

A survey on contrast enhancement based image forensics of Digital Images

Krati Shrivastava

Research Scholar, SoIT, RGPV, Bhopal, India

kritidamoh@gmail.com

Abstract

Image forensics is been an emerging domain of research these days. Whenever any tampering to the image is done, contrast enhancement is imparted to image to hide tampering. In this paper a survey is done on different type of image forgery and their detection techniques which based on contrast enhancement.

Keywords: Contrast based image forensics, peak/gap based method, copy move, copy paste, splicing

I. INTRODUCTION

In this day and age it is anything but difficult to control the picture by including and erasing a few components from the image. Various free tools are available on internet, So whether to trust digital image or not is main concern. In manipulation of digital image contrast enhancement play vital role by adjusting the contrast and brightness of merge image [1].

For long time image were generally accepted as proof that event is occurred. The manipulation of pictures exploitation computer techniques is not new and gained plenty of recognition and even acceptance in

various area like forensic investigation, IT, intelligence service, medical imaging

etc, as a evidence [2]. Due to which the event mention in digital image is at no time in the future believable. In case of any forgery with the image like converge of two images contrast usually changes and there is considerable difference between the foreground and the background image. So in such cases to make image original contrast enhancement over one of the images is performed. Differentiate improvement brings about significant changes in histogram. That is peak and gaps of the histogram changes.

The central objective of this paper is to review about First: various type of forgery, Second: how contrast enhancement play vital role in manipulating any digital image and Third:

Image forgery detection techniques which will be pixel based image forgery detection.

The rest of the paper is organized as following

II. KIND OF DIGITAL IMAGE FORGERY

Images forgery is done with different objectives, it classify as innocent and malicious.

- a. **Innocent forgery** – If image editing is use to improve quality of picture without changing its meaning then this kind of forgery is known as innocent forgery.
- b. **Malicious forgery** – If image editing is done purposefully which alter the meaning of image.

INNOCENT EDITING	MALICIOUS EDITING
Color modification	Copy – move
Contrast adjustment	Copy – paste
Filtering	Splicing

Figure-1: Image editing operations.

Picture altering is characterised as “adding, changing, or deleting some necessary options from a picture while not departure any obvious trace [3]. There are totally different techniques utilized for manipulation a picture. Taking into consideration the strategies used to create forged picture, digital image forgery are often isolated into three primary classification:

Copy – Move, copy – paste and image splicing.

A. COPY – MOVE FORGERY

In Copy – move forgery some piece of a picture of any size is driven and glue to an alternate range inside a similar picture. Properties like noise, colour, and texture don't modified and create trouble. Fig 1

B. COPY – PASTE FORGERY

In Copy-paste forgery a piece of one picture is replicated and glue on another picture and joining locale is stow away by utilizing contrast enhancemen.Fig 2.

C. IMAGE SPLICING FORGERY

In this forgery two different images are joined to generate a new image.Fig 3



Figure.2: An example of copy-move forgery



a) Source image-1



b) Source image-2



**c) Copy –paste forgery(Image 1 paste into image 2)
Fig.2 Copy – paste forgery.**



Figure 3: Example of splicing[3]

III. DIGITAL IMAGE FORGERY DETECTION TECHNIQUES:

The blind image forensics detection methods that are presently in use is sorted in to five broad classes [4] i.e

- Pixel based techniques
- Format based techniques
- Camera based techniques
- Physical based techniques
- Geometry based techniques

IV. CONTRAST ENHANCEMENT TECHNIQUE:

The usually utilized methods for picture improvement are evacuation of commotion, edge upgrade and differentiation improvement. Out of these contrast enhancement is a mainstream one. Differentiate improvement is a standout amongst the most essential procedures for picture upgrade [5]. In this method contrast of the image is upgrade to improve image quality. The contrast is nothing but a variation of dark and bright areas present in the image. Among all popular methods histogram equalization (HE) is most popular one for contrast enhancement

The methods for contrast enhancement are ordered as global enhancement method and local enhancement method are quick and basic, and are appropriate for general upgrade of the picture. These strategies can't adjust to local brightness components of the information picture in light of the fact that exclusive global histogram data over the entire picture is utilized [6]. This reality restricts the complexity proportion in a few sections of the picture and consequently causes critical differentiation misfortunes out of sight and other little districts. One such case of global upgrade strategy is global histogram adjustment.

