ISSN: 2321-7782 (Online)
Volume 3, Issue 6, June 2015
International Journal of Advance Research in Computer Science and Management Studies
Research Article / Survey Paper / Case Study
Available online at: www.ijarcsms.com

Detecting Image Forgery using Intrinsic Fingerprints

Jayshri Charpe[1]
Second Year M.Tech Student, Department of CSE
G. H. Raisoni Institute of Engi. & Tech. for Women's
Nagpur, India

Antara Bhattacharya[2]
Assistant Professor, Department of CSE
G. H. Raisoni Institute of Engi. & Tech. for Women's
Nagpur, India

Abstract: ***Digital images play an important role in many application areas. Because of the easy availability of photo editing software and tools, it becomes problematic to use the digital images in applications where their genuineness is of prime importance. Therefore, it is necessary to create forensic techniques which are capable of detecting the tampering in image. Most common operations that are involved in the creation of forged images are contrast enhancement, copy-paste forgery etc. In this paper, we present different techniques for detecting global contrast enhancement and copy-paste forgery. The proposed technique for the detection of contrast-enhanced image is based on zero-bin calculation. The technique can efficiently detect the contrast enhancement on both uncompressed and JPEG-compressed images. In copy-paste forgery detection, we proposed the two different techniques for detection of copy-paste forged images created using single source and forged images created using two sources.***

Keywords: contrast enhancement; copy-paste forgery; copy-move forgery; image processing; image forgery

I. INTRODUCTION

With the increased importance of the digital images in various applications, where authenticity is of prime importance, it is necessary to verify the integrity and authenticity of digital images. But, the usage of digital images has become more frequent throughout society; creation of digitally forged images has increased. Because of the easy avaibility of image editing software such as Photoshop, making forgeries in digital images becomes an easy task without leaving obvious evidence that can be recognized by human eyes. So the image authentication came forth as an important problem. Digital image authentication techniques broadly have two types i.e. active and passive. The active approach includes intrusive methods like watermarking and digital signature. These are also known as non-blind methods. The major drawback of watermark approach is that watermarks need to be embedded in the image before distribution. In the market, most cameras nowadays are not equipped with the function for embedding watermark. Also, use of these methods deteriorates image quality. To verify the image authenticity using passive approach, no information needs to be embedded in images for distribution. These methods are also known as blind as the presence of original image not required to verify the authenticity. So, these methods also have the application in the field of image forensic. Since the problem of image forensics is very broad, this paper focuses on forgery detection in digital images. This paper present efficient and reliable techniques for detecting globally and applied contrast enhancement, and copy-paste forgery in the digital image

II. RELATED WORK

S. Bayram, I. Avcubas, B. Sankur, and N. Memon [1] proposed a technique for the detection of doctoring in digital image. Doctoring includes multiple steps i.e. a sequence of basic image-processing operations such as rotation, scaling, smoothing, contrast shift etc. The technique used could detect whether image manipulations occurred or not but it fails to determine which specific type of manipulation was enforced.

M. Stamm and K. Liu [2] proposed a blind forensic algorithm for identifying the practice of global contrast enhancement procedure on digital images. A different algorithm is presented to detect the histogram equalization which is also a type of contrast enhancement operation.

M. C. Stamm and K. J. R. Liu [3] proposed different methods not only for the detection of global and local contrast enhancement but also for identifying the use of histogram equalization and for the detection of the global inclusion of noise to an already JPEG-compressed image. The method proposed detects contrast enhancement in previously high quality JPEG compressed image. However, it fails to determine the contrast enhancement in previously middle/low quality JPEG compressed image.

M. C. Stamm and K. J. R. Liu [4] focuses on recovering the possible information about the unmodified form of image and the operations used to modify it, once image alterations have been detected. The proposed algorithm gives an accurate estimation if the enhancement is non standard.

G. Cao, Y. Zhao, and R. Ni [5] present a blind method for the detection of gamma correction, a special type of contrast enhancement. The technique used is based on the histogram characteristics that are measured by patterns of the peak gap features. These peak gap features for the gamma correction detection are distinguished by the precomputed histogram of images. The approach fails to detect the contrast enhancement in previously middle/low quality JPEG compressed image.

