ISSN: 2321-7782 (Online)
Volume 3, Issue 4, April 2015
International Journal of Advance Research in Computer Science and Management Studies
Research Article / Survey Paper / Case Study
Available online at: www.ijarcsms.com

Image Forensics Based on Fingerprint Analysis

Boby Kurian
Dept. of Electronics and Communication Engineering
College of Engineering, Cherthala
Kerala, India

Abstract: ***Most of the image alteration techniques will leave behind certain distinct, traceable artifacts or "fingerprints" in the output image. Because these artifacts or fingerprints are often unique to each operation, various tests or analysis need to be carried out to find the presence of these manipulations. In this paper two types of artifacts are used to check the authenticity of digital images. The first one is the statistical traces introduced by contrast enhancement in an image's pixel value histogram. This is very useful in the case of large size images and high quality JPEG compressed images. The second one is the inconsistencies in the Blocking Artifact Grid which is used in the case of low quality JPEG compressed images. Both these techniques are used to find the presence of cut and paste forgery in an image.***

Keywords: Image forensics, contrast enhancement, fingerprint analysis, JPEG compression, blocking artifact grid.

I. INTRODUCTION

In recent years, digital images are extensively used in the field of news media, law enforcement, social networking, military, etc. At the same time, the availability of a wide range of image editing software has made it an easy task even for ordinary people to introduce suitable changes into image content. These manipulations can be either content preserving such as contrast enhancement, compression, sharpening filtering, etc. or content changing operations such as splicing , cut and paste, etc.When somebody introduces some malicious changes to the content of an image we call it as an image forgery. In such situations digital image forensics plays a vital role. Its aim is to verify the authenticity and integrity of the content of a digital image.

Image forensic techniques can be broadly divided into two. They are known as (1) Active methods and (2) Passive methods [2]. Active forensic methods make use of digital signatures and watermarking techniques. The watermark or the digital signature is added to the image at the source side and at the receiving side if it is satisfactorily recovered, the image is considered as an original one. Any change in its content will be considered as the sign of an image alteration. On the other hand, passive methods do not use any additional information. Instead they blindly ensure the authenticity of digital images. The passive forensic methods are classified as pixel–based, format-based, camera-based, physics–based and geometric-based techniques [1]. This paper introduces some pixel based methods which can be used in the case of a wide variety of digital images.

It is to be noted that most of the image editing operations will leave behind certain unique marks or fingerprints somewhere in the image content. By properly exploring the presence of these fingerprints one can arrive at a conclusion that whether certain manipulations are done or not. It is seen that most of the manipulators will do some sort of contrast adjustment globally or locally in order to produce some desirable results. Especially when somebody tries to create a composite image by pasting a suitably selected region on to another location (cut and paste forgery), there is a need for adjusting the brightness and contrast of the selected region in order to match the background region.

It is given in [3] that the histogram of an unaltered image possess a smooth contour .Color filter array (CFA) interpolation ,the presence of sensor noise and the continuity of color values seen in most of the natural world images are the reasons given

to justify it. On the other hand, when contrast enhancement is done the histogram envelope will be no more smooth. Stamm et al. [4] explains the reasons behind it. It is seen that some peaks and gaps are introduced into the histogram when contrast enhancement is applied as shown in fig.1. It can be considered as an intrinsic fingerprint or image artifact associated with the contrast enhancement operation. Another type of artifact which I want to consider in this discussion is blocking artifact associated with the low quality JPEG compressed images. The presence of some horizontal and vertical breaks in the low quality JPEG image is known as the Blocking artifact.

