IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 16, Issue 5, Ver. IX (Sep-Oct. 2014), PP 01-07
www.iosrjournals.org

Digital Image Forgery Detection by Contrast Enhancement

Remya S.

***Abstract**: For decades, photographs have been used to document space-time events and they have often served as evidence in courts. Today, powerful digital image editing software makes image modifications straightforward. This undermines our trust in photographs and, in particular, questions pictures as evidence for real-world events. Contrast enhancement is mainly to adjust the brightness globally. Users may also perform local contrast enhancement for creating a realistic composite image. Most latest technology in the literature uses two algorithms to find the contrast enhancement for the manipulation of digital imagees. First algorithm focus on the detection of global contrast enhancement applied to previously JPEG compressed images. Here images are converted to non-overlapping blocks ie histogram of images, then gap/peak detection of blocks are performed. Locate the gap and peak bins. Pixel value mappings are analyzed theoretically, and difference between the pictures are obtained by identifying the zero-height gap fingerprints. Second method is used to identify the composite image created by enforcing contrast adjustment on any of the source regions/over the entire region of the image. This is followed by finding out the positions of the peak/gap bins, and clustering them for identifying the contrast enhancement applied to different source regions. Finally check for the similarity between peak/gap bins reference vectors calculated for both forged region and unforged region.If it is found to be dissimilar then the image is treated as a forged one.*

***Index Terms:** Contrast enhancement, image forgery.*

I. Introduction

IMAGE forensics is a multidisciplinary science aiming at acquiring important information on the history of digital images,including the acquisition chain ,the coding process, and the editing operators. The extraction of such data can be exploited for different purposes, one of the most interesting is the verification of the trustworthiness of digital data. Image forensic techniques work on the assumption that digital forgeries, although visually imperceptible, alter the underlying statistics of an image. These statistical properties can be interpreted as digital fingerprints characterizing the image life-cycle, during its acquisition and any successive processing. One of the tasks of image forensics is then to verify the presence or the absence of such digital fingerprints, similar to intrinsic watermarks, in order to uncover traces of tampering.

At present, an image forger can easily alter a digital image in a visually realistic manner.As a result, the field of digital image forensics has been born. Identification of images and image regions which have undergone some form of manipulation or alteration.No universal method of detecting image forgeries exists.Different techniques, with their own limitations. Some techniques are Lighting Angle Inconsistencies, Inconsistencies in chromatic aberration, Absence of Color Filter Array (CFA) interpolation induced correlations,Classifier based approaches. When assessing the authenticity of an image, forensic investigators use all available sources of tampering evidence.Among other telltale signs, illumination inconsistencies are potentially effective for splicing detection: from the viewpoint of a manipulator, proper adjustment of the illumination conditions is hard to achieve when creating a composite image.

Contrast enhancement techniques in the first and third subgroups often use multiscale analysis to decompose the image into different bands and enhance desired global and local frequencies. These techniques are computationally complex but enable global and local contrast enhancement at the same time by enhancing the appropriate scales. Several contrast enhancement techniques have been introduced to improve the contrast of an image.These techniques can be broadly categorized into two groups: direct methods and indirect methods. Direct methods define a contrast measure and try to improve it. Indirect methods, on the other hand, improve the contrast through exploiting the under-utilized.

Contrast enhancement techniques in the second subgroup modify the image through some pixel mapping such that the histogram of the processed image is more spread than that of the original image.

II. Related Work

1. Detection of Nonaligned Double JPEG Compression Based on Integer Periodicity Maps proposed a simple yet reliable algorithm to detect the presence of nonaligned double JPEG compression (NA-JPEG) in com- pressed images is proposed. The method evaluates a single feature based on the integer periodicity of the blockwise discrete cosine transform (DCT) coefficients when the DCT is computed according to the grid of the previous JPEG compression. Even if the proposed feature is computed relying only on DC coefficient statistics, a simple threshold detector can classify NA-JPEG images with improved accuracy with respect to existing

methods and on smaller image sizes, without resorting to a properly trained classifier. Moreover, the proposed scheme is able to accurately estimate the grid shift and the quantization step of the DC coefficient of the primary JPEG compression, allowing one to perform a more detailed analysis of possibly forged images.

