection Using Passive Techniques: A Survey. *Digital Investigation*, vol. 10, no. 3, pp. 226–245, 2013.
14. O.M. Al-Qershi and B.E. Khoo. Passive Detection of Copy-Move Forgery in Digital Images: State-of-the-Art. *Forensic Science International*, vol. 231, no. 1, pp. 284–295, 2013.
15. B. Mahdian and A. Saic S. Bibliography on Blind Methods for Identifying Image Forgery. *Signal Processing: Image Communication*, vol. 25, no. 6, pp. 389–399, 2010.
16. S. Battiato, O. Giudice, and A. Paratore. Multimedia Forensics: Discovering the History of Multimedia Contents. In: *Proceedings* of the 17th International Conference on Computer Systems and Technologies 2016. ACM, 2016, pp. 5–16.

Double Quantization, Multimedia Forensics, Image Authentication