Other local enhancement method are also used. Local enhancement systems can improve general contrast avll the more successfully. In nearby upgrade, a little window slides through each pixel of the info picture successively and just those square of pixels are improved that fall in this window. And grey level mapping is done just for the inside pixel of that window [7].

Hence, it makes great utilization of local method. In any case, in local upgrade systems, computational cost goes high because of its completely covered sub-pieces and causes over-improvement in a few segments of the picture. Another issue is that it improves the commotion impact in the picture too.

V. LITERATURE SURVEY

Swaminathan et al check the integrity of the image by both in-camera and post camera method. It was observed that both in camera and post camera device leave some unique trace on the digital images, hence on the basis of this observation, algorithm have been proposed and these unique fingerprints are used to check the integrity of the digital image. There are two types of fingerprint which are in-camera and post camera. If in-camera fingerprints are absent, that indicate that the image is not taken by camera and it was generated from another image. This research work describes the image acquisition model in digital camera. [8]

P. Ferrara, et al. proposed a paper in which a comparison has been done between two forensic techniques for the reverse engineering composed by a double JPEG. The first method is based on the well known peak-bin behaviour of the histogram of DCT coefficient on other side the second method 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. [9]

M. Kirchner et. al. discussed contrast enhancement techniques such as Gamma Correction (GC) and Histogram Stretching (HS) are studied and compared. However, the enhancement operations by itself will leave some artifacts. This is exploited by various researchers in the forensic community to detect such malicious operations [10, 11, 12].

Gang Cao, Y. Zhao, R. Ni and X. Li propose two algorithms based on contrast enhancement via. Histogram peak / gap artifacts analysis. First algorithm detect global enhancement in both JPEG- compressed and uncompressed image and it identify by zero – height gap bin. Definition is shown in Diagram 2: Second algorithm identifies composite image. In this way, with a specific end goal to make the forged image contrast enhancement is performed to hide manipulation. [1]

Zhenhua Qu, Guoping Qiu, and Jiwu Huang proposed a method for detecting digital image splicing type of

forgery. The technique is based on OSF, feature extraction and hierarching classifier which used to detect splicing forgery. They clarify that a reliable progressive classifier can be prepared with the discriminative components separated from the initial couple of observations anticipated with a visual consideration demonstrate with edge sharpness as visual prompts and limiting grafting limits. A disadvantage of this is the edge sharpness signs now utilized will fall flat when covering measures, for example, obscure, is helpful. [13]

Lin et al. proposed an image forgery detection algorithm for splicing and copy move type of forgery. In algorithm firstly an image is converted into YcbCr colour space then detection process is performed separately for splicing and copy move type of forgery. For splicing detection, the image is divided into blocks of equal size and feature of image is extracted by DCT. And for copy – move detection SURF is used. The algorithm give better result for both the forgeries. [14]

Y. Wang et. al. proposed a dualistic sub image histogram equalization technique. This technique divides image into two sub images one is the dark one and another is the brighter one. This division is based on the area. Both parts cover equal area of image. That is why it is termed as histogram equalization [15].

Y.-S. Chiu et. al. introduced automatic weighting mean separated histogram equalization which improve histogram of image. This technique has two phases:

- Automatic histogram separation (AHS).
- Piecewise transform function (PTF).

In AHS image is separated based on the weighting function. In PTF sub histograms of sub images are equalized. The method is best suited for gray scale images and is not applicable for colored or RGB image [16].

T. Celik et. al. proposed a contextual and variation based contrast enhancement (CVC) performs inter pixel transformations to enhance the contrast of the image. For overall quality improvement of the image in this technique brightness and contrast both are increased. The main aim of this technique is to keep the overall content of the original image [17].

