International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

Contrast Enhancement Based Image Manipulation Detection

Anju Gopinath[1]

[1]M.Tech Student, Dept. of Computer Science and Engineering,
M.G University, Mount Zion College of Engineering,
Kadammanitta, Pathanamthitta, Kerala, India

Abstract: ***Today photograph may be used for several beneficial purposes such as evidence in court. Contrast enhancement is used for adjusting the brightness and contrast of a digital image. Users may change the contrast locally and many image editing software's are now available. Malicious activities are also will happen, so verification is needed to detect the authenticity of the image. Here proposes two algorithms, first for detecting the contrast enhancement based manipulation involved in JPEG compressed images and the second one is used for detecting composite image.***

Keywords: Contrast enhancement, image forgery, digital image forensics, composite image

1. Introduction

By the immediate development in the field of editing in digital image, image manipulation becomes very easy. Sometimes it is legal and beneficial and sometimes it is suspicious. Some application such as crime related situations it is necessary to detect any suspicious activity will be happened and the history of that image. For verifying these, digital image forensic technique have been proposed.

Some forensic methods detects whether manipulation occurred or not but fails to detect which specific type of activity is done. Another category of forensic techniques detect specific image manipulations. The prior works focus on detecting different types of alterations, which can be broadly divided into two categories: 1) non-content-changing operations including resampling, compression, sharpening filtering, contrast enhancement and median filtering ; 2) content changing operations, i.e., composition and splicing.

The previous contrast enhancement forensic algorithm performs well under the assumption that the gray level histogram of an unchanged image exhibits a smooth curves. In real applications, such as the Internet and mobile phones, digital images are often stored in the JPEG format and even heavily compressed with a middle/low quality factor (Q). It is well-known that the low quality JPEG compression usually generates blocking artifacts, which might cause unsmoothness and even locally dense peak bins in the gray level histogram. In such cases, the existing approaches fail to detect contrast enhancement in the previously low quality JPEG-compressed images, since the assumption of smoothness becomes dissatisfied. To solve such a problem, propose to detect the global contrast enhancement not only in uncompressed or high quality JPEG-compressed images, but also in low quality ones. The main strategy relies on the blind identification of zero-height gap bins. Besides global contrast enhancement, the detection of local contrast enhancement is also significant. A valuable application is to identify the cut-and-paste type of forgery images, in which the contrast of one source object region is enhanced to match the rest. Although the composite image created by enhancing single source region could be identified, those enhanced in both source regions may not. In this, a new method is proposed to identify both single-source-enhanced and both-source-enhanced composite images. Peak/gap pattern of the pixel value mapping applied to each source region is self-learned from the detected block wise peak/gap positions. Then composition boundary is located by detecting the inconsistency between the position vectors in different regions.

2. Related Works

Generally, contrast enhancement inherently a pixel value mapping y =m(x), where m(.) is the mapping function, x,y = 0,1,2,...,255 are the pixel gray level before and after mapping respectively. The histogram of unrelated images typically conforms to a smooth envelope, while that of enhanced images presents peak/gap artifacts as indicated in Figure 1(b) and (c).

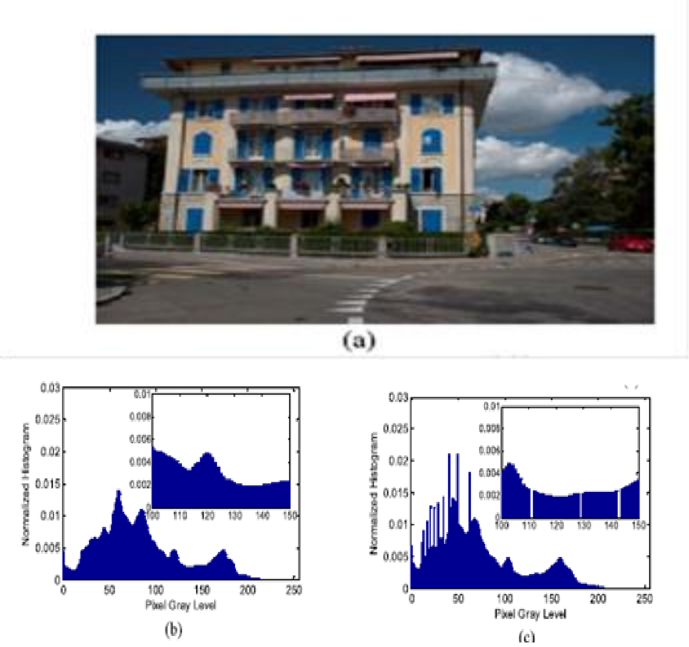

Figure 1: Gray level histogram of contrast-enhanced images. (a) Raw image; (b) the histogram of the raw image and (c) enhanced image histogram.