2. Digital Image Forensics via Intrinsic Fingerprints proposed a a new methodology for the forensic analysis of digital camera images. The proposed method is based on the ob- servation that many processing operations, both inside and outside acquisition devices, leave distinct intrinsic traces on digital images, and these intrinsic fingerprints can be identified and employed to verify the integrity of digital data. The intrinsic fingerprints of the various in-camera processing operations can be estimated through a detailed imaging model and its component analysis. Further processing applied to the camera captured image is modelled as a manipulation filter, for which a blind deconvolution technique is applied to obtain a linear time-invariant approximation and to estimate the intrinsic fingerprints associated with these postcamera operations. The absence of camera-imposed fingerprints from a test image indicates that the test image is not a camera output and is possibly generated by other image production processes. Any change or inconsistencies among the estimated camera-imposed fingerprints, or the presence of new types of fingerprints suggest that the image has undergone some kind of processing after the initial capture, such as tampering or steganographic embedding. Through analysis and extensive experimental studies, this paper demonstrates the effectiveness of the proposed framework for non- intrusive digital image forensics. None of the histograms contains sudden zeros or impulsive peaks.Do not differ greatly from the histogram's envelopeTo unify these properties, pixel value are described as interpolatably connected. A number of image processing operations can be specified entirely by a pixel value mapping.Leave behind distinct, forensically significant artifacts, which we will refer as *intrinsic fingerprint.*

3. Estimating EXIF Parameters Based on Noise Features for Image Manipulation Detection proposed a novel technique to cor- relate statistical image noise features with three EXchangeable Image File format (EXIF) header features for manipulation de- tection. By formulating each EXIF feature as a weighted sum of selected statistical image noise features using sequential floating forward selection, the weights are then solved as a least squares solution for modeling the correlation between the intact image and the corresponding EXIF header. Image manipulations like brightness and contrast adjustment can affect these noise fea- tures and lead to enlarged numerical difference between each actual and its estimated EXIF feature from the noise features. By using the numerical difference as a manipulation indicator, we achieve excellent performance in detecting common brightness and contrast adjustment. Based on cameras of different brands, our manipulation detection is also demonstrated to work well in a blind mode, where the camera brand/model source is unavailable. Several detection examples suggest that our model can be applied in detecting real-world forgeries.

4. Forensic Estimation And Reconstruction Of A Contrast Enhancement Mapping proposed a method for detecting image manipulation. Once image alterations have been identified, the next logical forensic task is to recover as much information as possible about the unaltered version of image and the operation used to modify it. Previous work has dealt with the forensic detection of contrast enhancement in digital images. In this paper propose an iterative algorithm to jointly estimate any arbitrary contrast enhancement mapping used to modify an image as well as the pixel value histogram of the image before contrast enhancement. To do this, we use a probabilistic model of an image's pixel value histogram to determine which histogram entries are most likely to correspond to contrast enhancement artifacts. Experimental results are presented to demonstrate the effectiveness of our proposed method.

5. A Histogram Modification Framework and Its Application for Image Contrast Enhancement proposed a framework. In this framework, contrast enhancement is posed as an optimization problem that minimizes a cost function. Histogram equalization is an effective technique for contrast enhancement. However, a con- ventional histogram equalization (HE) usually results in excessive contrast enhancement, which in turn gives the processed image an unnatural look and creates visual artifacts. By introducing specifically designed penalty terms, the level of contrast enhancement can be adjusted; noise robustness, white/black stretching and mean-brightness preservation may easily be incorporated into the optimization. Analytic solutions for some of the important criteria are presented. Finally, a low-complexity algorithm for contrast enhancement is presented, and its performance is demonstrated against a recently proposed method.

