Volume 2, Issue 6, June 2012 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Image Manipulation Detection using Intrinsic Statistical Fingerprints

S.Thirumagal, Dr.S.Allwin
Infant Jesus College of Engineering,
Thoothukudi,India

***Abstract*—The digital images or videos are becoming main part in the field of information forensics and security and there uses are increased, so it is must to create forensic techniques capable of detecting image or video frame alteration operations and forgery image. In forgery images and videos, there are number of image processing operations, such as contrast enhancement, histogram equalization, speckle noise, image scaling. We present the forensic methods for detecting globally and locally applied contrast enhancement and method for detecting histogram equalization in image by identifying the features of each operation's intrinsic fingerprint. Additionally we propose a method for detecting noise as well as the method for detecting image scaling or cropping by observing the intrinsic fingerprint of specific mappings. Finally, we test the efficacy of each proposed forensic technique.**

***Index Terms*—Contrast Enhancement, Cropping, Gaussian noise, histogram equalization, image scaling , Speckle noise.**

I. INTRODUCTION

The contrast enhancement, histogram equalization, noise and image scaling are the image processing operations, applied on the original image such as digital image or video frame to alter the image of video to the realistic or pseudo. Now a day, digital images or videos have wide variety of applications in news media, law enforcement, military applications, reconnaissance to medical diagnosis and consumer photography where the authenticity is of prime importance.

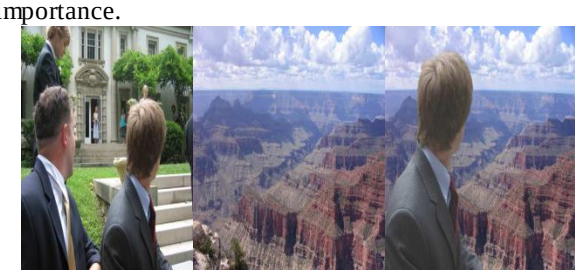


Fig (a) Fig (b) Fig (c)

Fig (a) shows the unaltered image from which an object is cut. Fig (b) shows the unaltered image into which the cut object is paste. Fig (c) shows the forgery image.

With such high popularity and the advent of low-cost and sophisticated image editing software, the integrity of image content can no longer be taken for granted and

a number of forensic related questions arise amidst such extensive use. For example, one can readily ask how an image was acquired? Was it captured using a digital camera, or an image scanner, or was it created artificially using image editing software? Has the image undergone any manipulation after capture? Is it authentic or has it been tampered in anyway? In recent years, digital image can be easily altered to visually realistic manner. This proves to be problematic due to the widespread availability of digital image editing software. The aim of the forensic techniques is the identification of image or video frame which has undergone some form of image alteration or manipulation. While digital representation of reality brings unquestionable advantages, digital images can be easily modified using powerful image editing software, which creates a serious problem of how much their content can be trusted when presented as silent witness in a court room. The image alterations can be gathered by modeling intrinsic properties of an image, then using these properties to identify the tampering.

II. RELATED WORK

Previous image forensic work has dealt with the detection of lighting angle inconsistencies[1]-[2],absence of Color Filter Array(CFA) interpolation-induced correlations[3]. These methods are used to detect the image forgery but these are not universal method. Prior work which deals with the identification of image tampering by detecting operation specific fingerprint include the detection of resampling, double JPEG compression [5]-[6].While each of these methods possesses their own limitations. Detection of inconsistencies in chromatic aberration [5] as well as the absence of CFA interpolation induced correlations. While

these methods are able to detect forgery images but unable to detect the image regions.

III. PROPOSED WORK

A. *Detecting globally applied contrast enhancement in image or video*

Contrast enhancement operations can be viewed as non linear pixel mapping which introduce artifacts in to an image histogram. Most of the contrast enhancement can be viewed as a nonlinear pixel value mapping, followed by quantization. A non linear mapping can be separated into regions where the mapping is locally contractive or expansive. The contract mappings can map multiple unique input pixel values to the same output pixel value, resulting in the addition of sudden peak to an image histogram. Similarly, expansive mappings can cause output pixel values to be skipped over, resulting in gaps in contrast enhancement which uses to perform detection.

We calculate a modified histogram g(l) by performing the multiplication between h(l) and a pinch off function p(l). So that

$$g(l)=p(l)h(l)$$

Where p(l) is the pinch off function, h(l) is the high frequency component. G(k) is discrete Fourier transform of g(l).

