Volume 5, Issue 7, July 2015 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Digital Image Forensic

Sushama Kishor Bhandare
Dept. of Computer Sci & Engg.
Anuradha Engineering College, Chikhali
Amravati University, Maharashtra, India

Nitin Krishnarao Bhil
Asst. Prof., Dept. of Computer Sci & Engg.
Anuradha Engineering College, Chikhali
Amravati University, Maharashtra, India

Abstract— The digital image plays a important role in various fields like information forensic , journalism, criminal and forensic investigations ,medical fields etc…Because of the widespread availability and popularity of photo editing tools and software it become easy to modify the images but such modified images become problematic in some areas where the geniuses of image has a prime important and in such fields it become extremely difficult to verify the authenticity and integrity of digital images. Modern software has made the manipulation of photos easier to carry out and harder to uncover than ever before. Therefore there feel a need to find out a forensic technique which will be capable to detect the tampering in modified digital images and to verify images authenticity. This paper reviews the forensic methods for detecting globally and locally applied contrast enhancement, cut-and-paste forgery, histogram equalization, and noise in the digital image .

Keywords —contrast enhance image, histogram equalization, Noise in image,

I. INTRODUCTION

With the increased importance of digital images in various applications, where authenticity is mandatory, the use of digital Images increases throughout society thus the creation of digital forged images by using various available and popular editing tools and modern software has also 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. So the image authentication emerged as an important problem in a digital image authentication field. There are two approaches of digital image authentication

1. Active approach
2. Passive approach

1. Active Approach

The active approach includes 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.

2. Passive Approach

In passive approach of digital image authentication technique, 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.

Digital image forensic is a computer technique for improving a digital image like surveillance, closed circuit TV ,infrared image, etc. These techniques involve digital "filters" that can suppress noise in the digital image, extract the details from shadow and provide image sharpening. The distribution of image pixels i.e. histograms can also be optimized for information extraction. And because of this it become easy to verify authenticity and integrity of digital images in a field where the geniuses of image has a prime important.

Since the problem of image forensics is very broad, this paper focuses on forgery detection in digital images. There are three lead directions for image forensics research.

- The source of images is identified.
- Attempts to classify computer generated images from natural images.
- Tackles the problem of forgery detection for digital images.

This paper gives 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.

II. RELATED WORK

A. S. Bayram, I. Avcubas, B. Sankur, and N. Memon proposed[2] a technique for the detection of doctoring in digital image. Doctoring includes 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 measure, image quality measure and Higher order wavelet statistics. The three categories of forensic features are as follows:

- **a. 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.
- **b. 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.
- **c. Higher Order Wavelet** Statistics: These are extracted from the multiscale decomposition of the image.

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.

B. G. Cao, Y. Zhao, R. Ni and X. Li [3][4], 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:

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.

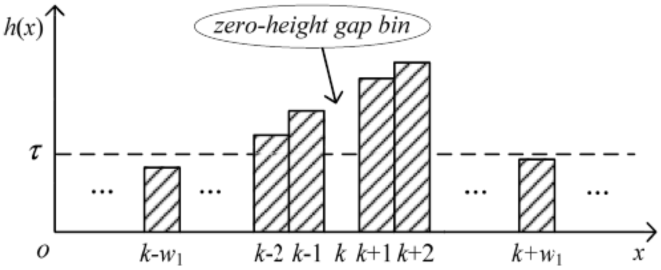

Fig. 1 the Definition of zero height gap bin

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.

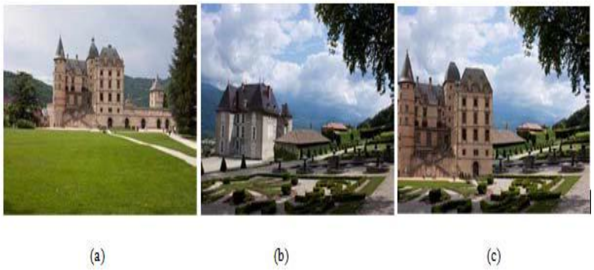

Figure 2: both-source enhanced cut-and- paste image forgery
(a) and (b) original source images. (c) both-source enhanced composite forged image.

c. Matthew C.Stamm and K.J.Ray Liu [4] 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

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.

2. 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.

3. 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.

4. 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.

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. Stamm and K. Liu 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.

a. Abhitha. E and V.J.Arul Karthick[8] 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.
b. *Marcus Borengasser, has focused on Forensic image processing technology [9] for many years.* Forensic image processing can help the analyst extract information from low quality, noisy imagery. Obviously, the desired information must be present in the image although it may not be apparent or visible. Forensic image processing techniques used open-source image processing software.

III. APPLICATIONS OF FORENSIC IMAGE PROCESSING

FIP technology is primarily used for enhancement of surveillance video. This surveillance imagery can be produced by video cameras or cameras that produce individual image frames. The surveillance video can be from a wide variety of locations such as bank lobbies and ATMs, hospitals, universities, retail locations, shopping malls, traffic signals, toll booths, outdoor venues, and much more. While the term “photograph” describes the output of a camera, an image refers to any type of graphical representation for depiction of an object, including a photograph. So, a photograph is an image but an image is not necessarily a photograph. In this context, forensic image processing is also applicable for the enhancement of images, such as images of fingerprints, retinal scans, shoe impressions, and so on.

Typically, in the event of a crime, a crime scene investigator will recover the surveillance video for analysis by a criminologist, or forensic image analyst. The goal of the analyst is to determine the image enhancement process that will allow maximum information extraction from the surveillance video.

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.

IV. CONCLUSION

This paper presents a brief survey on forgery detection methods for contrast enhanced and cut-and-paste type of forged images. The various approaches that we put up here have some merits and demerits . The techniques that are robust against the post processing operations and antiforensic techniques need to be developed.

REFERENCES

[1] Digital Image Forensic by Hany Farid “sciam08.pdf” .

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

[3] 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.

[4] G. Cao, Y. Zhao, R. Ni and X. Li, “Contrast Enhancement-Based Forensics in Digital Images,” IEEE Trans. Inf. Forensics Security, Mar. 2014 .

[5] 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.

[6] 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.

[7] 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

[8] 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.

[9] “Introduction to Forensic Image Processing.htm” by Marcus Borengasser.