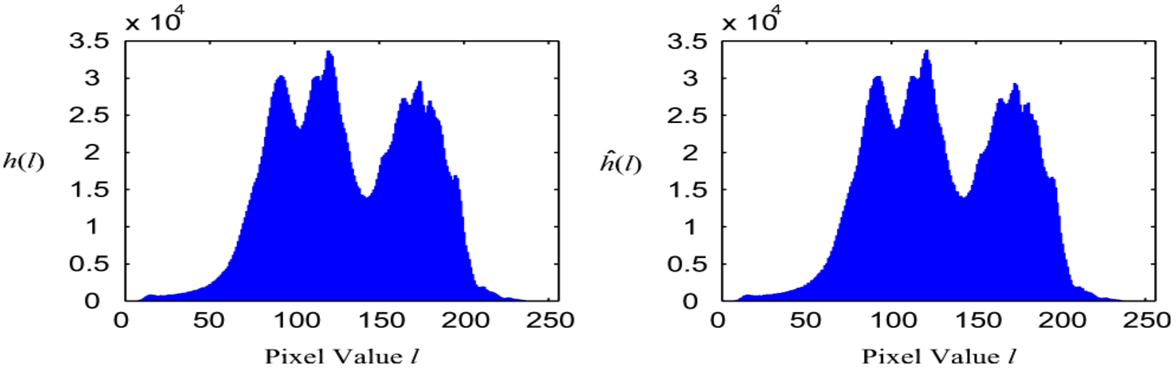
III. Contrast Enhancement

Histogram-based contrast enhancement techniques utilize the image histogram to obtain a single-indexed mapping T[n] to modify the pixel values.1 In HE and other histogram-based methods, mapping function is obtained from the histogram or the modified histogram, respectively.HE finds a mapping to obtain an image with a histogram that is as close as possible to a uniform distribution to fully exploit the dynamic range. A histogram,,can be regarded as an un-normalized discrete probability mass function of the pixel intensities. The normalized histogram of an image gives the approximate probability density function (PDF) of its pixel intensities. Then, the approximate cumulative distribution function (CDF),c[n], is obtained from p[n].The mapping function is a scaled version of this CDF. HE uses the image histogram to obtain the mapping function; whereas, other histogram-based methods obtain the mapping function via the modified histogram. The mapping function in the discrete form is given as

$$T[n] = \left[(2^B - 1)\sum_{j=0}^{n} p[j] + 0.5\right] \qquad (1)$$

where B is the number of bits used to represent the pixel values. Although the histogram of the processed image will be as uniform as possible, it may not be exactly uniform because of the discrete nature of the pixel intensities. It is also possible to enhance the contrast without using the histogram. Black stretching and white stretching are simple but effective techniques used in consumer-grade TV sets. Black stretching makes dark pixels darker, while white stretching makes bright pixels brighter. This produces more natural looking black and white regions; hence, it enhances the contrast of the image. Linear black and white stretching can be achieved by the mapping ofa typie. Right: Approximation of the histogram at left by sequentially removing then interpolating the value of each histogram entry

Fig. 1. Left: Histogram of a typical image. Right: Approximation of the histogram at left by sequentially removing then interpolating the value of each histogram entry.



$$T[n] = \begin{cases} n \times s_b, & n \le b \\ n \times g[n], & b < n < \omega \\ \omega + (n - \omega) \times s_{\omega,} & \omega \le n \end{cases} \qquad (2)$$

where b is the maximum gray-level to be stretched to black and ω is the minimum gray-level to be stretched to white, g[n] is any function mapping the intensities in between, and black and white stretching factors both of which are less than one.

IV. Proposed Method

Proposed method deals with peak/gap bins detection method and peak/gap similarity measurement method.Fig 2. Represents the flow chart of the proposed method.

A. *Peak/Gap bins detection Method*

First divide the images into blocks, then locate gap bins and peak bins The histogram peak/gap artifacts incurred by the JPEG compression and pixel value mappings are analyzed theoretically, and distinguished by identifying the zero-height gap fingerprints,correct the peak/gap values for selecting reference vector.

B. *Peak/Gap bins similarity measurement Method*

The positions of detected blockwise peak/gap bins are clustered for recognizing the contrast enhancement mappings applied to different source regions. The consistency between regional artifacts is checked for discovering the image forgeries and locating the composition boundary.Select gap reference vector from the corrected peak/gap bins. Compute the similarity of peak/gap bins from the reference vectors. Original image value is stored in the source index. Compare the index values of the original images and the blocks of images and detect result.