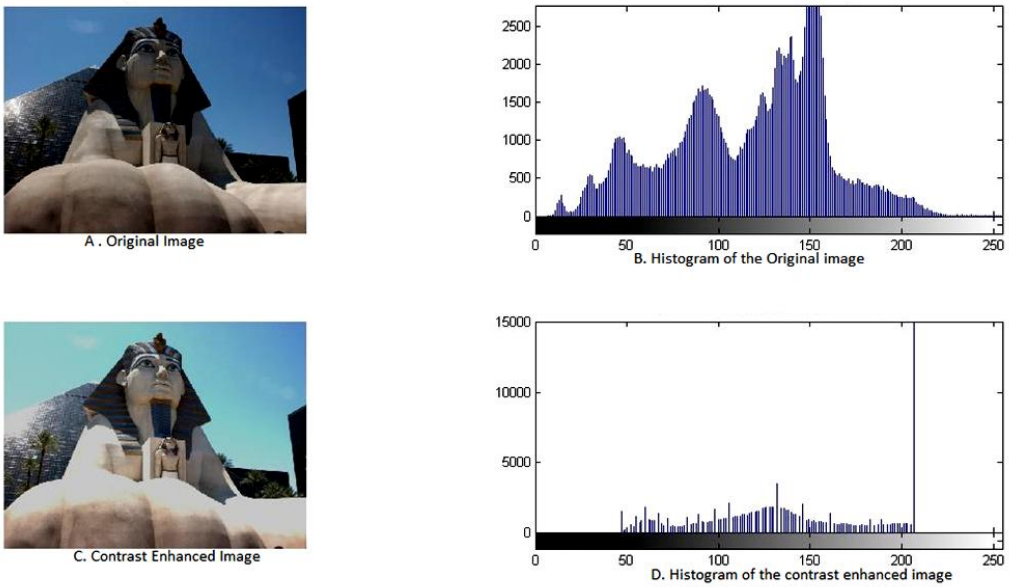

Figure 1: Comparison between the histograms of original and enhanced images.

II. Global Contrast Enhancement Detection

The global contrast enhancement detection algorithm basically makes use of the zero-height gap bins present in the gray level histogram of the image. The algorithm put forward by Cao et al. [5] is as follows:

1. At first, the normalized gray level histogram h*(x)* is obtained.
2. The isolated zero height gap bins present in the histogram are found out. In this process we need to avoid the connected zero bins at the tail ends of the histogram.
3. Count the number of zero height bins and if it is above a threshold value we can say that contrast enhancement is applied to the image.

III. Identification Of Cut And Paste Forgery

Here we consider the case of a forged image which contains a pasted region. Again, we need to ensure that both the regions (original one and the pasted one) have undergone some sort of contrast enhancement adjustments. Here we basically follow the techniques introduced by Cao et al. First of all the composite image is divided into a number of non overlapping blocks. The block size should be atleast 50 by 50.

a) Gap/ Peak Bins Location Matrix

(1) Gap bins location: Consider the case if the 'i^{th}' block. Obtain the gray level histogram of the block and find out the locations of the zero height gap bins by following the same algorithm used in section-II. It can be stored as a vector and can be labeled as $V_g{}^i = [V_g{}^i(0), V_g{}^i(1), \ldots\ldots V_g{}^i(k), \ldots\ldots V_g{}^i(255)]$ where $V_g{}^i(k) = 1$ if the bin is having zero height; otherwise $V_g{}^i(k) = 0$.

(2) Peak Bins Location: First of all, the gap bins in the histogram are filled with the average of the neighboring bins and the median filtering is applied to the histogram to obtain a smooth contour. Then the difference between the gap filled histogram and its filtered version is found out which will give us the location of the peak bins. The peak bin location vector for i[th] block is taken as $V_p{}^i$.

In most of the cases the histogram will be confined to a particular range of pixel values only. That is it will not cover the entire range of pixel values. This particular range is considered as the Effective Detection Range (EDR), R_i. That is outside EDR histogram bins will be all zeros. Tabulate the values of R_i of each block as we need to focus our analysis only within this range. To further reduce the errors, the co-existing peak/gap positions in most of the blocks are retained. The corrected gap and peak position vectors are named as $V_{gc}{}^i$ and $V_{pc}{}^i$ respectively.

b) Gap/ Peak Based similarity Measure

Here we need to take reference vectors form the entire corrected gap and peak position vectors. The vector having the largest number of gap/ peak positions is considered as the corresponding gap/peak position reference vector (V_{gr} *and* V_{pr}).The EDR of the reference vector is given by R_r. Now for the gap based similarity measure individual gap position vectors are compared with the gap reference vector and a similarity index is calculated by using the formula given below.

$$m_g{}^i = \frac{\sum_{k\in R_i\cap R_r} V_{gc}{}^i(\mathrm{k}).V_{gr}(\mathrm{k})}{\sum_{k\in R_i\cap R_r} V_{gc}{}^i(\mathrm{k}).V_{gr}(\mathrm{k}) + \overline{V_{gc}{}^i(\mathrm{k})}.V_{gr}(\mathrm{k}) + V_{gc}{}^i(\mathrm{k}).\overline{V_{gr}(\mathrm{k})}}$$

In the same manner, similarity indices for peak position vectors ($m_p{}^i$) are obtained by substituting the values of peak position vectors of each and every block ($V_{pc}{}^i$) and V_{pr} in the above equation. Finally the values of $m_g{}^i$ and $m_p{}^i$ are fused to obtain final index values of individual blocks. It is given by

$$m^i = {(m_g{}^i + m_p{}^i)}/{2}$$

Finally we can set a threshold *t* and compare the values of m^i with *t*. If $m^i \geq t$ then contrast enhancement is applied to the block. For blocks with $m^i \leq t$, we can say that some other contrast enhancement mapping is applied. Thus we can find out the presence of two different contrast enhancement mappings in a single image which shows that the image is a forged one.

