Forensic Detection of Multiple Tampering In Digital Images

Sreelekshmy.V [1],Shankar. J [2], A. Joel Livin [3]

[1] M.E Student, Applied Electronics, LITES Thovalai ,India, [2] Assistant Professor, ECE , LITES Thovalai,[3] HOD, Assistant Professor, ECE Dept, LITES Thovalai, India,
[1]vsreelekshmy@gmail.com[2] shankarjeyaraj@hotmail.co.in [3] joellivin.ece@lites.edu.in

Abstract

Digital imaging has experienced a tremendous growth in recent decades and the use of digital images has increased, so has the incentive to create digital image forgeries. Now a days several digital image editing tools are available, thus the originality and authenticity of digital images become more questionable. Such modified images create problems if they are used as an authenticated proof for any crime. Hence the study of digital image forensics technology is becoming a researching hotspot. It is such a challenging task to find out the marks of tampering in images and checks whether it is an original or doctored one. This paper presents detection of some multiple tampering such as contrast enhancement, composite image average filtering, median filtering, rotating, re-sampling, gamma correction and the combinations of each with the help of histogram peak/gap values and re-normalized noise histograms.

Index Terms—Composite Image, Digital image forensics, Multiple tampering, Re-normalized histogram.

I. INTRODUCTION

With the advancement of photo editing tools, electronic alterations of digital images for deceiving purposes become an easy task which results in a high number of image forgeries. These modifications cannot be noticed by human eyes. Therefore verification of originality of images has become a challenging task. A wide variety of manipulations such as contrast enhancement, composite image, average filtering, median filtering, rotating, re-sampling, gamma correction, splicing, scaling, blurring, cropping etc. are used to manipulate images.

The verification of originality of images is required in variety of applications such as military, forensic, media, scientific, glamour, etc. Image tampering is a digital art which needs understanding of image properties and good visual creativity. Detection of image tampering deals with investigation on tampered images for possible correlations embedded due to tampering operations. Detecting forgery in digital images is a rising research field with important implications for ensuring the credibility of digital images.

In order to restore the integrity of digital images, image tampering detection that is a technique for distinguishing whether an image is the original output from the camera or the tampered one, is developed as an important and urgent issue. Existing image tampering detection works rely on detecting the inconsistent regularities originated from different parts of digital still camera system. The phenomenon of image forgery leads to serious consequences such as reducing trustworthiness and creating false beliefs in many real-world applications.

For example fig 1(a) shows a doctored photograph of our present prime minister surveying the flood situation in Chennai, as released by PIB on 5 December 2015.

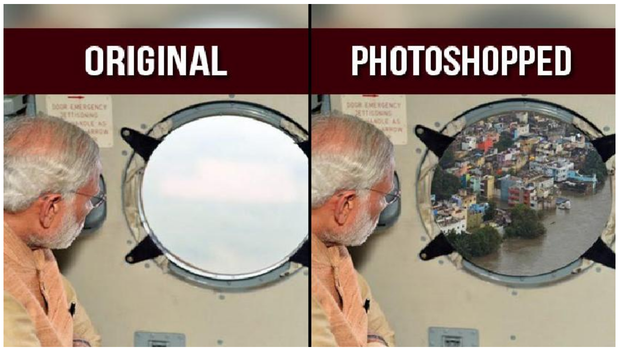

Fig 1(a): doctored photograph of narendra modi which is a composite image.

