International Journal of Scientific Engineering and Technology (ISSN : 2277-1581)
Volume No.3 Issue No.7, pp : 919-920 1 July 2014

Forensic Technique for Detecting Image Tampering using Statistical Intrinsic Fingerprints- A Survey

Dhanshri P. Patil
M.Tech CS Engineering,Astral Institute of Technology and Research, Indore
Email- dhanshreepatil31@gmail.com

Abstract- :The digital images are becoming important part in the field of information forensics and security, because of the popularity of image editing tools, digital images can be altered. Therefore it is must to create forensic techniques which is capable of detecting tampering in image. This paper reviews to the forensic methods for detecting contrast enhancement and copy- move forgery in image by identifying the features of each operation's intrinsic fingerprint.

Keywords-

Digital forensics, Cropping, Copy-move forgery, Contrast enhancement.

1. Introduction

As the use of digital images has become more common throughout society, to create digitally forged images has increased. Nowadays, image editing tools are very popular and easily available, that's why making forgeries in digital images is an easy task without leaving obvious evidence that can be recognized by human eyes [ii]. So the image authentication and reliability of images emerged as an important problem. There are two methods for digital image authentication, active and passive ones. The first area consists of image watermarking methods and second area consists of image forensic methods. The major drawback of watermark approach Is that watermarks need to be embedded in the image before distribution, in the market most cameras nowadays are not equipped with the function for embedding watermark. Image forensic is a passive method in which no information needs to be embedded for distribution.

Since the problem of image forensics is very broad, this survey focuses on forgery detection in digital images. There are three lead directions for image forensics research. The sources of images is identified by the first direction, the second direction attempts to classify computer generated images from natural images and third important direction tackles the problem of forgery detection for digital images. This paper gives a survey on the efficient and reliable techniques for detecting globally and locally applied contrast enhancement, cut-and-paste forgery, histogram equalization, noise and image scaling in the digital image.

2. Related work

Numbers of methods are available till date for detecting image tampering, each of which comes with advantages and disadvantages, but there is no universal technique that can detect each and every type of image forgery. Few of them is studied here:

Zhao Junhong targets copy-move forgery detection in digital image. This method uses a new approach based on one improved LLE, because a technique based on PCA to detect copy-move forgery can't detect the fused edge, that's why this paper present LLE method, which not only detect copy-move areas but also fused edges.

Matthew C.Stamm and K.J.Ray Liu [ii] targets number of techniques for identifying digital forgeries by detecting the unique statistical fingerprints that certain image altering operations leave behind in an images pixel value histogram. This work also deals with the methods to detect globally and locally applied contrast enhancement and also to detect noise in previously JPEG compressed image.

Abhitha. E and V.J.Arul Karthick [ix] proposed forensic techniques in SPHIT image compression, since most of the image manipulations occurs at the time of compression and image manipulations means changing any of the DCT and DWT coefficients.

3. Methodology

3.1 Detecting globally applied contrast enhancement in image:

Contrast enhancement operations are viewed as non linear pixel mapping which introduce artifacts into an image histogram. Non linear mappings are separated into regions where the mapping is locally contractive. The contract mapping maps multiple unique input pixel values to the same output pixel value. Result in the addition of sudden peak to an image histogram [i].

3.2 Detecting locally applied contrast enhancement in image:

The forensic technique is extended into a method of forgery image detection that is used to locate regions in image that can be performed by selecting a set of pixels comprising a region of interest. To achieve this, image can be segmented into fixed size blocks and each block constitutes a separate region of interest [i].

3.3 Detecting image scaling or cropping:

In this the method is proposed for detecting image scaling or cropping in image by identifying the intrinsic fingerprint of pixel

value mapping. To obtain the energy in the high frequency component of pixel value histogram .If the threshold value is greater than energy, then the image is resized, otherwise the image is unaltered [i].

3.4 Detecting Histogram equalization in image:

Just like any other contrast enhancement operation, histogram equalization operation introduces sudden peaks and gaps into an image histogram. The techniques are extended into method for detecting histogram equalization in image [i].

3.5 Detecting Noise in image:

The technique for detecting noise is able to detect whether the image is in noise or not, such as speckle noise, Gaussian noise etc. And every image is classified as altered or unaltered by using a series of decision thresholds to evaluate the performance of each forgery image by ROC curve [i].

4. Conclusion

There are number of techniques to detect forgery in image, each of which comes with some merits and demerits. We studied few of them in this paper. The techniques discussed above are useful for detecting cut and paste type forgeries. This paper does an extensive survey on the technique to detect copy-move forgery that is duplication in image.

