Abstract

Over the past decade digital images has become a very popular way to communicate, store and process information. With the rapid advancement and easy availability of technology, there is a flood of devices that are able to capture, store and create digital images. Over the past years image processing techniques have been developed that makes it really easy to tamper images. From journalism to social media edited images are appearing everywhere with increasing frequency. Authentication of images is very necessary as visual data effects what people perceive and believe. Digital image Forensics is an emerging field that uses intrinsic and extrinsic methods to authenticate digital images. Passive techniques extract and analyze inherent patterns introduced by various image processing steps and use these artifacts to associate the image with source device as well as to detect tampering of the digital images. This paper gives an overview of passive techniques of Digital Image Forensics which are based on intrinsic fingerprints inherent in digital images.

References

- Alessandro Piva, “An Overview on Image Forensics”, ISRN Signal
A Comprehensive Study of Passive Digital Image Forensics Techniques based on Intrinsic Fingerprints

Processing Article ID 496701, 22 pages, Volume 2013
- Chih-Ming Kung, Shu-Tsung Chao, Yen-Chen Tu, Yu-Hua Yan and Chih-Hsien Kung, "A Robust Watermarking and Image Authentication Scheme used for Digital Content Application", JOURNAL OF MULTIMEDIA, VOL. 4, NO. 3, JUNE 2009.
- J Sravanthi, Dr. MHM Krishna Prasad, "Robust and secure Digital Signature for Image Authentication over Wireless Channels", International Journal of Computer Trends and Technology- July to Aug Issue 2011.
- J. Fridrich, "Digital image forensic using sensor noise", in IEEE Signal
A Comprehensive Study of Passive Digital Image Forensics Techniques based on Intrinsic Fingerprints


Index Terms

Computer Science

Security

Keywords
