Review of digital image forgery detection based on histogram analysis

Shweta Panse
Department of Computer Science and Engineering
GH Rasioni Women's College of Engineering
Nagpur, India
Prakash Mohod
Department of Computer Science and Engineering
GH Raisoni Women's College of Engineering
Nagpur, India

Abstract—**Digital images are used for a variety of applications such as news media, film industry, military application etc. With the help of image editing software tools, it is easy to alter the content of an image. So the content of an image is no longer believable nowadays. Contrast enhancement is an important factor for image enhancement. There are various types of techniques to create forged images for various intentions. When an attacker manipulates an image, contrast enhancement is used for avoiding traces left by the image forgery. There are so many methods to enhance contrast of an image. So in order to detect an image forgery, it is necessary to perform contrast enhancement detection. This paper reviews various methods for detecting contrast enhancement in digital images**

Keywords-digital image processing, forgery detection, histogram analysis, contrast enhancement

I. INTRODUCTION

Digital images are widely used for a variety of applications such as governmental, legal, scientific, and military to make critical decisions. Digital images are considered as proofs against various crimes or evidences for various purposes. The aim of image enhancement is to enhance quality of the image so that visual appearance can be improved. By using media editing software such as Photoshop and Picasa, it is easy to alter an image. So, the authenticity and originality of a digital image is no longer believable. So there is a need for digital image forensic techniques in order to verify image alternations and forged images. Image manipulations like brightness and contrast enhancement can be used by the attacker to avoid leaving visual clues after forging an image. Contrast enhancement is mainly to adjust the brightness of the image. Attackers may perform contrast enhancement locally and globally for creating manipulated images. Histogram equalization is one of the contrast enhancement methods. Most of the contrast enhancements are based on pixel-value mapping operations which introduces some statistical traces in the histogram that can be used to explain the image forgery. So it is necessary to detect contrast enhancement for verifying the authenticity and originality of the digital images. Histogram is the graphical representation of an image. When applying contrast enhancement, it will change the pixel –value mappings of the image. The changes in the pixel-value mapping results sudden peaks and gaps in the histogram. This paper discussed about the various contrast enhancement detection methods in digital methods.

II. BACKGROUND

Figure.1. Shows the image-acquisition model in digital cameras. We model digital images as the output of the following image capture process. The real-world scene is captured using a digital camera. The information about the scene passes through the various camera components before the final digital image is produced. Each component modifies the input using a particular algorithm and leaves some fingerprint traces on the output. The image acquisition model in digital cameras have

components like lens, optical filter, color filter array etc. the light passes through the lens and optical filters and it is recorded by color sensors. Color filter array is used to sample the real-world scene. After interpolation the light components go through a post-processing stage. The images may undergo operations like denoising, gamma correction, white balancing etc. For any digital images, a his4togram of its pixel values can be calculated by creating equally spaced bins which span the range of possible pixel values and tabulating the number of pixels whose value falls within the range of each bin. We model the histogram of an unaltered image as a digital function which approximately conforms to a smooth envelop.

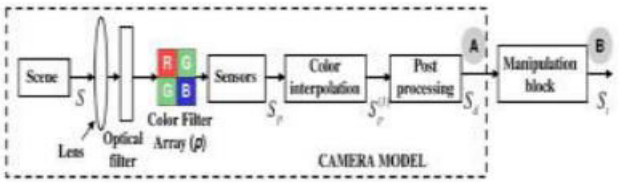

Figure 1. Image acquisition

Digital image forgery detection techniques are classified into two categories: active image forgery and passive-blind image forgery. In active forgery, preprocessing operations are involved. Active approaches could be divided into digital watermarks and signatures. In the passive approaches, no pre-calculation are required. Image retouching, image splicing and Copy-move forgery are passive approach. Operations such as contrast enhancement, rescaling, rotation are performed in image retouching. In image splicing, two or more images are considered from which region is copied to form new image. In copy-move forgery, one region is copied from an image and pasted onto other region of same image. Another copy-move forgery through composition is copying and pasting areas from one or more images and pasting onto an image being forged. This is called composite image forgery. Copy-move forgery manipulates both, image statistics and image content as well. There are many tools available for image forgery detection. Hany Farid groups the image forensic tools [1] into five main categories :1) pixel-based techniques that detect statistical artifacts introduced at the pixel level; 2) format-based techniques that leverage the statistical correlations introduced by a specific lossy compression scheme; 3) camera-based techniques that exploit artifacts introduced by the camera components; 4) physically based techniques that detect anomalies in the three dimensional interaction between physical objects, light, and the camera; and 5) geometric-based techniques that make measurements of objects in the world and their positions relative to the camera.