C. *Histogram*

h(l) can be generated by creating L equally spaced bins which span the range of possible pixel values.Tabulate the number of pixels whose value falls within the range of each bin.Gray levels values in P = {0, … , 255}, Color values in P^3Pixel value histogram uses 256 bins. None of the histograms contains sudden zeros or impulsive peaks.Do not differ greatly from the histogram’s envelope.To unify these properties, pixel value are described as interpolatably connected.Any histogram value h(l) can be aproximated by ĥ(l).Each value of ĥ has been calculated by removing a particular value from h then interpolating this value using a cubic spline.Little difference from h and ĥ.

D. Detection of Globally Applied Contrast Enhancement

Contrast Enhancement operations seek to increase the dynamic range of pixel values within images.Usually nonlinear mappings.Consider only monotonic pixel value mappings.Thereby,disconsidering simple reordering mappings.All contrast enhancement mappings result in an increase in energy.This energy is related to the intrinsic fingerprint.Expected DFT's to be strongly low-pass signal.Therefore, the presence of energy in the high frequency regions is indicative of contrast enhancement.Contrast enhancement will cause isolated peaks and gaps in the histogram.Database of different unaltered images, taken in different resolutions and light conditions.The green color layer created the grayscale images.γ ranging from 0.5 to 2.04092 grayscale images.Solution to the problem is g(l)=p(l)h(l).

$$P(I)=\begin{cases} \frac{1}{2}-\frac{1}{2}\cos\left(\frac{\Pi l}{N_p}\right), & l \le N_p \\ \frac{1}{2}+\frac{1}{2}\cos\left(\frac{\Pi(l-255+Np)}{N_p}\right), & l \ge 255-N_p \\ 1, & else \end{cases} \qquad (3)$$

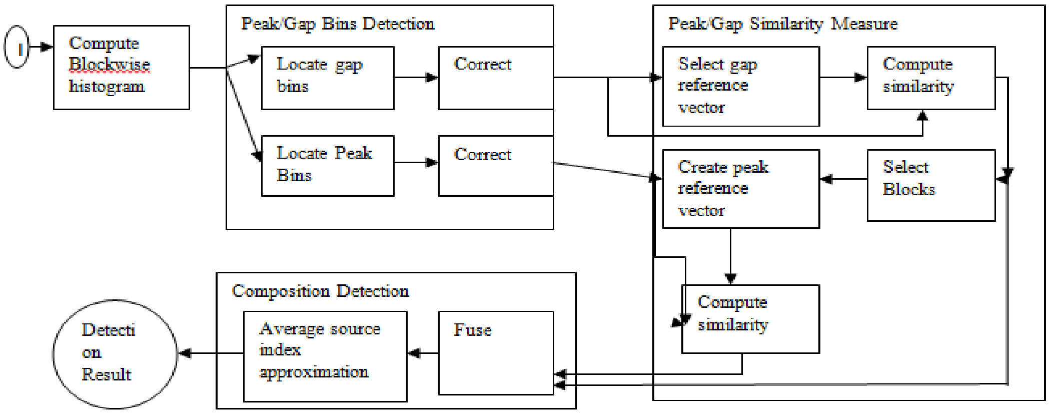


Fig 2.Flowchart of the composite image detection technique

Measuring the energy by the equation(4)