Acknowledgement

We are thankful to all the researchers who helped us throughout this survey. We would like to express our special thanks to our professors for giving us constant motivation and encouragement. After that the detection and false alarm probability are calculated at each decision threshold.

References

i.S. Thirumagal and Dr. S. Allwin, "Image manipulation detection using intrinsic statistical fingerprints", International Journal of Advanced Research in Computer Science and Software Engineering, vol. 2, Issue 6, June 2012.

ii.Matthew C. Stamm and K.J. Ray Liu, "Forensic detection of image manipulation using statistical intrinsic fingerprints", IEEE Trans. ON Information forensics and security, vol. 5, No. 3, September 2010.

iii.A Swaminath, M. Wu and K. J. R. Liu, "Digital image forensics via intrinsic fingerprints", IEEE Trans. Inf. Forensics Security, vol. 3, no. 1, pp. 101-117, mar. 2008.

iv.J Luka's, J. Fridrich and M. Goljan, "Detecting digital image forgeries using sensor pattern noise", in Proc. SPIE, Electronic Imaging, Security, Steganography, Watermarking of Multimedia Contents, San Jose, CA, Feb 2006, vol. 6072, pp. 362-372.

v.AC. Popescu and H. Farid, " Exposing digital forgeries by detecting traces of resampling", IEEE Trans. Signal Process., vol. 53, pp. 758, Feb. 2005.

vi.M.C. Stamm and K. J. R. Liu, " Forensic detection of image tampering using intrinsic statistical fingerprints in histograms", in Proc. APSIPA Annual Summit and Conf., Sapporo, Japan, Oct. 2009.

vii.M. Stamm and K. J. R. Liu, "Blind forensics of contrast enhancement in digital images", in Proc. ICIP, San Diego, CA, Oct. 2008, pp. 3112-3115.

viii.R. C. Gonzalez and R.E. Woods, Digital Image processing. Boston, MA: Addison-Wesley, 2001.

ix.Abhitha E. and V. J. Arul Karthick, "Forensic technique for detecting tamper in digital image compression", International Journal of Advanced Research in Computer and Communication Engineering, vol. 2, issue 3, March 2013.

x.S. Khan and A. Kulkarni, "Reduced time complexity for detection of copy-move forgery using discrete wavelet transform", IJCA, vol. 6, no. 7, pp. 31-36,2010.

xi.H. Farid, "Image forgery detection", IEEE Signal Processing Magazine, vol. 26, no.2, pp. 16-25, Mar. 2009.

xii.C.McKay, A. Swaminathan and M. Wu, "Image acquisition forensics: forensic analysis to identify imaging source", 2008 IEEE International Conference on Acoustics, Speech and Signal Processing, pp. 1657-1660, mar.2008.

xiii.X. Bo, W. Junwen, L. Guangjie and D. Yuewei, "Image copy-move forgery detection based on SURF", 2010 International Conference on Multimedia Information Networking and Security, pp. 889-892,2010.

xiv.I. Amerini, L. Ballan, S. Member, R. Caldelli, A. Del Bimbo and G. Serra, "ASIFT-based forensic method for copy-move attack detection and transformation recovery", IEEE Trans. On Information Forensics and Security, vol. 6, no. 1, pp. 1-12, 2011.

xv.B. Mahdian and S. Saic, "On periodic properties of interpolation and their application to image authentication", Third International Symposium on Information Assurance and Security, pp. 439-446, Aug. 2007.

xvi.T. Bianchi and A. Piva, "Reverse engineering of double JPEG compression in the presence of image resizing", 2012 IEEE International Workshop on Information Forensics and Security (WIFS), no. 1,pp. 127-132, Dec.2012.

xvii.F. Huang, J. Huang, S.Member and Y. Q. Shi, "Detecting double JPEG compression with the same quantization matrix", IEEE Trans. On Information Forensics and Security, vol. 5, no.4, pp. 843-856, 2010.

xviii.P. Ferrara, T. Bianchi, A. De Rosa, A. Piva and S. S. Member, "Image forgery localization via fine-grained analysis of CFA artifacts", IEEE Trans. On Information Forensics and Security, vol.7, no.5, pp. 1566-1577, 2012.

xix.M.K.Johnson and H. Farid, "Exposing digital forgeries through chromatic aberration", Proceeding of the 8th Workshop on Multimedia and Security- MM and Sec '06, no. 2, pp. 48, 2006.

xx.B. Rajner and M. Kirchner, Counter-Forensics: Attacking Image Forensics. Springer 2012.