A set of previous works are there which deal with image manipulation detection. In [1] which gives what are the types of manipulations can be occurred in images. Swaminathan *et al* fails to determine which specific type of manipulation was forced [2], Stamm and Liu fails to determine the contrast enhancement in middle/low quality jpeg compressed images and also both source enhanced cut-paste forgeries [3], Cao *et al* detect the contrast enhancement in either uncompressed or previously JPEG compressed images and local contrast enhancement in both single and both-source enhanced composite image [4] but fails to determine the contrast enhancement in middle/low quality jpeg compressed images and also both source enhanced cut-paste forgeries.. There also exist another category of forensic techniques which focus on detecting specific image manipulations. Farid *et al* considers chromatic aberrations as forensic tool for detecting image tampering [5]. With the help of sensor noise identify the camera which the photo is taken forensics tasks are achieved by detecting the presence of PRNU but Chen *et al* fails to determine which specific type of manipulation was forced [6], [7] models correlation between image and its EXIF header for the manipulation detection but fails to determine type of manipulation, [8] fails to detect other noise related features since they are using statistical features these may get lost due to multiple tampering.

The rest of this paper is organized as follows. In Section II, we revisit the previous works on contrast enhancement forensics in digital images. Section III gives the algorithm for detecting multiple tampering using re-normalized histogram noise and noise difference and an universal image authentication scheme for detecting single and multiple tampering. The constructed re-normalized histogram is used to detect image tampering operations in Section IV. Section V concludes this paper.

II. RELATED PRIOR WORKS

Two novel algorithms are proposed in [4] to detect contrast enhanced manipulations.

1. Detection of global contrast enhancement applied to JPEG compressed and uncompressed images by identification of height-gap bins.2. Identify the fake/composite image from single or both source enhanced composite images by detecting block-wise peak/gap positions and their composite boundary by detecting inconsistency b/w position vectors in different regions.

A. Proposed Contrast Enhancement Detection Algorithm

1) Get image's normalized gray level histogram *h(y)*.

2) Detect the bin at k as a zero height gap bin if it satisfies:

$$\begin{cases} h(k) = 0 \\ \min\{h(k-1), h(k+1)\} > \tau \\ \frac{1}{2w_1+1}\sum_{x=k-w_1}^{k+w_1} h(x) > \tau \end{cases} \qquad (2.1)$$

3) Count the no: of detected ZHGB denoted by Ng.

Experiments show that w1 = 3 and τ = 0.001 are appropriate. If Ng is greater than the decision threshold, contrast enhancement is detected else not.

B. Proposed Source- Enhanced Composite Image Identification

Here the consistency between peak/gap artifacts detected in different regions is checked for discovering composite images. The block-wise similarities m_g^i =−1 or m_p^i=−1 are updated by averaging the available neighboring effective measurements. The resulting similarity for the i-th unlabeled block, denoted by m^i, can be generated by fusing the peak/gap based similarities.

$$m^i = \frac{m_g^i + m_p^i}{2} \qquad (2.2)$$

When $m_g^i = -1$ or $m_p^i = -1, m^i$ = max(m_g^i, m_p^i). m^i= -1 occurs rarely in both source enhance images. All blocks in an unsaturated region own m^i= -1 while blocks out of region own $m^i \geq$ t indicate single source enhanced composite image. Each block is classified as

1. If $m^i \geq$ t , CE mapping is applied to that source region is detected.
2. If $m^i <$ t , a different CE mapping is applied to other source region.

The both-source enhanced composite image is detected if two different mappings are detected in two complementary regions, respectively. The threshold *t* is experimentally set as 0.2. The composition boundary was accurately located by detecting the inconsistency between detected block-wise peak/gap positional distributions. The proposed contrast enhancement based forensic methods could work particularly well when contrast enhancement is performed as the last step of manipulation.

Existing image tampering detection works rely on detecting the inconsistent regularities originated from different parts of digital still camera system, such as chromatic aberration [5] in optical system, photo response non-uniformity (PRNU) sensor pattern noise [6], EXIF information [7]. When an image is subject to manipulations, intrinsic image regularities become inconsistent and specific artifacts are introduced as opposed as the original image. It is noted that these intrinsic regularities are usually designed for one specific tampering operation, such as compression or gamma correction. When a wide range of tampering operations are used to process one digital image, image pixels are unavoidable to be modified when manipulating the image by image operation processes. Such modified image pixels could weaken or destroy existing intrinsic image regularity which is designed for a specific type of tampering operations. Thus, image tampering detection accuracy could be seriously degraded.