$$E=\frac{1}{N}\sum_k \setminus \beta(k)G(k)| \qquad (4)$$

$$B(k)=\begin{cases} 1, c \le k \le 128 \\ 0, else \end{cases}$$

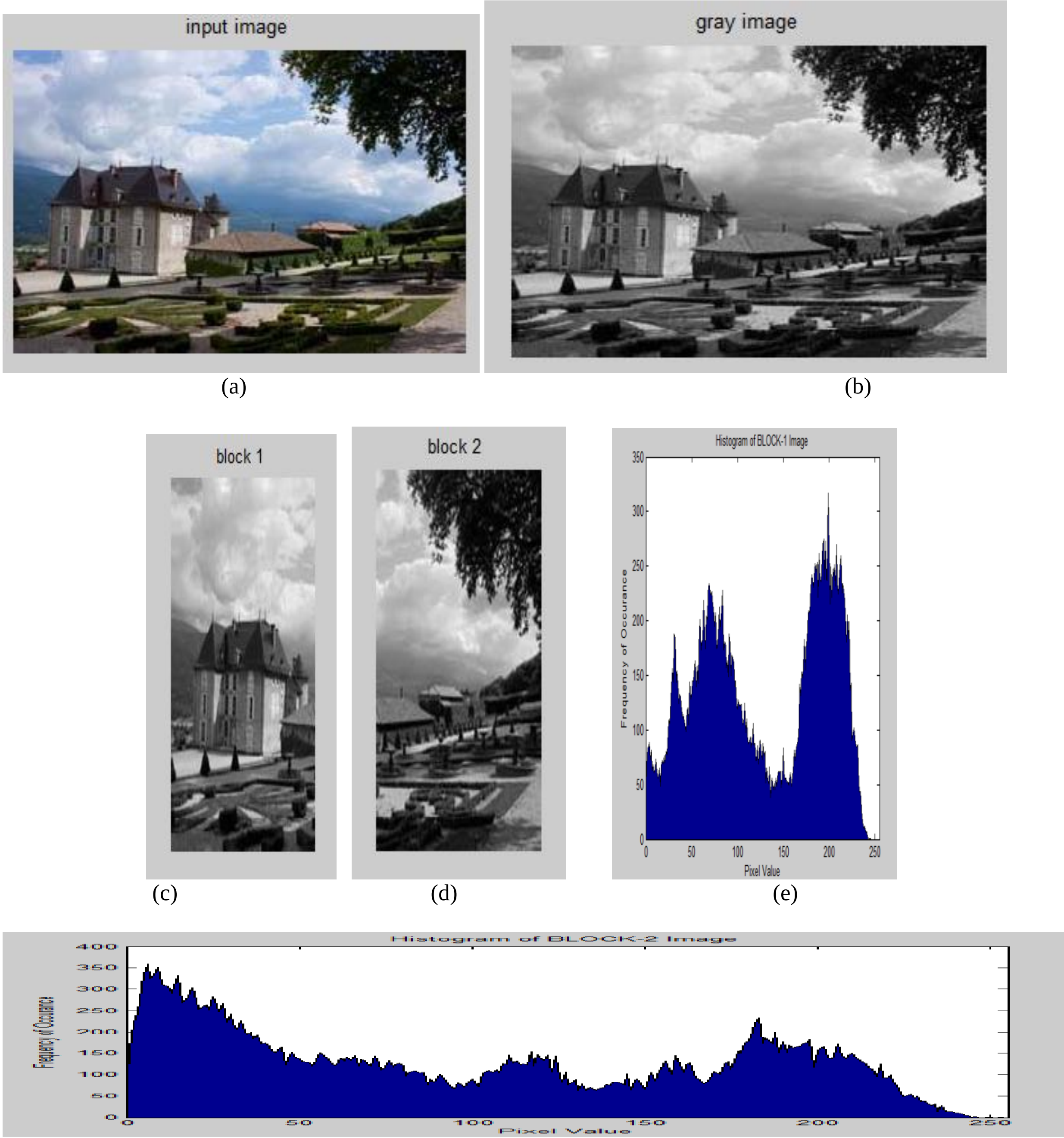
E. Detection of Locally Applied Contrast Enhancement

Defined as applying a contrast mapping to a set of contiguous pixels within an image.Can identify cut-and-paste forgeries.To detect it, the image is divided in smaller blocks and the global technique is applied to the blocks.Who small(and big!?) are these blocks? Test different unaltered images and use γ ranging from 0.5 to 0.9.Blocks of size 200x200, 100x100, 50x50, 25x25, and 20x20.The contrast enhancement can be reliably detected using testing blocks sized 100x100 pixels with a P**d** of at least 80% in every case at a P**fa** of 5%.When γ ranged from 1.0 to 2.0, the P**d** was of 95% at a P**fa** of 5%.