G. Cao, Y. Zhao, R. Ni and X. Li [6] proposed two different algorithms for the detection of global and local contrast enhancement in an image. Algorithm detects the contrast 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. An important application is to identify cut-and-paste type of forged images. The work proposed is used to detect the cut and paste type of forged images created by using two sources. The methods can detect the contrast enhancement only if the contrast enhancement is the last step applied.

S. Bravo-Solorio, A. K. Nandi [7] proposed a method to detect copy-paste forged images affected with scaling, reflection and rotation. The proposed method uses color dependent feature vectors. A.C. Popescu et.al [8] uses PCA to obtain reduced dimension feature vector. Each block is of the size 16 *16. Li Jing et.al [9] proposed a method which uses feature points to locate copied and pasted areas. The Scale Invariant Transform algorithm is used to extract the features. S. Bayrament et.al [10] proposed an algorithm which uses Fourier Mellin transform (FMT) to extract the features. The algorithm proposed in [11] uses SIFT. The method can efficiently detect rotated duplicated regions.

III. PROPOSED METHODOLOGY

In proposed research work, there are three different techniques that are used to detect the forged images created using different types of image forgery techniques.

» Global contrast enhancement detection algorithm

» Copy-paste forgery detection algorithm for two-sourced forged images

» Copy-paste forgery detection algorithm for single source forged images.

a) Global contrast enhancement detection algorithm

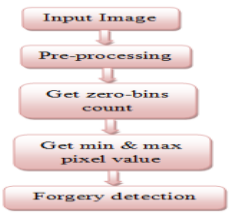


Fig. 1: flowchart for Global contrast enhancement detection algorithm

1. Pre-processing:

In pre-processing, we convert color image into gray image and apply histogram equalization on the converted image. Here we are applying histogram equalization as a form of contrast enhancement in order to create a contrast enhanced image.

2. Histogram Calculation & zero bin count:

The input image is then used in histogram calculation and histogram of the image is calculated. Zero-bins are calculated from the histogram of the image. Zero bins are the bins whose value is found to be null.

3. Min & Max Pixel Value calculation:

In Min & Max pixel value calculation, we calculate the minimum and maximum pixel value of the image.

4. Forgery Detection:

After getting the zero-bin count and minimum & maximum pixel value of the image, we apply the threshold condition. Threshold condition can be given as:

Threshold = zero count >18 && max > 248 && min < 10

If this condition is satisfied, contrast enhancement is said to be detected otherwise, no contrast enhancement is said to be done.

b) Two source Copy-paste image forgery detection algorithm:

There are two parts of two source copy-paste image forgery detection algorithm.

1. ***Training:*** In training part, we select the training path for possible source image. Each image in the selected folder for training is processed under following algorithm.

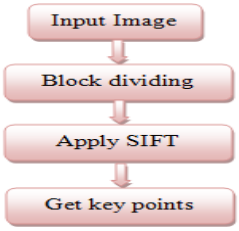


Fig.2: flowchart for training sub module

A. Block dividing:

Each image is divided into the small blocks. of different size. Each image of size 512*512 is first divided into the block size of 32 in order to create total 16 blocks. The same image is again divided into the blocks size of 64 in order to create 8 blocks. After that the image is divided into block size of 128 to create 4 blocks and again into block size of 256 to create 2 blocks.

B. Applying SIFT and feature extraction:

SIFT i.e. Scale Invariant Feature Transform is applied on the each block in order extract the features. The features extracted using SIFT are invariant to scaling, rotation and other lighting conditions.

2. Detection Algorithm:

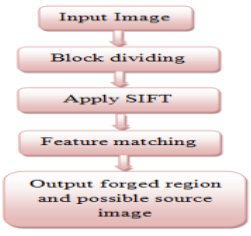


Fig.3: flowchart for detection of copy-paste forged images

A. Block dividing:

Each image is divided into the blocks of different size. Each image of size 512*512 is first divided into the block size of 32 in order to create total 16 blocks. The same image is again divided into the blocks size of 64 in order to create 8 blocks. After that the image is divided into block size of 128 to create 4 blocks and again into block size of 256 to create 2 blocks.

