ISSN: 2321-7782 (Online)
Volume 2, Issue 11, November 2014
International Journal of Advance Research in Computer Science and Management Studies
Research Article / Survey Paper / Case Study
Available online at: www.ijarcsms.com

Literature Survey on Forensic Techniques for Image Forgery Detection

Jayshri Charpe[1]
Second Year M.Tech Student, Department of CSE
G. H. Raisoni Institute of Engi. & Tech. for Women's
Nagpur, India

Antara Bhattacharya[2]
Assistant Professor, Department of CSE
G. H. Raisoni Institute of Engi. & Tech. for Women's
Nagpur, India

Abstract: ***The digital images have a significant role in various fields like medical imaging, journalism, criminal and forensic investigations. Because of the widespread availability of photo editing software and tools, the process of verifying the authenticity and integrity of digital images becomes extremely difficult. It becomes problematic to use the digital images in applications where their genuineness is of prime importance. As a result, secure techniques for verifying an image's authenticity must be developed. Therefore, there is a need to create forensic techniques which is capable of detecting tampering in image. This paper reviews the forensic methods for detecting contrast enhancement in image by identifying the unique artifacts that appeared into the histogram of an image as a consequence of the particular operation under seen.***

Keywords: digital forensic; histogram equalization; contrast enhancement; image forgery; image processing

I. INTRODUCTION

With the increased importance of digital images in various applications, where authenticity is of prime importance, it is necessary to verify the integrity and authenticity of digital images. But, the use of digital images has become more common throughout society; creation of digitally forged images has increased. Because of the easy avaibility of image editing software such as Photoshop, making forgeries in digital images becomes an easy task without leaving obvious evidence that can be recognized by human eyes. So the image authentication came forth as an important problem. Digital image authentication techniques broadly have two types i.e. active and passive. The active approach includes intrusive methods like watermarking and digital signature. These are also known as non-blind 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. Also, use of these methods deteriorates image quality. To verify the image authenticity using passive approach, no information needs to be embedded in images for distribution. These methods are also known as blind as the presence of original image not required to verify the authenticity. So, these methods also have the application in the field of image forensic. Since the problem of image forensics is very broad, this survey focuses on forgery detection in 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, and noise in the digital image.

The three main aspects of operations that are performed in blind image forensics are:

» Identification of source, which specifies the source device that has been used to capture the image.

» Forgery detection which include tracing the tampering evidence.

» Detection of computer generated images as owing to the sophisticated software and hardware tools, it is possible to create computer generated images.

II. Related Work

S. Bayram, I. Avcubas, B. Sankur, and N. Memon [1] proposed a technique for the detection of doctoring in digital image. Doctoring includes multiple steps i.e. a sequence of basic image-processing operations such as rotation, scaling, smoothing, contrast shift 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 Measure: These focus 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.

M. Stamm and K. Liu [2] proposed a blind forensic algorithm for detecting the use of global contrast enhancement operations on digital images. Proposed work is based on the fact that, gray level histogram of the unaltered images exhibit a smooth contour whereas, gray level histogram of contrast enhanced images shows unsmoothness (peak/gap artifacts). A separate algorithm is proposed to identify the use of histogram equalization, a commonly Implemented contrast enhancement operation. The methodology used is as follows.

The methodology used is known as global contrast enhancement detection technique. This algorithms works by seeking out the unique artifacts left behind by histogram equalization. However, the paper specifies only about the detection of global enhancement and not about the local enhancement.

M. C. Stamm and K. J. R. Liu [3] 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.

a) 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.

b) 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.

c) 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.

d) 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 [4] 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.

G. Cao, Y. Zhao, and R. Ni [5] present a blind method for the detection of gamma correction, a special type of contrast enhancement.

The technique used is based on the histogram characteristics that are measured by patterns of the peak gap features. These peak gap features for the gamma correction detection are distinguished by the precomputed histogram of images.

