International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 02 Issue: 04 | July-2015 www.irjet.net p-ISSN: 2395-0072

Literature Survey on Image Manipulation Detection

Rani Mariya Joseph[1], Chithra A.S.[2]

[1]*M.Tech Student, Computer Science and Engineering, LMCST, Kerala, India*

[2] *Asso. Professor, Computer Science And Engineering, LMCST, Kerala, India*

Abstract - ***Digital imaging has experienced tremendous growth in recent decades, and digital camera images have been used in a growing number of applications. Now a days several softwares are available that are used to manipulate image so that the image is look like as original. Images are used as authenticated proof for any crime and if these images do not remain genuine then it will create a problem. Detecting these types of forgeries has become serious problem at present. To determine whether a digital image is original or doctored is a big challenge. To find the marks of tampering in a digital image is a challenging task. This paper presents a literature survey on some of the image Manipulation detection techniques such as contrast enhancement detection, splicing and composition detection, image tampering etc.Comparison of all the techniques concludes the better approach for its future research.***

Key Words: *digital Forensics and Anti-forensics, image forgery. Image manipulation, contrast enhancement, composite image.*

1. INTRODUCTION

In today's world it is easy to manipulate the image by adding or removing some elements from the image which results in a high number of image forgeries. With the increasing applications of digital imaging, different types of software are introduced for image processing. Such software can do an alteration in digital image by changing blocks of an image without showing the effect of the modification in the forged image. These modifications cannot be noticed by human eyes. Therefore verification of originality of images has become a challenging task. An image can be manipulated with a wide variety of manipulation techniques such as scaling, rotation, blurring, resampling, filtering, cropping, etc. Image forgery detection technique is needed in many fields for protecting copyright and preventing forgery. The verification of originality of images is required in variety of applications such as military, forensic, media, scientific, glamour, etc. Image tampering is a digital art which needs understanding of image properties and good visual creativity. Detection of image tampering deals with investigation on tampered images for possible correlations embedded due to tampering operations. Detecting forgery in digital images is a rising research field with important implications for ensuring the credibility of digital images.

With the rapid development of digital media editing techniques, digital image manipulation becomes rather convenient and easy. While it benefits to legal image processing, malicious users might use such innocent manipulations to tamper digital photograph images. Currently, image forgeries are widespread on the Internet and other security-related applications such as surveillance and recognition that utilize images are therefore impacted. The event and scene information delivered in images might become no longer believable. In the applications such as law enforcement and news recording, it is also necessary to verify the originality and authenticity of digital images, and make clear the image manipulation history to get more information. To circumvent such a problem, digital forensic techniques have been proposed to blindly verify the integrity and authenticity of digital images.

Generally, image manipulations could be classified into

i. content-changing manipulations
ii. content-preserving manipulations

Accordingly, prior works on image manipulation forensics fall into two categories. As the first category, the forensics methods focus on detecting image tampering such as copy –move and splicing, by which the image content is

reshaped arbitrarily according to semantic content. In the second category, common manipulations, as compression, blur and contrast enhancement are detected passively. These content-preserving manipulations are often applied as post processing to conceal the residual trail of malicious tampering operations and create realistic forgeries.

The phenomenon of image forgery leads to serious consequences such as reducing trustworthiness and creating false beliefs in many real-world applications. For example, Fig.1 (a) shows a doctored photograph of celebrities Cher and Brad Pitt, falsely implying their simultaneous presence at the same location. Fig. 1(b) shows a copied-and-pasted British soldier pointing his machine gun at Iraqi people. It was published on the front page of L.A. Times in 2003, causing the public image of the British Army to be brutal, merciless. Besides splicing, doctored images can be generated with other operations.

Fig 1: Examples of doctored photographs

(a) Celebrities Cher and Brad Pitt spliced side-by-side

Fig 1: Examples of doctored photographs

(b) British soldier pointing machine gun at Iraqi people

2. CRITICAL ANALYSIS OF VARIOUS TECHNIQUES

The objective of the literature review is to find and explore the benefits of image manipulation detection techniques and also to find the shortcomings in existing methods and techniques. The main goal of this literature review is to find the gaps in existing research and techniques and to find possible solutions to overcome these holes.

3. LITERATURE SURVEY

S. Bayram, et al. [1] proposed a technique for the detection of doctoring in digital image. Doctoring typically involves multiple steps, which typically involve a sequence of elementary image-processing operations, such as scaling, rotation, contrast shift, smoothing, etc. The methodology used is based on the three categories of statistical features including binary similarity, image quality and wavelet statistics. The three categories of forensic features are as follows:

1. Image Quality Measures: These focuses on the difference between a doctored image and its original version. The original not being available, it is emulated via the blurred version of the test image.
2. Higher Order Wavelet Statistics: These are extracted from the multiscale decomposition of the image.
3. Binary Similarity Measure: These measures capture the correlation and texture properties between and within the low significance bit planes, which are more likely to be affected by manipulations.