Contrast enhancement techniques improve the perceptibility of objects in the scene by enhancing the brightness difference between objects and their backgrounds. Some of the contrast enhancement techniques are Contrast Stretching, Histogram equalization etc. Histogram equalization is widely used for contrast enhancement in a variety of applications .It works by flattening the histogram and stretching the dynamic range of the gray levels. One problem of the histogram equalization is that the brightness of an image is changed after the histogram equalization. Contrast enhancement operations usually modify the histogram of pixel intensity values. Due to observational noise and various complex lighting environments, image histograms do not contain sudden zeros or impulsive peaks [9]. So the variation of the histogram of an unaltered image is low. Contrast enhancement manipulation will expand or squeeze the original histogram and lead to sudden peaks and gaps in the histogram. So it will increase the high-frequency energy in the histogram spectrum.

III. Related Work

M. Stamm and K. Liu [2] proposed an algorithm for detecting the use of contrast enhancement operations and also proposed a separate algorithm for detecting the use of histogram equalization, a contrast enhancement operation. These methods are based on the fingerprints introduced into an image's histogram as a result of the contrast enhancement operations. The proposed method is based on the fact that the histogram of original images exhibit a smooth contour whereas the histogram of altered images show peak and gap artifacts. This paper specifies only about the detection of global contrast enhancement and not about the local enhancement.

A. Swaminathan, M. Wu, and K. J. R. Liu [3] proposed a new method for the forensic analysis of digital camera images. The various traces that are left behind in a digital image when it goes through various processes are called intrinsic fingerprints. These fingerprints are used to identify the source and are used to establish the authenticity of the image. There are in-camera and post-camera fingerprints. The absence of in-camera fingerprints suggests that the test image is not a camera output and it is generated by other image production processes. The presence of new post-camera fingerprints suggests that the image has undergone some kind of post-camera processing. This work describes the image acquisition model in digital cameras. The light from the real world scene passes through various components of the information chain before the final image is created. The light from the scene passes through lens and optical filters and recorded by the color sensors. Most digital cameras use a color filter array to sample the real world scene. This paper also describes method to estimate the camera component parameters and also describe method to estimate the post-camera fingerprints of manipulated camera outputs. Any further post-camera processing is considered as a manipulation filter.

M. C. Stamm and K. J. R. Liu [4] again proposed the method for detecting general forms globally and locally applied contrast enhancement and also proposed a method for identifying the use of histogram equalization by searching for the identifying features of each operation's intrinsic fingerprint. The pixel value mappings leave behind statistical artifacts are visible in an image's histogram. By observing the common properties of the histogram of unaltered images, the model of an unaltered image's histogram is proposed. None of the original image's histograms contain sudden zeros or impulsive peak. Using this model, we can identify the features of a pixel value mapping's intrinsic fingerprint. Contrast enhancement operations can be applied locally to remove visual clues of image tampering. Locally applied contrast enhancement detection can be used to identify cut-and-paste forgery. Contrast enhancement operations increase the range of pixel values within the image. Most operations uses non-linear mapping to the values of each pixel in the image. The increase in energy within the pixel value histogram corresponds to the energy of the fingerprint left by the contrast enhancement mapping. By measuring the strength of the high frequency components of an image's pixel value histogram, contrast enhancement operation can be detected. A composite image can be created by replacing a contiguous set of pixels in one image with a set of pixels corresponding to an object from a separate image. A manipulator may need to perform contrast enhancement on one of the source image so that the lighting conditions match across the composite image. The test image is segmented into blocks. Each block is tested for evidence of locally applied contrast enhancement. Here only pasted region has undergone contrast enhancement.