In the global contrast enhancement detection method is applied to image blocks for detecting local enhancement. In practice, the two source images used for creating a composite image may have different color temperature or luminance contrast. In order to make the composite image more realistic, contrast enhancement is typically performed in one or both source regions. In such cases, the composite image created by applying contrast enhancement to a single source region can be detected by the prior method. However, if contrast enhancement is enforced in both the source regions, such method may fail since all blocks are detected as enhanced ones.

3. Global Contrast Enhancement Detection

Here proposes an efficient algorithm which detects the enhancement in both uncompressed and previously JPEG-compressed images.

The proposed system contains two different methodologies for the detection of global and local contrast enhancement in an image. The methodologies are:

Identifying Globally Contrast-Enhanced Images:

Previous algorithms work well under the assumption that, gray level histogram of unaltered images shows smoothness while that of contrastly 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 the proposed method solves this problem. Algorithm detects the contrast based 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.

Identifying locally contrast enhanced images:

An important application is to identify cut-and-paste type of suspected images, in which the contrast of one source region is shifted to match the next. In 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 the proposed work, a new method was proposed to identify not only single source enhance but also both source enhanced cut-and-paste type of forged images.

The methods used in this 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.+

Here proposes an efficient algorithm which detects the enhancement in both uncompressed and previously JPEG-compressed images. The algorithm is as follows.

1) Retrieve the image's normalized gray level histogram, say as h(x).

2) Identify the bin at k as a zero-height gap bin and check if it satisfies:

$$\begin{cases} h(k) = 0 \\ \min\{h(k-1), h(k+1)\} > \tau \end{cases} \qquad (1)$$

Here, the first sub-equation assures that the current bin is null. To define a gap bin, the second sub-equation keeps two neighboring bins larger than the threshold τ. To exclude the zero-height gap bins this may be incorrectly detected in histogram trail-ends.

3) Count the number of detected zero-height gap bins from equation, denoted by Ng. If it is larger than the decision threshold, then contrast enhancement is encountered, else not.

4. Identify Source Enhanced Composite Image

Here an algorithm is proposed to identify the source-enhanced composite image created by enforcing contrast adjustment on either single or both source regions. Figure 2 describes the flow chart of the technique. Since positional distribution of the peak/gap bins incurred by contrast enhancement is unique to the involved pixel value mapping, such positional information could serve as fingerprinting feature for identifying different contrast enhancement manipulations. Consistency between the peak/gap artifacts detected in different regions is checked for discovering composite images.

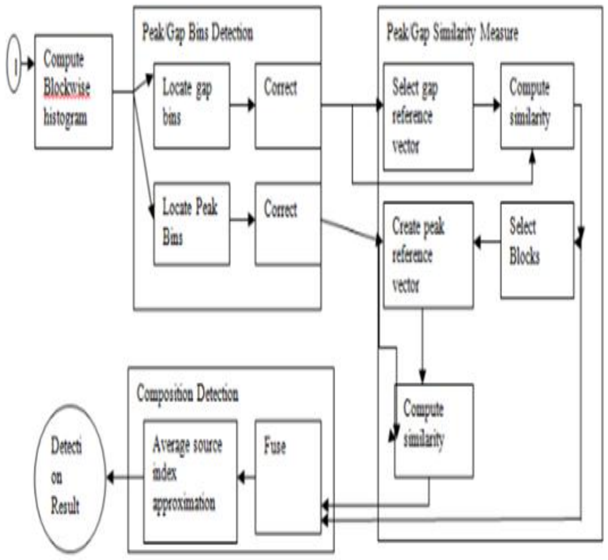

Figure 2: Flow Chart

Gap Bins Location: The zero-height gap bins are detected. The position of detected gap bins is labelled as Vig = [Vig (0), Vig (1),…, Vig (k),…, Vig (255)], where Vig (k) = 1, if the bin at k is a gap; Vig (k) = 0, otherwise.