III. PROPOSED METHODOLOGY

A. Image Noise Estimation

Image noise is extracted using four de-noising filters.

1. Averaging filter- removal of high frequency noise.
2. Gaussian filter - removal of high frequency noise.
3. Median filter - removal of salt & pepper noise.
4. Wiener filter - remove noise associated with local pixels.

Let A = $\{A^{(c)}\}$ be a color image where c ∈ {red , green ,blue }. L be the gray scale image and can be compute as

$$L= 0.2989A^{(r)}+0.5870A^{(g)}+0.1140A^{(b)} \qquad (3.1)$$

$G^{(d)}$ be de-noising filter, d=1,2,3,4.

Compute de-noising version, $D^{(d)}$ using

$$D^{(d)} = L * G^{(d)} = \begin{bmatrix} D^{(d)}(1,1) & \cdots & D^{(d)}(1,N) \\ \vdots & \ddots & \vdots \\ D^{(d)}(M,1) & \cdots & D^{(d)}(M,N) \end{bmatrix} \qquad (3.2)$$

* : convolution

Compute noise residuals $f^{(d)}(m,n)$ at location(m, n).

$$f^{(d)}(m,n)= L(m,n) - D^{(d)}(m,n) \qquad (3.3)$$

$D^{(d)}(m,n) \in D^{(d)}$

B. Noise Histogram Construction

Since actual noise pattern inside camera is unknown they use histogram of noise and noise difference because high correlation among neighboring pixels are influenced by tampering.

Histogram of noise,

$$h(k)=\frac{\#\{(m,n):f(m,n)=k\}}{M*N} \qquad (3.4)$$

# *:* cardinal number set.

Compute difference of image noise residuals between two de-noising filters by

$$f^{(d,b)}(m,n)= f^{(d)}(m,n)-f^{(b)}(m,n) \qquad (3.5)$$

b=1,2,3,4 and $b \neq d$.

6 different combinations of noise difference are obtained.

Compute re-normalized histogram of noise,

$$\check{h}(k)=\frac{h(k)}{h(0)}=\frac{\#\{(m,n):f(m,n)=k\}}{\#\{(m,n):f(m,n)=0\}} \qquad (3.6)$$

Finally, a set of $n \times (4 + 6) = n \times 10$ histogram features are selected for image tampering detection.

C. Proposed Scheme

(1) Compute the image noise by using four different de-noising filters, to obtain $f^{d}(m, n)$ by Eq. (3.3).

(2) Compute the image noise difference between different two combinations of the image noise by Eq. (3.5).In total,6 image noise differences are obtained.

(3) Represent the noise and noise differences in absolute value and construct the histogram noise and noise difference by Eq. 3.(6).

(4) Select a total of $n \times 10$ features as compact feature set.

(5) Use support vector machine (SVM) to train and classify. In the training process, use one versus all strategy to train an SVM classifier, the radial basis function kernel (RBF) is used to calculate the distance between two image histogram features.

IV. RESULT & DISCUSSION

For testing the performance of our proposed contrast enhancement detection technique, each test image is classified by determining if it is contrast-enhanced or not using a series of decision thresholds. The probabilities of detection (Pd*)* and false alarm (Pfa*)* determined by thresholds are calculated as the percentage of the enhanced images correctly classified and that of the unenhanced images incorrectly classified, respectively. Contrast enhancement detection indicates that our proposed algorithm achieves high detection rates even under low Pfa. Pd attains 100% when Pfa = 1%. Note that the same high Pd is always gained when the raw images are JPEG-compressed with different Qs.

Table I: Performance of multiple tampering operation detection.