In [2], the detection algorithm fails to estimate the gray-level mapping function including gamma mapping. In [5], a method to reconstruct the gamma mapping via the recognition of the peak-gap fingerprints in the histograms is proposed. Gamma correction is a contrast enhancement operation. The peak-gap fingerprint patterns and the methodology of pattern matching are employed to achieve fast gamma estimation. The general peak-gap characteristic which is unique to gamma mapping should be identified firstly. The peak-gap pattern for different gamma mappings can be pre-computed theoretically. The amount of gamma correction is estimated by matching the peak-gap feature pattern extracted from test images to those pre-computed ones.

M. C. Stamm and K. J. R.Liu [6] proposed a method for detecting image manipulation. The intrinsic fingerprints are the evidence of image manipulation and can be used to determine which operations were used to modify an image. This paper proposed an iterative algorithm to estimate any contrast enhancement mapping used to alter the image. Once the image modifications have been detected, the next task is to recover as much information as possible about the unaltered version of image and also the operation used to modify it. A probabilistic model is used to estimate contrast enhancement mapping used to modify the images as well as the histogram of the unaltered version of the image. This model identifies the histogram entries that are most likely to occur with corresponding

enhancement artifacts. It describes the pixel value histograms of the image as interpolated and connected. Once an image has been identified as contrast enhanced, an estimate of the contrast enhancement mapping used to modify the image as well as an estimate of the unaltered image's pixel value histogram can be jointly obtained through an iterative process. The results indicate that the iterative algorithm is capable of providing accurate estimates even when nonstandard forms of contrast enhancement are applied to an image.

M. C. Stamm and K. J. R. Liu [7] proposed a forensic method of exposing cut-and-paste image forgery through detecting contrast enhancement. It is about the inter-channel correlation introduced by color image interpolation, and shows how a linear or nonlinear contrast enhancement can disturb this natural inter-channel dependency. In order to measure the correlation, a metric is constructed. Using this metric we can distinguish the original and contrast enhanced images. In a composite image, the contrast between the background and the pasted region is not consistent with that of original image. Contrast enhancement operations introduce some statistical traces. So this method exposes cut-and-paste forgery by detecting contrast enhancement. Stamm and Liu proposed a general contrast enhancement detection algorithm based on the observations in the histogram of the images. But there are some parameters need to be determined by users. As the parameters may vary with different forms of contrast enhancements, it is not convenient in practice. If the attacker removes the peak and gap artifacts in the histogram, this histogram based methods will fail to find out the contrast enhancement operations. This paper describes how the contrast enhancement can be disturb the inter-channel similarities of high frequency components of an image and what will happen to its high frequency components if it is enhanced.

IV. PROPOSED APPROACH

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 pre-computed histogram of images.

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.

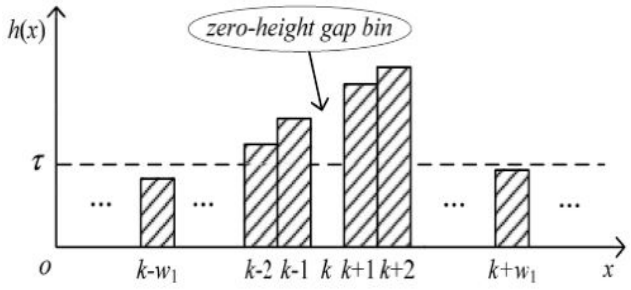

Figure 2. Gap bin detection

V. CONCLUSION

In this paper, a brief survey of image contrast enhancement detection methods is discussed. Many methods have been proposed for identifying image manipulations like cut-and- paste type image forgery. Each of these methods has certain merits and limitations. The attacker will introduce new methods to remove the traces left by the image modifications. So it is necessary to develop new methods to overcome such situations and also try to improve the robustness of such detection methods against post processing. The security enhancement of such methods will also consider in the future works.

REFERENCES

[1] Hany Farid "Image Forgery Detection [A survey]", IEEE Signal Processing Magazine, March 2009.

[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] 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.

[4] 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.

[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] 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] Lin, X., Li, C.-T., and Hu, Y., "Exposing image forgery through the detection of contrast enhancement," Proceedings of IEEE International Conference on Image Processing, Melbourne, Australia (Sept. 2013).

[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.