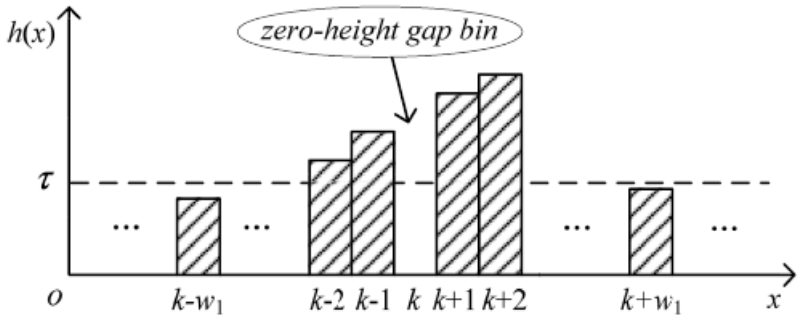

Figure 1: Defination of zero-height gap bin

G. Cao, Y. Zhao, R. Ni and X. Li [6] proposed two different algorithms for the detection of global and local contrast enhancement in an image. The methodologies are:

a) Identifying globally contrast-enhanced images:

Previous algorithms work well under the consideration that, gray level histogram of unmodified mages shows smoothness while that of contrast enhanced images shows peak/gap artifacts. In real applications, digital images are stored in JPEG format and are compressed with middle/low quality factor. It is well known that, low quality lossy compression usually generates blocking artifacts. So, prior approaches fail to detect the contrast enhancement in previously middle/low quality JPEG (lossy) compressed images. Algorithm proposed in this paper, solves such a problem. Algorithm 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. 1 shows the definition of zero-height gap bin.

b) Identifying locally contrast enhanced images:

An important application is to identify cut-and-paste type of forged images, in which the contrast of one source region is shifted to match the rest. Fig. 2 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. However, cut-and-paste type of images created by enhancing single source could be identified in prior work, but it fails to detect the both source-enhanced

cut-and-paste type of forged images. In this paper, a new method was proposed to identify not only single source enhance but also both source enhanced cut-and-paste type of forged images.

Figure 2: both-source enhanced cut-and-paste image forgery
(a) and (b) original source images. (c) both-source enhanced composite forged image.

III. COMPARATIVE ANALYSIS

The technique used in [1] could detect whether image manipulations occurred or not but it fails to determine which specific type of manipulation was enforced. In [2], the technique is specified only for the detection of globally applied contrast enhancement in images. However, detection of locally applied contrast enhancement is not mentioned in the paper. The method proposed in [3] 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 [4] gives accurate estimation if the enhancement is non standard. The approach in [5] again fails to detect the contrast enhancement in previously middle/low quality JPEG compressed image. The methods used in [6] 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 composite image. However, it can detect the contrast enhancement only if the contrast enhancement is the last step applied.

IV. CONCLUSION

This paper presents a brief survey on forgery 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 in [6] overcome the limitations of previous approaches. However, we still believe that the domain has not gained as much attention as the copy/move forgery. The techniques that are robust against the post processing operations and antiforensic 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. M. Stamm and K. Liu, “Blind forensics of contrast enhancement in digital images,” in 15th IEEE Int. Conference on Image Processing, 2008. ICIP 2008, Oct. 2008, pp. 3112–3115.
3. M. Stamm and K. Liu, “Forensic detection of image manipulation using statistical intrinsic fingerprints,” IEEE Trans. Inf. Forensics Security, vol. 5, no. 3, pp. 492–506, Sep. 2010.
4. M. C. Stamm and K. J. R. Liu, “Forensic estimation and reconstruction of a contrast enhancement mapping,” in Proc. IEEE Int. Conference Acoust., Speech Signal, Dallas, TX, USA, Mar. 2010, pp. 1698–1701.
5. G. Cao, Y. Zhao, and R. Ni, “Forensic estimation of gamma correction in digital images,” in Proc. 17th IEEE Int. Conf. Image Process..Hong Kong, 2010, pp. 2097–2100.
6. G. Cao, Y. Zhao, R. Ni and X. Li, “Contrast Enhancement-Based Forensics in Digital Images,” IEEE Trans. Inf. Forensics Security, Mar. 2014