Two types of Operation		Accuracy%	Average%
Type I	Type II		
Average filtering(3)	Median filtering(5)	99.00	95.59
	Rotating(5)	94.50	
	Re-sampling(130)	95.62	
	Gamma correction(0.7)	93.27	
Median Filtering(5)	Average filtering(3)	92.62	95.02
	Rotating(5)	98.00	
	Re-sampling(130)	90.87	
	Gamma correction(0.7)	98.62	
Rotating(5)	Average filtering(3)	94.87	93.59
	Median filtering(5)	98.75	
	Re-sampling(130)	88.87	
	Gamma correction(0.7)	91.87	
Re-sampling(130)	Average filtering(3)	94.25	91.31
	Median filtering(5)	98.00	
	Rotating(5)	87.75	
	Gamma correction(0.7)	85.25	
Gamma correction(0.7)	Average filtering(3)	92.25	92.00
	Median filtering(5)	98.62	
	Rotating(5)	91.87	
	Re-sampling(130)	85.25	

All 17 different tampering operations are tested in the previous experiments. When using multiple types of tampering operations to tamper an image, there are 272 possible combinations by considering the tampering types, parameters, and tampering orders. Due to the page limit, we list some typical cases of 2 types of image tampering operations in Table III. Specifically, we choose the average filtering with filter order 3, median filtering with filter order 5, rotating with 5, re-sampling with 130% and gamma correction with 1.3. Each of 800 original images from CASIA dataset is first operated by Type I operation and then processed by Type II operation. Following the same experimental setup, 100 original images are randomly selected to generate the tampered images and the remaining images are for testing. The average accuracies for the different combinations of two types of tampering operations are above 91.31%. It can be seen that the histograms of noise and noise difference has the ability to capture the changes resulted from multiple types of tampering operations. By using noise histogram features, our proposed method can consistently detect image tampering with high accuracy, without the prior knowledge of tampering types, parameters and tampering orders.

V. CONCLUSION

The techniques that are robust against the post processing operations and anti-forensic techniques need to be developed IN [4].This paper proposes a method for image tampering detection by using noise histogram features. This histogram is constructed by the noise and noise difference among different de-noising filters, which has the ability to capture the variation changes by different tampering operations, including single type and multiple types. When applying such constructed histogram for detecting multiple types of tampering operations, the proposed method can detect the tampered image without the prior knowledge of tampering types, parameters and tampering orders. For future enhancement Thus extensive survey is done in this paper to detect duplication in images and provides future enhancement directions in the area of image forgery detection.

REFERENCES

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

[2] 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.

[3]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.

[4] Gang Cao, Yao Zhao, Rongrong Ni “Contrast Enhancement-Based Forensics in Digital Images” IEEE transactions on information forensics and security, vol. 9, no. 3, march 2014

[5]“Exposing digital forgeries through chromatic aberration,” M. K. Johnson and H. Farid, in *Proc. of the 8th Workshop on Multimedia and Security*, 2006, pp. 48–55.

[6]“Determining image origin and integrity using sensor noise,” M. Chen, J. Fridrich, M. Goljan, and J. Luk´as, *IEEE Transactions on Information Forensics and Security*, vol. 3, pp. 74–90, 2008.

[7] “Digital image forensics via intrinsic fingerprints,” A. Swaminathan, M. Wu, and K. J. R. Liu, *IEEE Transactions on Information Forensics and Security*, vol. 3, pp. 101–117, 2008.

[8] “Modeling the exif-image correlation for image manipulation detection,” J. Fan, A. C. Kot, H. Cao, and F. Sattar, in *IEEE International Conference on Image Processing (ICIP)*, Sept 2011, pp. 1945–1948.

[9] “Intrinsic Sensor Noise Features for Forensic Analysis on Scanners and Scanned images,” H. Gou, A. Swaminathan, and M. Wu, *IEEE Transactions on Information Forensics and Security*, vol. 4, pp. 476–491, 2009.

[10] “Image Tampering Detection Using Noise Histogram Features”Jiayuan Fan, Tao Chen, Jiuwen Cao in IEEE International Conference in Digital Signal Processing on 24 July 2015.