To deal with the detection of doctoring effects, firstly, single tools to detect the basic image-processing operations are developed. Then, these individual “weak” detectors assembled together to determine the presence of doctoring in an expert fusion scheme.

Swaminathan et al. [2] proposed a method to estimate both in-camera and post-camera operation fingerprints for verifying the integrity of photographs. This paper introduces a new methodology for the forensic analysis of digital camera images. The proposed method is based on the observation that many processing operations, both inside and outside acquisition devices, leave distinct intrinsic traces on digital images, and these intrinsic fingerprints can be identified and employed to verify the integrity of digital data. The intrinsic fingerprints of the various in-camera processing operations can be estimated through a detailed imaging model and its component analysis. Further processing applied to the camera captured image is modelled as a manipulation filter, for which a blind deconvolution technique is applied to obtain a linear time-invariant approximation and to estimate the intrinsic fingerprints associated with these post camera operations. The absence of camera-imposed fingerprints from a test image indicates that the test image is not a camera output and is possibly generated by other image

production processes. Any change or inconsistencies among the estimated camera-imposed fingerprints, or the presence of new types of fingerprints suggest that the image has undergone some kind of processing after the initial capture, such as tampering or steganographic embedding.

H. Cao et al. [3] designed a new ensemble manipulation detector to simultaneously detect a wide range of manipulation types on local image patches. Fan et al. [4] proposed to correlate statistical noise features with exchangeable image file format header features for manipulation detection.

M. C. Stamm and K. J. R. Liu, [5] proposed different methods not only for the detection of global and local contrast enhancement but also for identifying the use of histogram equalization and for the detection of the global addition of noise to a previously JPEG-compressed image. The methodologies used are as follows.

i). 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.

ii).Detecting locally applied contrast enhancement in image

Contrast enhancement operation may be locally applied to disguise visual clues of image tampering. Localized detection of these operations can be used as evidence of cut-and-paste type forgery. The forensic technique is extended into a method to detect such type of cut-and- paste forgery.

iii).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

iv). Detecting Noise in image

Additive noise may be globally applied to an image not only to cover visual evidence of forgery, but also in an attempt to destroy forensically significant indicators of other tampering operations. Though the detection of these types of operations may not necessarily pertain to malicious tampering, they certainly throw in doubt the authenticity of the image and its content. The technique for detecting noise is able to detect whether the image is in noise or not, such as speckle noise, Gaussian noise etc.

M. Stamm and K. Liu [6] focuses on recovering the possible information about the unmodified version of image and the operations used to modify it, once image alterations have been detected. An iterative method based on probabilistic model is proposed to jointly estimate the contrast enhancement mapping used to alter the image as well as the histogram of the unaltered version of the image. The probabilistic model identifies the histogram entries that are the most likely to occur with the corresponding enhancement artifacts.

P. Ferrara, et al.[7] proposed a paper in which a comparison between two forensic techniques for the reverse engineering of a chain composed by a double JPEG compression interleaved by a linear contrast enhancement is presented. The first approach is based on the well known peak-to-valley behaviour of the histogram of double-quantized DCT coefficients, while the second approach is based on the distribution of the first digit of DCT coefficients. These methods have been extended to the study of the considered processing chain, for both the chain detection and the estimation of its parameters. More specifically, the proposed approaches provide an estimation of the quality factor of the previous JPEG compression and the amount of linear contrast enhancement.

G. Cao, Y. Zhao, R. Ni and X. Li [8] proposed two novel algorithms to detect the contrast enhancement involved manipulations in digital images. First for detecting the contrast enhancement based manipulation involved in JPEG compressed images and the second one is used for detecting composite image. The methodologies are:

i. Global Contrast Enhancement Detection

Algorithm proposed in this paper, detects the contrast enhancement not only in uncompressed or high quality JPEG compressed images but also in middle/low quality ones. The main identifying feature of gray level histogram used is zero-height gap bin. Fig. 2 shows the definition of zero-height gap bin.