Peak Bins Location: Peak bins which behave as impulse noise can be located by median filtering. Specifically, the gap bins are first filled with the average of neighboring bins, then median filtering is applied to the gap-filled histogram. Then the filtered histogram possesses a smooth contour. Lastly, peak positions are located by thresholding the difference between the gap-filled histogram and its filtered version.

5. Conclusion and Future Works

Here proposed two contrast enhancement based forensic algorithms based on histogram peak/gap artifacts analysis. First, extended to detect the global contrast enhancement in both uncompressed and already JPEG-compressed images. Second, proposed a new method to find out both source enhanced composite image, which not validated the previous forensics methods. The composition boundary was accuratelylocated by detecting the inconsistency between detected blockwise peak/gap positional distributions.

The proposed contrast enhancement based image manipulation methods could work particularly well when contrast enhancement is performed as the last step of manipulation. In the future work, I would try to improve the robustness of such methods against post processing, such as JPEG compression. It is also essential to enhance the security rather than forensics.

References

[1] S. Bayram, Avcuvas.I.and N.Menon(2006) “Image Manipulation Detection”in J. Electron. Imag., vol. 15, no. 4, pp. 04110201–04110217.
[2] T. Bianchi and A. Piva, “Detection of non-alligned double JPEG Compression,” IEEE Trans. Inf. Forensics Security, vol.7, no. 2 pp. 842-848, in Apr 2012
[3] H. Cao and A. C. Kot, “Manipulation detection on image patches using Fusion Boost,” IEEE Trans. Inf. Forensics Security, vol. 7, no. 3, pp. 992–1002, Jun. 2012.
[4] G. Cao, Y. Zhao, R. Ni, and A. C. Kot, “Unsharp masking sharpening detection via overshoot artifacts analysis,” IEEE Signal Process. Lett.,vol. 18, no. 10, pp. 603–606, Oct. 2011.
[5] G. Cao, Y. Zhao, and R. Ni, “Forensic estimation of gamma correctionin digital images,” in Proc. 17th IEEE Int. Conf. Image Process.,Hong Kong, 2010, pp. 2097–2100.
[6] C. Chen, J. Ni, and J. Huang, “Blind detection of median filteringin digital images: A difference domain based approach,” IEEE Trans.Image Process., vol. 22, no. 12, pp. 4699–4710, Dec. 2013.
[7] J. Fan, H. Cao, and A. C. Kot, “Estimating EXIF parameters basedon noise features for image manipulation detection,” IEEE Trans. Inf.Forensics Security, vol. 8, no. 4, pp. 608–618, Apr. 2013.
[8] H. Farid, “Image forgery detection,” IEEE Signal Process. Mag., vol. 26,no. 2, pp. 16–25, Mar. 2009.
[9] 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.
[10] B. Mahdian and S. Saic, “A bibliography on blind methods for identifying image forgery,” Image Commun., vol. 25, no. 6, pp. 389–399,Jul. 2010.
[11] A. C. Popescu and H. Farid, “Exposing digital forgeries by detectingtraces of resampling,” IEEE Trans. Signal Process., vol. 53, no. 2,pp. 758–767, Feb. 2005.
[12] M. C. Stamm and K. J. R. Liu, “Forensic detection of image manipulationusing statistical intrinsic fingerprints,” IEEE Trans. Inf. ForensicsSecurity, vol. 5, no. 3, pp. 492–506, Sep. 2010.
[13] A. Swaminathan, M. Wu, and K. J. R. Liu, “Digital image forensics viaintrinsic fingerprints,” IEEE Trans. Inf. Forensics Security, vol. 3, no. 1,pp. 101–117, Mar. 2008.

Author Profile

Anju Gopinath received the B.Tech degree in Computer Science and Engineering from Mahatma Gandhi University, Kerala at Caarmel Engineering College Ranni-Perunad in 2012 and now she is doing her M.Tech degree under M.G university, Kerala in Mount Zion College of Engineering.