Although this method gives us a very good result even for low quality JPEG compressed images, it will be highly difficult to implement in the case low size and very low quality JPEG compressed images. I have already stated that the block size should be atleast 50 by 50 for getting satisfactory results. So in this paper I also want to add a technique for forgery detection in the case of low quality, low size JPEG compressed images

Figure 2: A typical output of contrast enhancement based forgery detection algorithm implemented using MATLAB

IV. FORGERY DETECTION IN LOW-JPEG IMAGES USING BAG EXTRACTION

This technique uses the presence of blocking artifacts in the low quality JPEG images. It is well known that the low quality JPEG compression, will introduce some horizontal or vertical breaks into image which is known as blocking artifact. These blocks form an 8 by 8 grid known as blocking artifact grid (BAG). When copy-paste processing is done, the copied slice must be pasted in the proper place to mock human eyes, thus the grid in pasted slice and that in the target image are usually mismatched, see Fig.3.

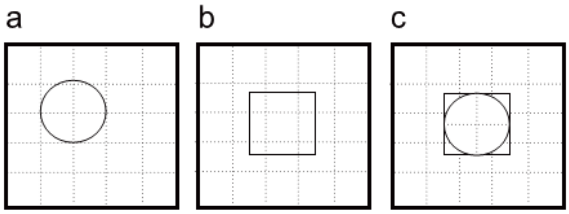

Figure 3: Demonstration of BAG mismatch; (a) &(b) Original images (c) Composite image.

Fig .1(a) and (b) are two original low quality JPEG compressed images and (c) is a composite image produced by pasting a disc shaped portion from fig.(a) to fig.(b) . The dotted lines are BAGs and we can see in fig.(c) how the BAG mismatch takes place in a composite image.

BAG Extraction Algorithm [6]

The presence of blocking artifacts is usually treated as shortcoming of JPEG, and many efforts have been done to estimate it and to reduce it. However, the blocking artifacts is utilized in this section to detect the copy paste forgery in low quality and low size JPEG compressed images in which the contrast enhancement artifacts detection is very difficult. The first step in this process is the detection of blocking artifacts grid in the image.

Here we consider BAG lines as weak horizontal edges. Weak horizontal edges can be detected by finding an absolute second order difference. Suppose a(x, y) represents the pixels in doubtful image A and d(x, y) are the elements in the absolute second-order difference D which can be calculated by the formula given below.

$$d(x,y) = |2a(x,y) - a(x,y-1) - a(x,y+1)|$$

Strong images edges in the image can be eliminated by applying median filtering to the image. This will reduce its influence on BAG. Again we can reduce the false alarm due to periodic line edges by ignoring the differences above 50. Generally, the differences due to blocking artifacts are less than 50.Then we can enlarge the weak horizontal edges by accumulating every 33 columns as shown by the formula given below. Finally a local median is reduced from each element to equalize the amplitudes throughout the resulting pattern.

$$e_a(x,y) = \sum_{i=x-16}^{x+16} d(i,y)$$

$$e(x,y) = e_a(x,y) - Mid[\{e_a(x,i)|_{y-16\le i\le y+16}\}]$$

Blocking Artifact Grid is periodic and it appears only on boundaries of 8 by 8 blocks, so the extracted grid pattern should also have a period of eight. Another interesting feature is that BAGs are local phenomenon, or we can say that blocking artifact is only related to an 8 by 8 block and its four neighbouring blocks. Sometimes BAGs even does not appear on some boundaries. In order to reduce the influence of noise on BAGs, the weak horizontal edge image (E_h) is further periodical median filtered with the formula

$$g_h(x,y) = Mid[\{e(x,i)|i = y-16, y-8, y+8, y+16\}]$$

The horizontal bag line image is given by G_h and its pixels are $g_h(x, y)$. Next, the vertical BAG pattern which can be denoted as G_v can be extracted by putting suitable variations to the above algorithm. Finally add G_h and G_v together to obtain the final BAG image. Then we can manually examine the BAG mismatch in the final BAG image and if it is present then it can be treated as the presence of a cut and paste region in the tested image. This method is a very effective in finding the presence of pasted regions in a low-quality and low-size JPEG compressed image where the contrast enhancement based forgery detection is not possible.

