A Novel Approach for Contrast Enhancement-Based Forensics in Digital Images

Kalyani Ravindra Chintawar
Department of Electronics & Communication Engineering
P.V.P.I.T. College of Engineering, Chandani Chawk, Bawdhan, Pune

Abstract

The contrast enhancement technique is specifically used to adjust the global brightness and contrast of images. Malicious users may perform local contrast enhancement for creating realistic composite images. In project, novel Approach for Contrast Enhancement Detection is used to detect the contrast enhancement in the images for verifying the originality and authenticity of the images. The new methodology involves two novel algorithms to detect the manipulations of contrast enhancement in digital images. One of the algorithms focuses on the detection of global contrast enhancement applied to the JPEG-compressed images, as these are widespread in real applications. The histogram artifacts incurred by the JPEG compression and also the pixel value mappings are analyzed theoretically and then distinguished by identifying the zero-height gap bins. Another algorithm helps to identify the composite image which is created by enforcing contrast adjustment on either single source region or both source regions. Then the positions of detected block wise peak/gap bins are clustered to recognize the contrast enhancement mappings which are applied to different source regions. At last, the consistency between regional artifacts is checked for discovering the image forgeries and also for locating the composition boundary. Matlab tool is used for evaluating the performance of these two algorithms on various images. The extensive experiment also verified the effectiveness and efficacy of the new methodology.
Keywords: JPEG compressed image, Histogram Artifacts, Peak/Gap bins, Contrast Enhancement, Contrast Detection

I. INTRODUCTION

Images are effective means of natural communication for humans due to their immediacy as well as the easy way of understanding the image content. Traditionally, there has been confidence in the integrity of visual data. Digital imaging has experienced tremendous growth in recent decades. Digital camera images have been used in a growing number of applications [1].

The rapid development of cheap and usable devices easily enables the acquisition of visual data. These devices improve the possibility of recording, storing and then sharing large amount of digital images. At the same time, the large availability of image editing software tools helps simply to alter the content of the images or to create new ones. Thus, the restriction of visual content's tampering and counterfeiting is no more to experts.

Now a day's, several software are available for manipulation of images to get the images which look like original images. Software allows creating photorealistic computer graphics that viewers can indistinguishable from photographic images or also generating hybrid generated visual content. Today, a visual digital object might go through several processing stages during its lifetime from its acquisition to its fruition. This is aimed at creating new content by mixing pre-existing material, enhancing the quality or also tampering with the content.

As a consecution of all previous facts, doctored images are appearing with a large number in various application fields. Thus, digital technology has started to erode the trust on visual content, so that apparently "seeing does no longer believe". The processing tools become more and more sophisticated which results in the worst of all the above issues. This highlights the demand of methods which will allow the reconstruction of the history of a digital image aimed to verify its truthfulness and assess its quality.

Two questions about the history and credibility of an image can be asked: was the acquired image from the device it is claimed to be sensed with? Is the image still depicting the captured original scene? Answering to those queries is relatively easy when the original image is known. Practically, no information can be assumed to be a known priori of the original image.

Images are as well used as authenticated proof for any crime. If these images do not remain genuine then it will create a problem. Detecting such types of forgeries became a serious problem now. Determining the originality of the image is a challenging task.

II. NEW APPROACH

The contrast enhancement technique is typically used to adjust the global brightness and also the contrast of digital images. Malicious users may perform contrast enhancement locally for creating composite image which looks like real image. Thus, it is important to detect contrast enhancement for verifying the originality and even the authenticity of the digital images. The proposed approach [7] includes two algorithms for the detection of contrast enhancement manipulations in digital images.

A. Method for Global Contrast Enhancement Detection:

The algorithm detects global contrast enhancement applied to both uncompressed and JPEG-compressed images, as these images are widespread in real applications. The histogram artifacts incurred by the JPEG compression and pixel value mappings are theoretically analyzed and then distinguished by identifying the zero-height gap fingerprints. Algorithm is explained as below [7]:

1) Get normalized gray level histogram h(x) of input image.
2) Detect the bin at k as a zero-height gap bin if it satisfies:

$$h(k) = 0$$
$$\min \{h(k-1), h(k+1)\} > \tau$$
$$\frac{1}{2_{w1}+1} \sum_{x=k-w1}^{k+w1} h(x) > \tau$$

The first sub-equation assures that the current bin is null. The second sub-equation defines a gap bin and keeps two neighboring bins larger than the threshold τ. To exclude the zero-height gap bins which may be detected incorrectly in histogram trail-ends, the average of neighboring $(2_{w1} + 1)$ bins should be larger than τ as constrained by the third sub-equation. Focus is on the detection of isolated zero-height gap bins and not on connected bins. Connected bins are rarely present in the middle of the histogram of image.

3) Count number of detected zero-height gap bins (Ng).

If the count is larger than the decision threshold, contrast enhancement is detected; otherwise no contrast enhancement is detected.

B. Identify Source Enhanced Composite Images:

This algorithm [7] identifies the composite image created by enforcing contrast adjustment on either single source region or both source regions. Positions of the detected block wise peak/gap bins are clustered to recognize the contrast enhancement mappings applied to various source regions. Consistency between artifacts of region is checked to discover the image forgeries and also to locate the composition boundary.