The pinch off function, defined as

$$p(l)=\begin{cases} \frac{1}{2}\left(1-\cos\left(\frac{-\pi l}{N_p}\right)\right), & l \le N_p \\ \frac{1}{2}\left(1+\cos\left(\frac{\pi(255-N_p-l)}{N_p}\right)\right), & l \ge 255-N_p \\ 1, & else \end{cases}$$

We calculate E, a normalized measure of the energy in the high frequency components of the pixel value histogram from g(l) according to the formula

$$\text{Energy}=\begin{cases} \frac{1}{N}\sum_k |\alpha(k)G(k)|, & c \le k \le 128 \\ 0, & else \end{cases}$$

Where c is range from 32 to 112.

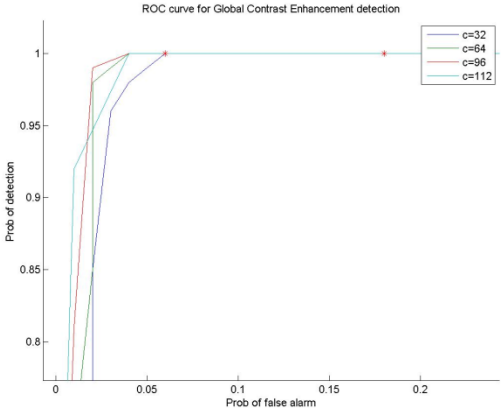


Fig 1

Roc curve shown in Fig1 detects globally applied contrast enhancement with 'c' varies from 32 to 112.In this paper we improve the forensic techniques of forgery image or video frame. After E has been calculated, the decision rule δ_c is used to classify an image or video as unaltered or contrast enhanced by using μ_c threshold, such that

$$\delta_c=\begin{cases} \text{image is not contrast enhanced. Energy} < \mu_c \\ \text{image is contrast enhanced. Energy} \ge \mu_c \end{cases}$$

B. *Detecting locally applied contrast enhancement*

The forensic technique can be extended into a method of the forgery image detection that can be used to locate regions in image or video that can be performed by selecting a set of pixels comprising a region of interest and then applying the test. To accomplish this, the image can be segmented into fixed sized blocks, where each block constitutes a separate region of interest. Detection can be performed on each block individually and the results can be aggregated to identify image or video image regions which exhibit evidence of locally applied contrast enhancement.

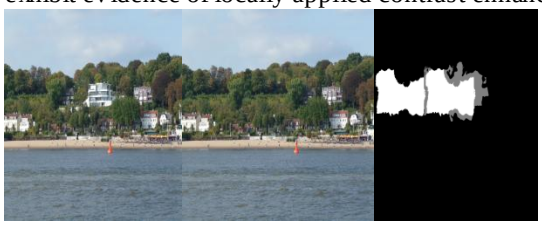


Fig (i) Fig(ii) Fig (iii)

Fig (i) shows the original image, Fig (ii) shows the forgery image and Fig (iii) white represents the forgery image region, black represents the unaltered image region.

C. *Detecting image scaling or cropping*

In this section, we propose the method for detecting image scaling or cropping in image or video frame by identifying the intrinsic fingerprint of pixel value mapping. By observing the common properties of the histogram of unaltered images, we are able to build a model of an unaltered image's pixel value histogram. We then use this model to identify diagnostic features of a pixel value mapping's intrinsic fingerprint. To obtain the energy in the high frequency component of pixel value histogram. Determine whether the energy is below the threshold value or not. If the energy is below the decision threshold, then the image is resized, otherwise the image is unaltered. Finally we plot the ROC curve to calculate the detection and false alarm probability shown in Fig 7. Probability of detection means classified the altered image correctly and probability of false alarm means classified the unaltered image incorrectly.

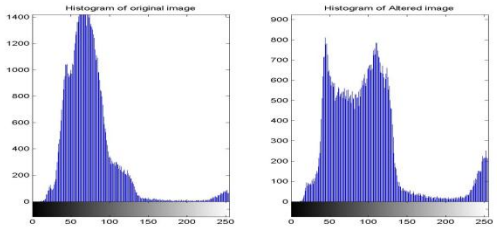


Fig II

Fig II shows the unaltered image pixel value histogram and image scaling histogram

D. Detecting histogram equalization in image

The techniques can be extended into method for detecting histogram equalization in image and video. Histogram equalization, like any other contrast enhancement operation, introduces sudden peaks and gaps into an image histogram. If contrast enhancement is performed using histogram equalization a unique set of traceable artifacts are left behind in addition to those previously discussed. To understand what these artifacts are, we must first briefly describe how histogram equalization is performed. Histogram equalization effectively increases the dynamic range of an image's pixel values that is approximatively uniform. We calculate the frequency domain measure of the distance D, the distance between image normalized histogram and the uniform distribution, then using this distance we determine whether the image or video has undergone histogram equalization, applied or not.