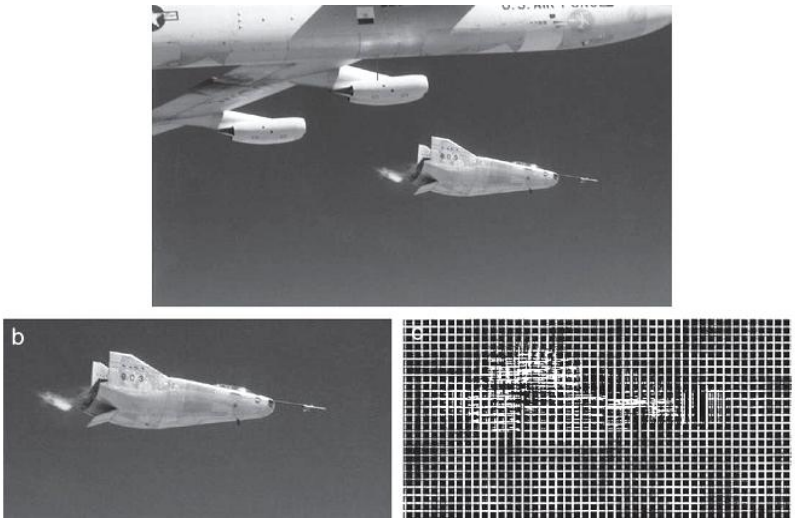

Figure 4: Detection of image forgery using BAG extraction (a) composite image (b) pasted region (c) grid mismatch

V. PERFORMANCE LIMITS

It should be pointed out that the effectiveness of the contrast enhancement based forensic algorithms reduce drastically due to post-processing operations on the image which affects the accurate detection of zero-height gap bins. As such the contrast enhancement based methods are suitable to work in the scenario that contrast enhancement is the last step of manipulation applied to images. Again, anti-forensic techniques adversely conceal abnormal histogram traces, and make the histogram of an enhanced image behave like that of an unaltered one. These forensic techniques could not resist such targeted anti-forensic attacks. In the case of BAG detection algorithm, the BAG in the copied section should not be exactly over the BAG of the background image. In such a case the mismatch will not be visible. The chance for such an error is 1 out of 64.

VI. CONCLUSION

The proposed methods are for detecting the image forgery in both high quality images and very low quality JPEG compressed images. Thus the forensic analysis of a range of different classes of images is successfully done here. As expected from any other forensic technique, these methods also have their own limitations. However, if a set of forensic detection methods are developed and enforced cooperatively, it would be difficult for a malicious user to create a forged image which can invalidate the forensic analysis. It is also essential to develop methods for countering the existing and potential anti-forensic techniques. An image can also be forged without using any of the basic operations such as compression, rescaling, contrast enhancement, histogram equalization etc. All these have become motivations for the development of further improved image forensic techniques.

References

1. H. Farid, “Image forgery detection,” IEEE Signal Process.Mag., vol. 26, no. 2, pp. 16 −25,Mar. 2009.
2. Luo Weiqi, Qu Zhenhua, Pan Feng, Huang Jiwu “A survey of passive technology for digital image forensics,” Front.Comput. Sci., China, 2007.
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. 101117, 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. 492506, Sep.2010.

5. Gang Cao,Yao Zhao,Rongrong Ni and Li , "Contrast Enhancement-Based Forensics in Digital Images," IEEE Trans. Inf. Forensics Security, vol. 9, no. 3, pp. 515-525, March 2014.

6. Weihai Li,Yuan and Nenghai Yu , "Passive detection of doctored JPEG image via block artifact grid extraction," Signal Processing, Elsevier , 2009.

AUTHOR(S) PROFILE

Boby Kurian, received the B.Tech. degree in Electronics and Communication Engineering from Rajiv Gandhi Institute of Technology, Kottaym, in 2006. During 2007-2013, he worked as a Lecturer in ECE at MBCCET, Peermade, Kerala. Currently pursuing the M.Tech. in Signal Processing from College of Engineering, Cherthala affiliated to CUSAT, Kerala.