V. Experimental Results And Discussions

To verify the efficacy of our proposed forensic methods, extensive experiments are performed in three test image setsTo evaluate the proposed composition detection scheme, we first test the example forged image shown in Fig. 3. If contrast enhancement is enforced in both regions, such a method may fail since all bocks are detected as enhanced ones. As shown in Fig. 3, a composite image (c) is created by copying a region of the source image (a) and pasting onto another source image4 (a). For matching the regional contrast perception, the two source regions are enhanced by different mappings using the 'Curve' tool in AdobePhotoshop. Fig 3(a) represents the original image,convert the image into gray image by using gray world conversion,fig 3(b) shows the gray conversion of the image.dividing the image into blocks,fig 3(c)and 3(d) shows block representation of the original image.Find out the histogram of each blocks.Fig 3(e),(f)represents the histogram of each block.Fig

4(a) represents the composite image is created by copying a region of the original image.Convert the image into gray image by using gray world conversion of the image,dividing the image into blocks,fig 4(b)represents the gray conversion of the image.Find out the histogram of each block.Fig 4(c)(d)represents the blocks of the composite image,Fig(e)(f) represents the histogram of the images.Compare the histogram of the original image and composite image.From the histogram values can identify the original image and enhance image.Histogram modifications techniques,such as histogram equalization and the intelligent approaches,are the most widespread indirect contrast enhancement techniques. In such techniques, a target pixel value mapping is generally pre-computed and then applied to the global image for adjusting contrast automatically. The zero-height gap artifacts would still be yielded so that such contrast enhancement can be detected. Histogram equalization effectively increases the dynamic range of an image's pixel values by subjecting them to a mapping such that the distribution of output pixel values is approximately uniform. In order to identify it, we calculate the "uniformity" of the histogram.



(a) (b)

(c) (d) (e)

(f)

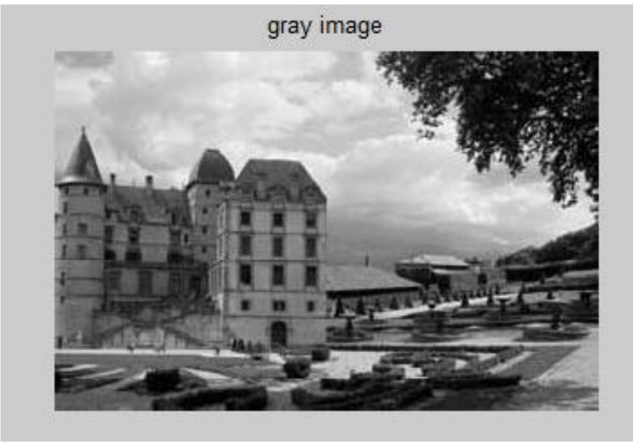
Fig 3(a).Original image,(b)Gray image(c)Block1of the image(d)Block2 of the image(e)Histogram of block1(f)Histogram of block (2)

input image

(a)

block 1

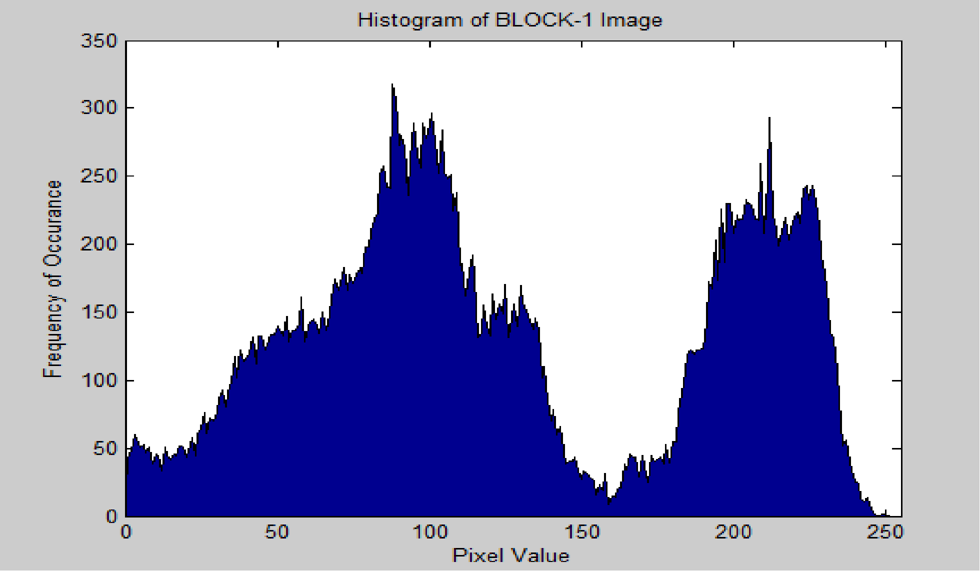
(c)