$$D=\frac{1}{N}(\sum_{k=0}|H(k)|\vartheta(k))$$

Where $\vartheta(k)$ is a weighting function used to deemphasize the high frequency regions in H(k), the energy introduced by histogram equalizations intrinsic fingerprint tends to accumulate. Detection was performed using two different weighting functions.

$$\vartheta_1(k)=\begin{cases} e^{(-r_1 k)}, & \text{if } 0 < k < 128 \\ e^{(-r_2 k)}, & \text{if } 128 \le k \le 255 \\ 1, & \text{else} \end{cases}$$

We use decision rule to determine the presence or absence of noise in image.

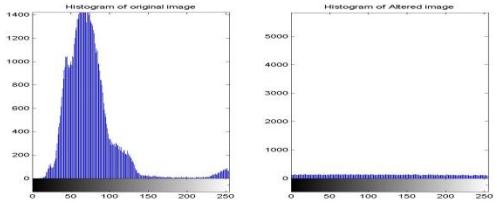


Fig IV

Fig IV shows the unaltered image histogram and altered image histogram.

IV. RESULTS

$$\vartheta_2(k)=\begin{cases} 1, & \text{if } k \le r_2 \text{ or} (256-k) \le r \\ 0, & \text{else} \end{cases}$$

Where r_1 value ranging between 0.6 and 1, r_2 value ranging between 4 and 16.

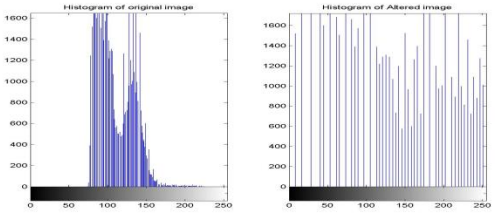


Fig III

Fig III shows the pixel value histogram of unaltered and altered image

E. Detecting noise in image or video

The technique is able to detect whether the image is in noise or not, such as Speckle noise, Gaussian noise. We obtain a frequency domain representation $G_{zi}(k)$ of the histogram of z_i, values free from any possible high or low end histogram saturation effects. This is accomplished by defining as the DFT of $g_{zi}(l)$, which we calculate by using the equation.

$$g_{zi}(l)=h_{zi}(l)P(l)$$

where $p(l)$ is pinch off function, $h_{zi}(l)$ is the normalized histogram of z_i . We measure the strength of the peak to test for the presence of the periodic fingerprint.

$$S=\min\left\{\frac{|G_{z_i}(k^*)|}{mean|G_{zi}(j_1)|}, \frac{|G_{z_i}(k^*)|}{mean|G_{zi}(j_2)|}\right\}$$

where j_1 value ranging from 61 to 68 and j_2 value ranging from 74 to 81. After we calculating the strength of peak S, check whether the image or video frame is added in noise or not by using δ_n decision rule.

$$\delta_n=\begin{cases} noise\ not\ applied, & if\ S > \mu_n \\ otherwise, & if\ S \le \mu_n \end{cases}$$

To evaluate the performance of each and every forgery image or video detection by ROC curve, each image is classified as altered or unaltered by using a series of decision thresholds. The detection and false alarm probability are calculated at each decision threshold. Probability of detection (Pd) is correctly classified the altered image and Probability of false alarm (Pfa) is incorrectly classified the unaltered image. Fig 1(a), We test the performance for detecting contrast enhancement with gamma varying from 1.1 to 1.5. Fig 1(b), We plot the curve for performance of global contrast enhancement in video (Pd of 0.99 and Pfa of 0.03 or less with gamma =1.1). Fig 7, ROC curve for detecting image scaling or cropping and curve to achieve Pd of 0.94 and Pfa of 0.3. Fig 2, Detecting locally applied contrast enhancement. Fig 3, Pd of above

0.94 and Pfa of 0.01 or less by using the ROC curve for detecting histogram equalization with 'r' ranges from 0.6 to 1.0. Fig 4, ROC curve for detecting histogram equalization with 'r' ranges from 4 to 16 (Pd of 0.99 and Pfa of 0.03 with 'r' = 4). Fig 5, Plot the performance for detecting additive noise, Pd of above 0.92 and Pfa of 0.3 or less. Fig 6, plot the ROC curve for detecting additive noise with quality factor 'Q' ranges from 30 to 90. Fig 8,ROC curve for detecting speckle noise to achieve Pd of above 0.92 and Pfa of 0.37 or less. Thus, we extent the techniques of tampering detection for both uncompressed image database and compressed image database.