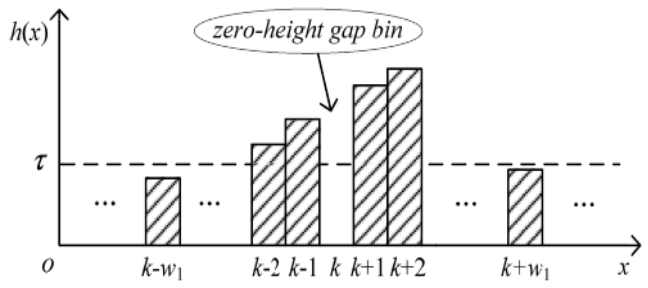

Fig 2: Definition of zero-height gap bin

ii. Identify Source-Enhanced Composite Images

A novel algorithm is proposed to identify the source-enhanced composite image created by enforcing contrast adjustment on either single or both source regions.Fig. 3 shows the both-source enhanced composite forged image. The two source images used for creating cut-and-paste type of forged images may have different color temperature or luminance contrast. So, in order to make the forged image more real, contrast enhancement is performed on either one or both the regions. In this paper, a new method was proposed to identify not only single source enhanced but also both source enhanced cut-and-paste type of forged images.

Fig 3: both-source enhanced cut-and-paste image forgery (a) and (b) original source images. (c) both-source enhanced composite forged image.

4. COMPARATIVE ANALYSIS

The techniques used in [1]-[4] could detect whether image manipulations occurred or not but it fails to determine which specific type of manipulation was enforced. The method proposed in [5] detects contrast enhancement in previously high quality JPEG compressed image. However, it fails to determine the contrast enhancement in previously middle/low quality JPEG compressed image. Also, a separate algorithm is proposed which could detect the local contrast enhancement in single source enhanced cut-and-paste forged images but, fails to detect the same in both source enhanced cut-and-paste forged images. The algorithm proposed in [6] gives accurate estimation if the enhancement is non standard. In [7], a method is designed to identify an operation chain, which is composed by double JPEG compression interleaved by a linear contrast enhancement. The special type of contrast enhancement, i.e., linear pixel value stretching, can be detected on condition that the operation chain occurs. The methods used in [8] detect the contrast enhancement in either uncompressed or previously JPEG compressed images. It also detects the local contrast enhancement in both single-source enhanced and both-source enhanced composite image. However, it can detect the contrast enhancement only if the contrast enhancement is the last step applied.

5. CONCLUSION

This paper presents a brief survey on image manipulation detection methods for contrast enhanced and cut-and-paste type of forged images. Many approaches have been proposed for such type of retouching forgery detection, each one has certain merits and demerits. The techniques described in [8] overcome the limitations of previous approaches. The techniques that are robust against the post processing operations and anti-forensic techniques need to be developed.

REFERENCES

[1] S. Bayram, I. Avcubas, B. Sankur, and N. Memon, "Image manipulation detection," *J. Electron. Imag.*, vol. 15, no. 4, pp. 04110201–04110217, 2006.

[2] A. Swaminathan, 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.

[3] H. Cao and A. C. Kot, "Manipulation detection on image patches using FusionBoost," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 3, pp. 992–1002, Jun. 2012.

[4] J. Fan, H. Cao, and A. C. Kot, "Estimating EXIF parameters based on noise features for image manipulation detection," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 4, pp. 608–618, Apr. 2013.

[5] M. C. Stamm and K. J. R. Liu, "Forensic detection of image manipulation using statistical intrinsic fingerprints," *IEEE Trans. Inf. Forensics Security*, vol. 5, no. 3, pp. 492–506, Sep. 2010.

[6] M. C. Stamm and K. J. R. Liu, "Forensic estimation and reconstruction of a contrast enhancement mapping," in *Proc. IEEE Int. Conf. Acoust., Speech Signal*, Dallas, TX, USA, Mar. 2010, pp. 1698–1701.

[7] P. Ferrara, T. Bianchiy, A. De Rosaz, and A. Piva, "Reverse engineering of double compressed images in the presence of contrast enhancement," in *Proc. IEEE Workshop Multimedia Signal Process.*, Pula, Croatia,Sep./Oct. 2013, pp. 141–146.

[8] Gang Cao, Yao Zhao, Rongrong Ni "Contrast Enhancement-Based Forensics in Digital Images" IEEE transactions on information forensics and security, vol. 9, no. 3, march 2014

BIOGRAPHIES

Rani Mariya Joseph received B.Tech degree in Information technology from Kerala University, at Lourdes Matha College Of Science And Technology-Trivandrum in 2012 . Currently she is pursuing her M.Tech degree under Kerala university, Kerala in Lourdes Matha College Of Science And Technology-Thiruvananthapuram

Chithra A.S received M-Tech in computer science and engineering with specialization in Digital image Computing from University of Kerala, Karyavattom in 2010 and B-Tech Degree in Computer Science and Engineering from LBS Institute of Technology for Women, University of Kerala in 2005. She got 10 years of experience in the teaching field.