B. *Applying SIFT and feature extraction:*

SIFT i.e. Scale Invariant Feature Transform is applied on the each block in order extract the features. The features extracted using SIFT are invariant to scaling, rotation and other lighting conditions.

C. *Feature Matching:*

In feature matching, each block obtained in training part is compared with the each block obtained in detection part. After feature matching, we obtaine the keypoints in the form of matrix as follows:

Matrix: [no. of key points in current block, max no. of key points matched, index of Matching block]

The threshold condition is obtained using this matrix values: Threshold = mat (k, 2)/mat (k, 1)*100 >= 60 && mat (k, 1) >= 12

Where, mat (k, 1) is the number of key points in current block and mat (k, 2) is the maximum number of key points matched.

If this condition is satisfied, we get the result in the form of detected forged region along with the possible source image.

c) Single source Copy-paste image forgery detection algorithm:

Block Dividing: In block dividing, input image is divided into the small blocks of size 8*8.

DCT Transform and Feature Extraction: DCT transform is then applied on the each block. Here DCT transform (Discrete Cosine Transform) is applied in order to extract the features from the blocks.

Forgery Detection: Based on the extracted features from the blocks, forgery is detected. Forgery is detected using formula:

diff_val (k1) =sqrt (sum (abs (fea_ori - fea_frg). ^2))

Where, fea_ori is the feature of original image and fea_frg is the feature of forged image.

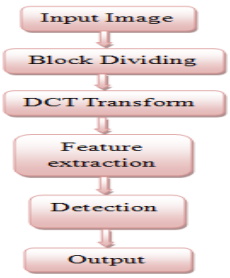
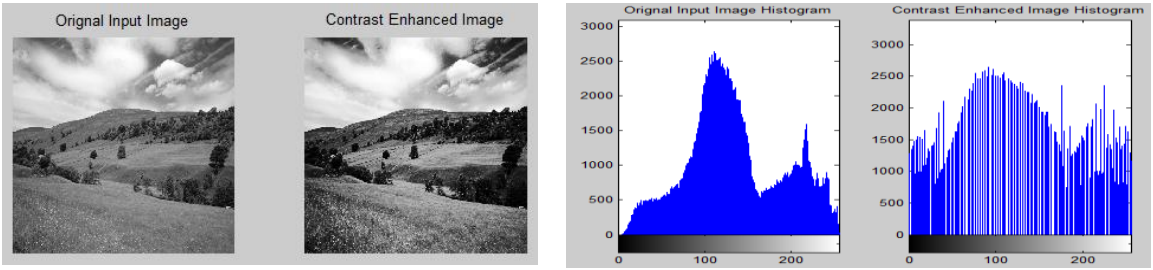


Fig 4: flowchart for copy-paste forgery detection algorithm for single source

IV. EXPERIMENTAL RESULTS

a) Global Contrast Enhancement Detection:

1. Pre-processing :

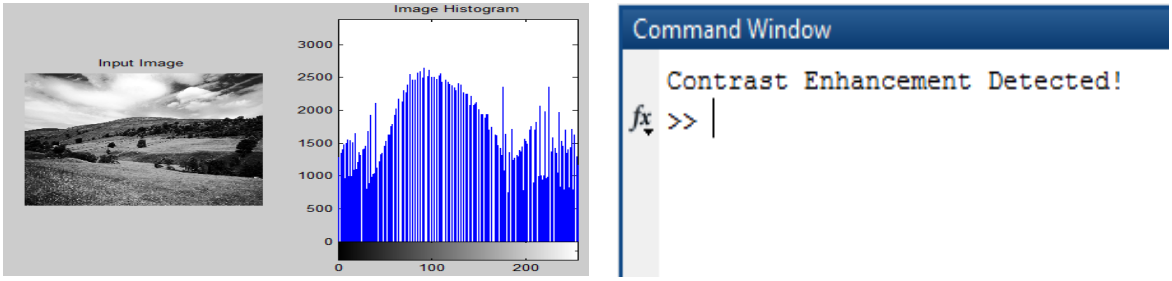


(a) **(b)**

Fig 5: a) and b) output of pre-processing step

Fig. 5 shows the output of pre-processing step. In fig a), original color image is converted to gray level image and then the image is contrast enhanced. Fig b) shows the histogram of original color image and the histogram of contrast enhanced image.