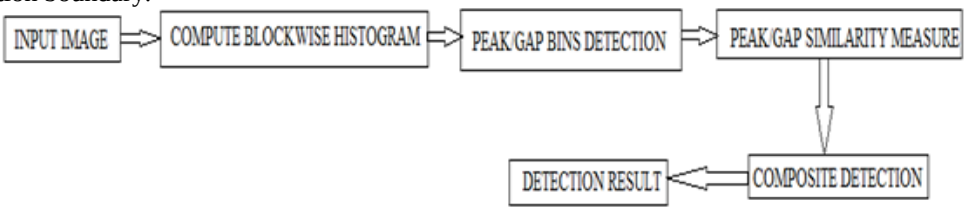


Fig. 1: Methodology for Identifying Source-Enhanced Composite Images [7]

The methodology for Identifying Source-Enhanced Composite Images in Fig.1. is explained as:

1) Block-wise Peak/Gap Bins Detection:

To locate composition, the test image is divided into non-overlapping blocks. The positional distribution of the peak/gap bins incurred by contrast enhancement is specific to the involved pixel value mapping. Such information of positions helps to identify different contrast enhancement manipulations. Consistency between the artifacts detected in various regions is checked to discover composite images.

2) Gap Based Similarity Measure:

Reference position vector is set for either source regions for discrimination purpose. Then each block is classified by the similarity between its position vector and the reference one.

3) Peak Based Similarity Measure:

As image block usually owns a narrow histogram, the theoretical gap bins might be not available in few blocks. Such blocks cannot be assigned to either source region merely based on the gap information. However, the narrow histogram with no gap bins might carry with peak bins. Such peak bins should be exploited for identifying the mappings.

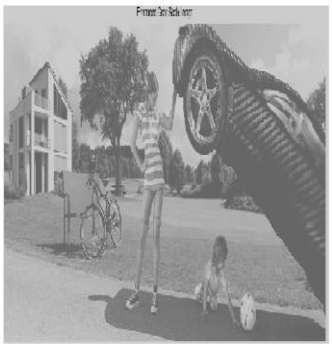
4) Similarity Maps Fusion for Composition Detection:

The block wise similarities are updated by averaging the available neighboring effective measurements before fusion. Resulting similarity can be generated by fusing the peak/gap based similarities. It actually detects whether the image contains contrast enhancement or not.

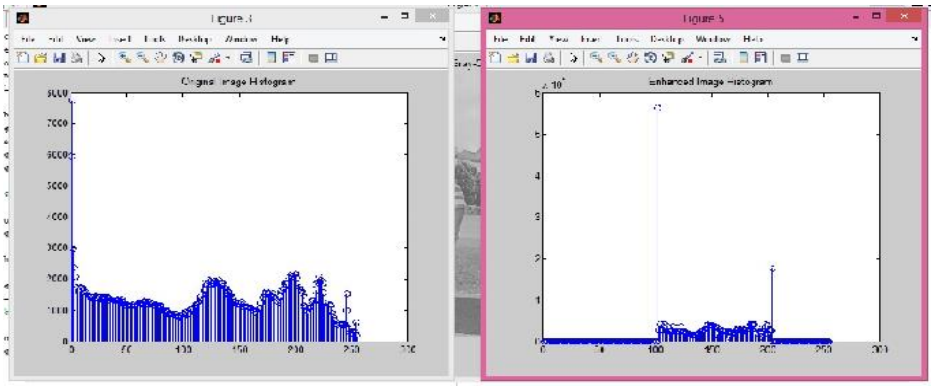
III. RESULT

Input Image

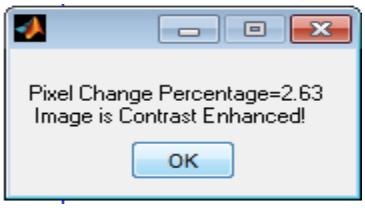
Input Gray-Scale Image



Enhanced Gray Image



Original Image Histogram Enhanced Image Histogram



Result shows that the enhanced image histogram is different from the original image histogram. Pixel Change factor is greater than the threshold i.e. 0.4. So, the contrast enhancement in JPEG compressed image is detected by making use of such pixel change differentiation.

IV. CONCLUSION

Two contrast enhancements based forensic algorithms are analyzed based on histogram peak/gap artifacts. The first algorithm is capable of detecting global contrast enhancement in both uncompressed and JPEG-compressed images. The zero-height gap bins are not present in compressed images since there is no distinct pixel value mapping which is applied to all pixels of the original image. Regular pixel value mapping exists in flat regions and not in other regions. Therefore, the zero-height gap feature is used for the detection of global contrast enhancement in both uncompressed and compressed images.

Second algorithm identifies the source-enhanced composite image created by enforcing contrast adjustment on either single source region or both source regions. Zero-height and zero-peak gap bins are used from the histogram of the input image for further processing to detect exactly where contrast enhancement is done in image.

ACKNOWLEDGEMENT

At the outset, I thank the Lord Almighty for the grace, strength and hope to make our endeavor a success. I thank my project guide Prof. N. N. Thune, for her boundless co-operation and help extended for the first project stage. I express sincere gratitude to her for her constant support and valuable suggestions without which the successful completion of the first project stage would not have been possible. Last but not the least; I thank all my classmates and especially my family members who in one way or another helped me in the successful completion of this project stage.

REFERENCES

[1] H. Farid, "Image forgery detection", IEEE Signal Process. Mag., vol. 26, no. 2, pp. 16–25, Mar. 2009.
[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] 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] 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.
[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] 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.
[7] Gang Cao, Yao Zhao, "Contrast Enhancement-Based Forensics in Digital Images", IEEE Transactions on Information Forensics and Security, vol. 9, no. 3, March 2014.