gray image

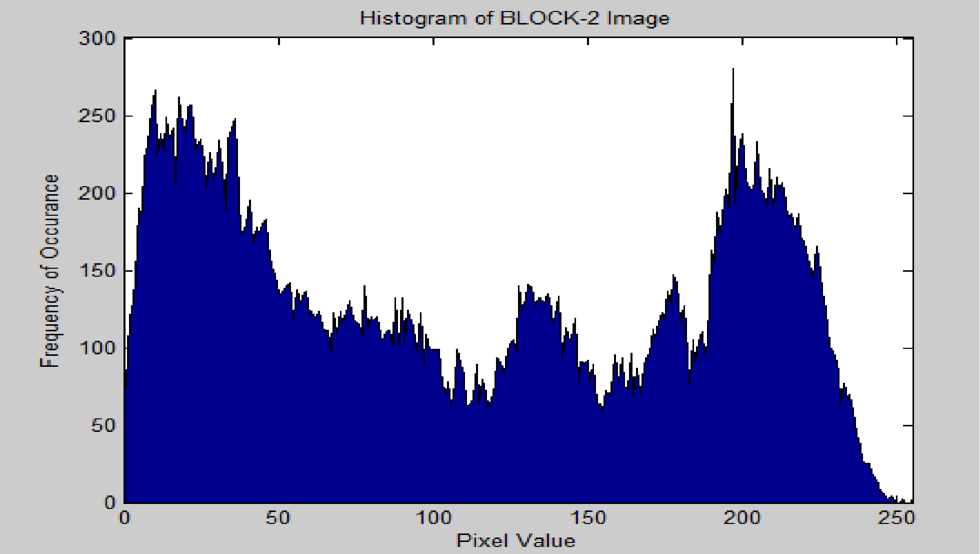
(b)

block 2

(d)


Histogram of BLOCK-1 Image
Frequency of Occurance
350
300
250
200
150
100
50
0
0
50
100
150
200
250
Pixel Value

(e)



(f)

Fig 4(a).Enhanced image,(b)Gray image(c)Block1of the image(d)Block2 of the image(e)Histogram of block1(f)Histogram of block (2)

VI. Conclusion

In this paper, we proposed two contrast enhancement based forensic algorithms via histogram peak/gap artifacts analysis. First, we extended to detect the global contrast enhance- ment in both uncompressed and previously JPEG-compressed images. The zero-height gap bins in gray level histograms were novelly exploited as identifying features. Large-scale experiments showed that our contrast enhancement detector achieved high performance, i.e., Pd = 100% at Pfa = 1%. Second, we proposed a new method to discover the both- source-enhanced composite image, which invalidated the previous detection methods. The composition boundary was accurately located by detecting the inconsistency between detected blockwise peak/gap positional distributions. The tests on both a specific composite image and quantitative synthetic samples verified the efficacy of our proposed composition detector.

References

[1] H. Farid, “Image forgery detection,” IEEE Signal Process. Mag., vol. 26, no. 2, pp. 16–25, Mar. 2009.

[2] 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.

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

[4] 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.

[5] 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.

[6] J. Fan, H. Cao, and A. C. Kot, “Estimating EXIF parameters based on noise features for image manipulation detection,” IEEE Trans. Inf. Forensics Security, vol. 8, no. 4, pp. 608–618, Apr. 2013.

[7] A. C. Popescu and H. Farid, “Exposing digital forgeries by detecting traces of resampling,” IEEE Trans. Signal Process., vol. 53, no. 2, pp. 758–767, Feb. 2005.

[8]. Gang Cao and Yao Zhao,”Contrast Enhancement based Forensics in digital images”,IEEE Trans.Information forensics and security,vol.9,no.3,March 2014.