T. Bianchi et. al. proposed contrast enhancement forensic algorithm performs well under the presumption that histogram of an gray level unaltered picture shows a smooth bends. In genuine applications, for example, the Internet and versatile phones, digital pictures are regularly put away in the JPEG organize and even intensely packed with a center/low quality element (Q). It is outstanding that the low quality JPEG pressure normally creates blocking

relics, which may bring about unsmoothness and even locally thick pinnacle containers in the dim level histogram. In such cases, the current methodologies neglect to identify differentiate improvement in the beforehand low quality JPEG-compacted pictures, since the presumption of smoothness ends up noticeably disappointed. To take care of such an issue, propose to distinguish the worldwide complexity improvement not just in uncompressed or excellent JPEG-packed pictures, additionally in low quality ones. The primary procedure depends on the visually impaired ID of zero-tallness whole containers. Other than worldwide complexity improvement, the discovery of local difference upgrade is likewise huge. A significant application is to recognize the cut-and-glue kind of fabrication pictures, in which the difference of one source protest locale is upgraded to coordinate the rest. In spite of the fact that the composite picture made by upgrading single source area could be recognized, those improved in both source locales may not. In this, another strategy is proposed to recognize both single-source-improved and both-sourceenhanced composite pictures. Top/crevice example of the pixel esteem mapping connected to each source area is self-gained from the identified square insightful pinnacle/hole positions. At that point creation

limit is situated by identifying the irregularity between the position vectors in various districts [18].

VI. CONCLUSION

In this paper a survey is done on digital image forgery detection by using contrast enhancement technique because technique is used in perform image forgery. It is found that there are mainly three digital image forgeries which use to mislead people. By making it more realistic by using contrast enhancement any one can believe in fake evidence. These three forgeries are Copy-paste, Copy- move, splicing. Global contrast enhancement techniques result in clear change in histogram of the image. While local contrast enhancement or blocked approach result in less alteration in histogram. To keep histogram unaltered peak or gap based methods are introduced. It is also found that technique which proved efficient for gray scale image need not always perform well for RGB image and also in copy-move Properties like noise, color and texture don't modified and create trouble. Same in splicing when two images are combined and contrast enhancement is done, so it became more difficult to detect whether image is manipulated or not.

Table 1: Various contrast enhancement techniques.

Technique	Image type	Description
Global contrast enhancement	Applied to gray scale images	This technique involves global changes in the contrast and the main issue is that changes results in increase in peak and reduction in gaps in histogram.
Local contrast enhancement	Applied to gray scale images	Here image is divided into blocks and contrast enhancement is done on the block level.
Contrast enhancement with compression	Applied to RGB	Here image is first compressed and then contrast is enhanced. So that resulting histogram will have minimum changes.
Peak based global contrast enhancement	Applied to gray scale	Here number of peak in original image histogram and tampered image are kept same so as to avoid forgery detection.

Table 2: Comparative Study Of Existing Forgery Detection Methods

S.No	Paper title	Method used	Tampering detection type	Pro/cons	Publication year
1	Image enhancement based on equal area dualistic sub-image histogram equalization method[15]	Dualistic sub image histogram	Brightness of image	Does not detect composite image	1999
2	Detect Digital Image Splicing with Visual Cues[13]	OSF, a visual saliency guided feature extraction And hierarchical classifier	Splicing forgery	Doesn't give result for blur image	2009
3	Forensic detection of image manipulation	Non linear pixel	Detect local and	Fail to detect CE in	

	using statistical intrinsic fingerprints[19]	mapping and histogram equalization	global CE on image	JPEG- compressed image	2010
4	An integrated technique for splicing and copymove forgery image detection[14]	DCT-SURF	Copy-Move and spliced both region detected	Works well for both copy-move and splicing	2011
5	Contextual and variational contrast enhancement[17]	CVC(contextual and variation based CE)	Enhance contrast of the image	Keep overall content as original image	2011
6	Detection of non-aligned double JPEG compression based on integer periodicity maps[18]	Blockwise peak/gap	Copy - move forgery	Only for gray scale image	2012
7	Reverse engineering of double compressed images in the presence of contrast enhancement[9]	double-quantized DCT coefficient	Estimation of the quality factor and the amount of linear CE	Provide best result for both compressed and uncompressed image	2013