2. Detection:

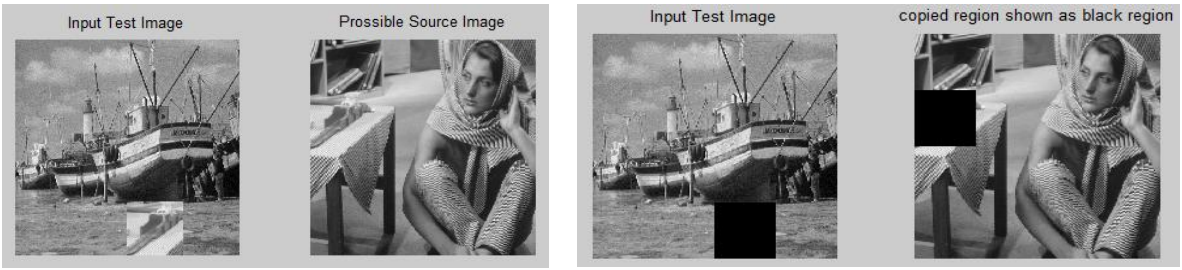


(a) (b)

Fig 6: a) and b) detection results of global contrast enhancement detection module.

Fig 6 shows the detection results of global contrast enhancement detection module. In this, fig a) is the input contrast enhanced image which we obtained in pre-processing and its histogram. Fig. b) shows the command window showing the contrast enhancement detection message.

b) Two source Copy-paste image forgery detection:



(a) **(b)**

Fig.7: a) and b) detection results of copy-paste forgery detection algorithm (for two sources)

Fig.7 shows detection results of copy-paste forgery detection algorithm (for two sources). In this, fig. a) shows the forged input image and its possible source image. fig. b) shows the input forged image with detected forged region (shown as a shaded black area) and possible source image with the copied region (shown as a shaded black area).

c) Single source Copy-paste image forgery detection:

Fig 8 shows the results of copy-paste image forgery detection module. Fig a) shows the detection result when portion of size 32*32 is copied and pasted on the same image. Fig b) shows the detection result when portion of size 64*64 is copied and

pasted on the same image and fig c) shows the detection result when portion of size 96*96 is copied and pasted on the same image.

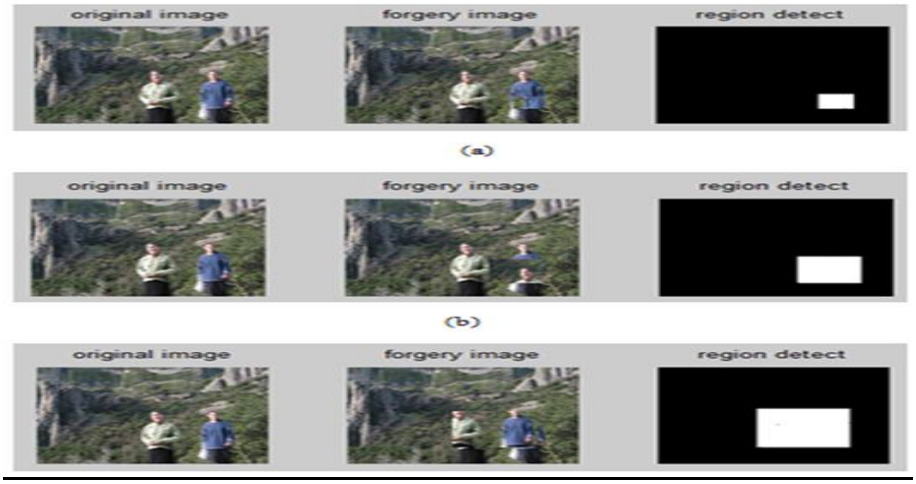


*Fig 8: results of copy-paste image forgery detection module for a) 32*32 block size area b) 64*64 block size area c) 96*96 block size area*