Detecting globally applied contrast enhancement in image or video

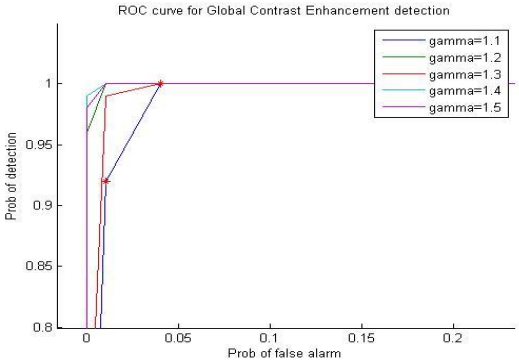


Fig 1(a)

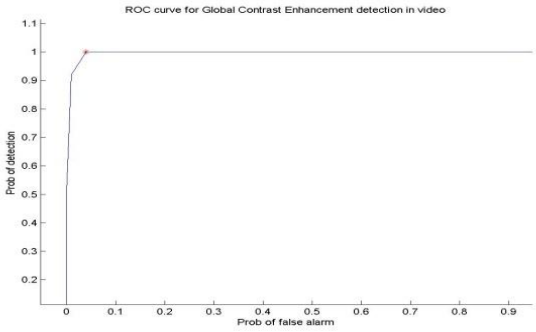
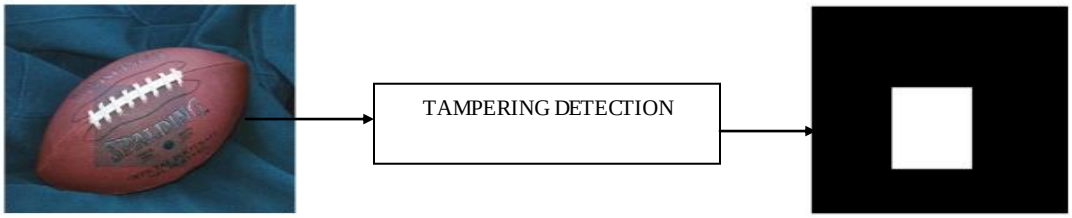


Fig 1(b)

Detecting locally applied contrast enhancement



Forgery image Output Image

Fig 2 White represents the altered image region and black represent the unaltered image region.