VII. REFERENCES

- [1] 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.
- [2] V. Tyagi, "Detection of forgery in images stored in digital form," Project report submitted to DRDO, New Delhi, 2010.
- [3] M.Ali Qureshi, M. Deriche, "A review on copy Move image forgery detection techniques" ResearchGate, 11, August , 2015.
- [4] H. Farid, "A survey of image forgery detection," IEEE Signal Process. Mag., Vol. 26, no. 2, pp. 16-25, Mar. 2009.
- [5] Kotkar V. A. and Gharde S. S, "review of various image contrast enhancement techniques" International Journal of Innovative Research in Science, Engineering and Technology Vol. 2, Issue 7, July 2013.
- [6] Nicholas Sia Pik Kong, Haidi Ibrahim, and Seng Chun Hoo, "A Literature Review on Histogram Equalization and Its Variations for Digital Image Enhancement" International Journal of Innovation, Management and Technology, Vol. 4, No. 4, August 2013.
- [7] Pujiono, Pulung N.A, I Ketut Eddy P., Mochamad H., "color enhancement of underwater coral reef images using contrast limited adaptive histogram equalization (clahe) with rayleigh distribution" The Proceedings of The 7th ICTS, Bali, May 15th-16th, 2013.
- [8] 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.
- [9] P. Ferrara, T. Bianchi, 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.
- [10] M. Kirchner and J. Fridrich, "On detection of median filtering in digital images," in Proc. SPIE, Electronic Imaging, Media Forensics and Security II, vol. 7541, San Jose, CA, USA, Jan. 2010, pp. 1–12.
- [11] C. Chen, J. Ni, and J. Huang, "Blind detection of median filtering in digital images: A difference domain based approach," IEEE Trans. Image Process., vol. 22, no. 12, pp. 4699–4710, Dec. 2013.
- [12] D. Mahajan, R. Ramamoorthi, and B. Curless, "A theory of frequency domain invariants: Spherical harmonic identities for BRDF/lighting transfer and image consistency," IEEE Trans. Pattern Anal. Mach. Intell., vol. 30, no. 2, pp. 197–213, Feb. 2008.
- [13] Zhenhua Qu, Guoping Qiu, and Jiwu Huang, "Detect Digital Image Splicing with Visual Cues", LNCS 5806, pp. 247–261, 2009.
- [14] S. D. Lin et al., "An integrated technique for splicing and copymove forgery image detection," in IEEE 4th International Congress on Image and Signal Processing (CISP), Vol. 2, 2011, pp. 1086_90.

[15] Y.Wang, Q. Chen, and B. Zhang, "Image enhancement based on equal area dualistic sub-image histogram equalization method," IEEE Trans. ConsumerElectron., vol. 45, no. 1, pp. 68–75, Feb 1999.

[16] Y.-S. Chiu, F.-C. Cheng, and S.-C. Huang, "Efficient contrast enhancement Using adaptive gamma correction and cumulative intensity distribution," in Proc. IEEE Conf. Syst. Man Cybern., Oct. 2011, pp. 2946–2950.

[17] T. Celik and T. Tjahjadi, "Contextual and variational contrast enhancement," IEEE Trans. Image Process. vol. 20, no. 12, pp. 3431–3441, Dec. 2011.

[18] T. Bianchi and A. Piva, "Detection of non-aligned double JPEG compression based on integer periodicity maps", IEEE Trans. Inf. ForensicsSecurity, vol. 7, no. 2, pp. 842–848, Apr. 2012.

[19] 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.

[20] Y.-S. Chiu, F.-C. Cheng, and S.-C. Huang, "Efficient contrast enhancement Using adaptive gamma correction and cumulative intensity distribution," in Proc. IEEE Conf. Syst. Man Cybern., Oct. 2011, pp. 2946–2950