V. EXPERIMENTAL SETUP & ANALYSIS

a) Experimental Setup

For results, we used an image manipulation dataset to test the images. The image manipulation dataset contain original test images for the detection of image manipulation features. It consists of 48 base images. In order to create the input image for global contrast enhancement detection module, we apply contrast enhancement processing on the benchmark image from dataset and created a new database which contain both original and contrast enhanced images. The results are tested against both compressed and uncompressed images.

b) Result Analysis

TABLE I

Comparison of proposed method with previous methods

Techniques	Uncompressed image	Compressed image with high quality factor (90%)	Compressed image with medium quality factor (50%)	Compressed image with low quality factor (20%)
Stamm Liu method [3]	succeeded	succeeded	Not succeeded	Not succeeded
Gang Cao et.al method [6]	succeeded	succeeded	succeeded	succeeded
Our proposed method	succeeded	succeeded	succeeded	succeeded

Proposed global contrast enhancement detection algorithm can detect the contrast enhancement in all types of images such as PNG, JPG, BMP, TIF etc. Algorithm works well for both uncompressed and compressed images. Proposed global contrast enhancement detection algorithm can detect the contrast enhancement efficiently for images compressed under the JPEG compression quality of 20%, 50% and 90%.

In single source copy-paste image forgery detection algorithm, the algorithm can efficiently detect duplicate areas of small, medium and large size. Proposed algorithm can efficiently detect copy-paste forged areas of size 32*32, 64*64, 96*96 etc. However, the execution time increases with the increase in duplicate area size.

In two source copy-paste image forgery detection, the algorithm can efficiently detect the forged images along with the possible source image and forged region.

VI. Conclusion

This paper presents algorithms for the detection of global contrast enhancement and copy-paste forgery in digital images for both single source and two source forged images. Proposed global contrast enhancement detection algorithm works well for both uncompressed and compressed images. It can detect the contrast enhancement efficiently for images compressed under the JPEG compression quality of 20%, 50% and 90%. Also, an efficient algorithm for the detection of copy-paste image forgery using single source is proposed. The algorithm can efficiently detect the large duplicate areas of size 32*32, 64*64 up to 96*96. Another algorithm for the detection of copy-paste forgery using two sources is proposed which detects the possible source image along with the forged region.

References

1. S. Bayram, I. Avcubas, B. Sankur, and N. Memon, "Image manipulation detection," J. Electron. Imag. vol. 15, no. 4, pp. 04110201–04110217, 2006
2. M. Stamm and K. R. Liu, "Blind forensics of contrast enhancement in digital images," 15th IEEE International Conference on Image Processing, 2008. ICIP 2008, Oct. 2008, pp. 3112–3115.
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. M. C. Stamm and K. J. R. Liu, "Forensic estimation and reconstruction of a contrast enhancement mapping," in Proc. IEEE Int. Conf. Acoust., Speech Signal, Dallas, TX, USA, Mar. 2010, pp. 1698–1701..
5. G. Cao, Y. Zhao, and R. Ni, "Forensic estimation of gamma correction in digital images," in Proc. 17th IEEE Int. Conf. Image Process..Hong Kong, 2010, pp. 2097–2100.
6. G. Cao, Y. Zhao, R. Ni and X. Li, "Contrast Enhancement-Based Forensics in Digital Images," IEEE Trans. Inf. Forensics Security, Mar. 2014.
7. S. Bravo-Solorio, A. K. Nandi, "Exposing Duplicated Regions Affected by Reflection, Rotation and Scaling," in International Conference on Acoustics, Speech and Signal Processing, May 2011.
8. A. Popescu and H. Farid, Exposing digital forgeries by detecting duplicate image regions, Dept. Computer. Sci. Dartmouth College, Tech.Rep. TR2004 515, 2004.
9. Li Jing, and Chao Shao," Image Copy-Move Forgery Detecting Based on Local Invariant Feature Journal Of Multimedia,Vol.7,No.1, February 2012
10. S. Bayram, H.T. Sencar, N. Memon," An efficient and robust method for detecting copy-move forgery", in: IEEE International Conference on Acoustics, Speech and Signal Processing, IEEE Press, New York, 2009.
11. Vincent Christlein," An Evaluation of Popular Copy-Move ForgeryDetection Approaches", IEEE Transactions On Information Forensics And Security, 2011