Detecting histogram equalization

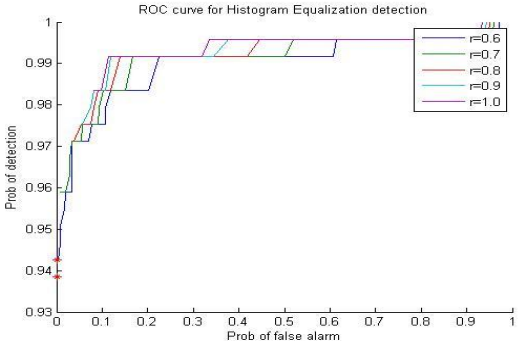


Fig 3

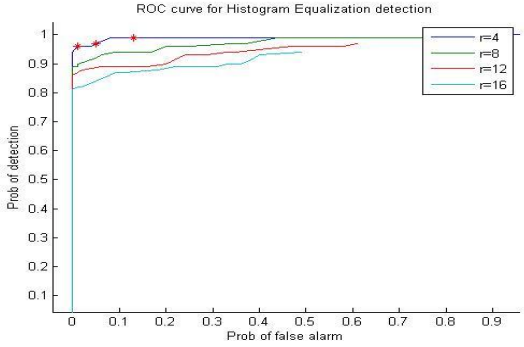


Fig 4

Detecting additive noise

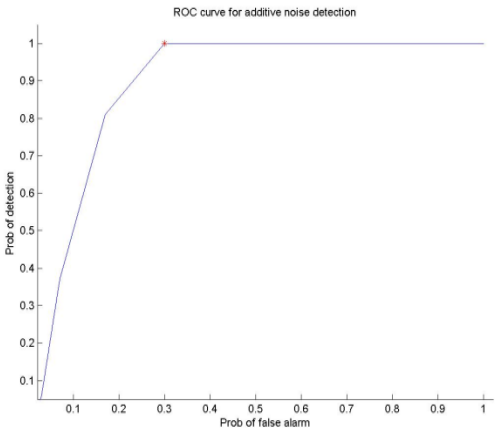


Fig 5

Detecting image scaling or cropping

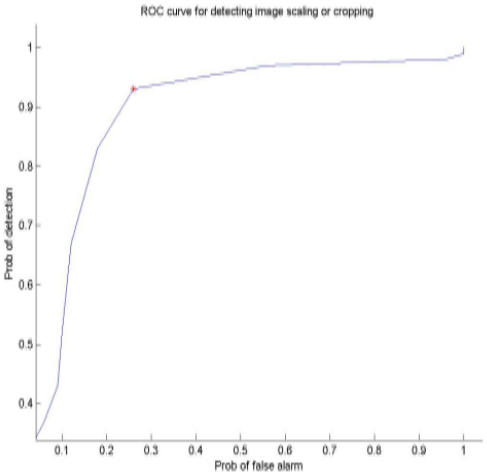


Fig 7

Detecting Gaussian noise

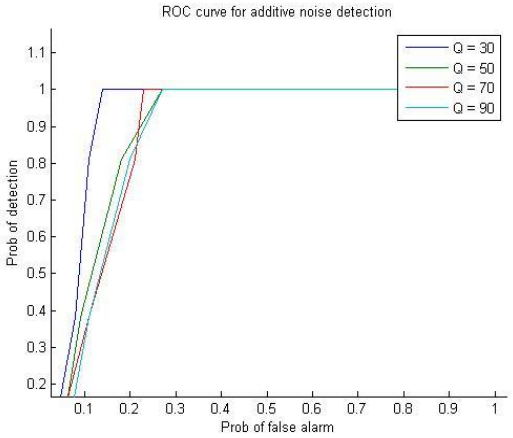


Fig 6

Detecting speckle noise

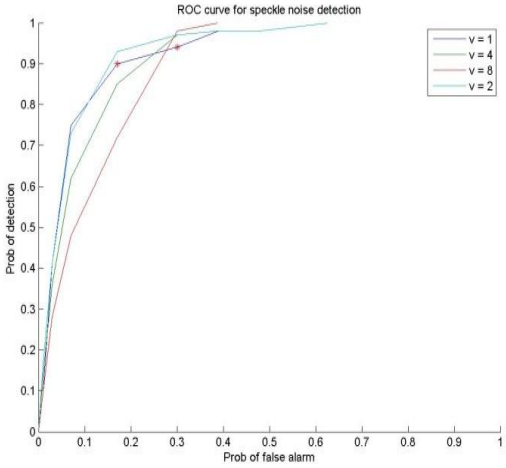


Fig 8

V. CONCLUSION

In this paper, we present the forensic technique for detecting globally and locally applied contrast enhancement and detecting histogram equalization in digital image or video. Additionally, we propose the method for detecting image scaling or cropping and detecting noise by observing the features of intrinsic fingerprint for both uncompressed image database and compressed image database. We test the efficacy for each and every forgery image by using ROC curve

REFERENCES

[1] M.K.Johnson and H.Farid, "Exposing digital forgeries by detecting inconsistence in lighting", in proc. ACM Multimedia and security workshop, New York, NY, 2005,pp. 1-10.

[2] T.-T.Ng, S.-F.Chang, and Q.sun, "Blind detection of photomontage using higher order statistics," in Proc, IEEE Int. Symp. Circuits Systems, Vancouver, BC, Canada, May 2004, vol.5,pp.V-688-V-691.

[3] J.Lukas,J.Fridrich, and M.Goljan, "Nonintrusive component forensics of visual sensors using output image,"IEEE Trans. Inf . Forensics Security, vol. 2, no, 1,pp.91-106,Mar,2007.

[4] T. Penvy and J. Fridrich, "Detection of double-compression in JPEG images for applications in steganography," , IEEE Trans, Inf. Forensics security, vol. 3, no. 2,pp.247-258, jun.2008.

[5] M.K. Johnson and H.Farid, " Exposing digital forgeries through chromatic aberration," in Proc. ACM Multimedia and Security Workshop, Geneva, Switzerland, 2006, pp. 48-55.

[6] A.C. Popescu and H.Farid, "Exposing digital forgeries by detecting traces of resampling," IEEE Trans. Signal Process., vol. 53,pp.758, Feb. 2005.

[7] A.C. PoPescu and H.Farid, "Statistical tools for digital forensics," in Proc. 6th Int.Workshop ukaon Information Hiding, Toronoto, Canada, 2004, pp. 128-147.

[8] J. Luka's, J. Fridrich, and M. Goljan, "Detecting digital image forgeries using sensor pattern noise," in Proc. SPIE, Electronic Imaging, Security, Steganography, Watermarking of Multimedia Contents, San Jose, CA, Feb. 2006, vol. 6072, pp. 362-372.

[9] A. Swaminath, 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.

