ISSN:0975-9646

Comprehensive Study of Contemporary Image forgery Identification Techniques

Gauravkumarsingh Gaharwar[1, 2], Prof. V. V. Nath[3], Raina Gaharwar[4]

[1]*Research and Development, Raksha Shakti University, Ahmedabad, India*
[2]*School of Business and Law, Navrachana University, Vadodara, India*
[3]*Institute of Management, Nirma University, Ahmedabad, India*
[4]*G. H. Patel Department of computer Science and Technology, Sardar Patel University, Vallabh Vidyanagar, India*

Abstract **- Image forgery is emerging as a big problem not only for law enforcement agencies but also for citizens as well. With the readily availability of low cost hardware & software and all the images being digital only, it becomes easy for criminals to forge any image. This paper studies contemporary solutions proposed by different researchers for identifying forgery in copy-move forgery, image splicing, image retouching, and lightning condition forgery. The aim of this paper is to study for the single algorithm which is effective enough to identify any type of forgery.**

Keywords **- Digital image forgery, copy-move forgery, image splicing, image retouching, lightning condition forgery**

I INTRODUCTION TO DIGITAL IMAGE FORGERY

This is the era of digital images where most of the images are captured and stored in digital nature due to low cost of digital cameras & storage, very high quality of images and ease of manipulating them with image editing tools. Also, many advance image editing tools are available online and offline with very cost effective alternatives. As it becomes easy to manipulate images, this is adopted by criminals for making money by forging digital images. Image forensics is a field of Digital forensics developed significantly to battle this problem and provide a tool to authenticate digital image.

II RELATED RESEARCH WORK

Image forgeries are broadly categorized into,

1 Copy-move forgery

Copy-move is one of the most widespread image tampering technique, also it is very difficult to identify this type forgery as the copied image is taken from the same image. In Copy-Move image forgery, a part of the image is copied and pasted to another part of the same image. Some contemporary methods proposed by various researchers for identifying copy move forgeries are,

Lin et al. [1] proposes a detection method in which image is divided into the blocks of equal size, and then feature of this block is extracted and sorted. The difference of the positions of every pair adjacent features is computed. The accumulated number of each of this difference is calculated, more accumulated number means possible occurrence of duplicate region.

Shahid and Mansoor [2] proposes the algorithm in which the input image of size a×b is divided into 'n' blocks of size m×m pixels then each block is iteratively compared to other block in the image. In case of complete match both blocks are marked as copied. In case of copy detection, the adjacent neighbors of the marked blocks are then compared. The algorithm confirms the manipulation if at least three blocks in the adjacent neighborhood of the both marked blocks is exact match of each other.

Jing and Shao [3] proposes Scale Invariant Feature Transform (SIFT) algorithm to detect local invariant features of image, then search the matched feature points by SIFT feature matching. If the number of matched points is larger than the assumed threshold value, we would judge the image has been tempered.

Deshpande and Kanikar [4] propose an algorithm in which Discrete Wavelet Transformation (DWT) is applied to image to get LL1 subband. This LL1 subband is divided into sub-images, and then phase correlation is applied to compute the spatial offset between copied regions.

Amerine et al. [5] propose feature based algorithm, in which keypoints that are stable local extrema in the scale space and, for each of them, a feature vector is computed from a local pixel area around the detected point. In presence of a copy-move manipulation the extracted Scale Invariant Feature Transform (SIFT) keypoints from the copied and the original regions have similar descriptor vectors. Therefore, matching among SIFT features is adopted to detect if an image has been tampered with and, subsequently, localize such forgery.

Gupta et al. [6] propose a method which detects region duplication forgery by dividing the image into overlapping blocks and then searching for the matching region in the image.

Asati and Pardhi [7] propose a method which extracts invariance to geometric and photometric transformations for object orientation. After that the algorithm identify the Statistical analysis of structure Information (SASI), viz., energy, entropy, correlation sum of energy and sum of correlation features. The extracted feature will pass to the kernel based binary classifier called Support Vector Machine (SVM) for prediction about the forgery in the image.

Kohale et al. [8] propose a method which combines block based approach and feature based approach for forgery identification.

Maind et al. [9] propose an improved block representing method which compares both the approaches viz Discrete Cosine Transform (DCT) and Principal Component Analysis (PCA) for identifying forgery.

Hashmi et al. [10] propose an image forgery detection using an efficient and robust method combining un-decimated wavelet transform and SIFT. In which, First image is transformed into wavelet domain and SIFT is applied on the transformed image to obtain the features. As wavelet produces multispectral components, features are more predominant. Thus after obtaining interest point feature descriptor we go for finding matching between these feature descriptors to conclude whether tampering is done to the given image or not.

All the above algorithms can be categorized in either block based method or keypoint based method. According to Kulkarni and Chavan [11] block based methods gives accurate result for identifying image forgery in any jpg image but also takes lot more time then keypoint based methods.

Also, forgery covered under geometric transformations like rotation and scaling are better suited for the keypoint based methods while methods like exhaustive block search method can find almost any type of copy-move forgery.

2 Image Splicing

Image splicing forgery involves composition or merging of two or more images changing the original image significantly to produce a forged image. In case images with differing background are merged then it becomes very difficult to make the borders and boundaries indiscernible. Some contemporary methods proposed by various researchers for identifying image splicing forgeries are,

Anusudha et al. [12] proposed an approach to image splicing detection by exploiting the magnitude and phase information to use the moments of wavelet characteristic function as one part of the image features to detect the spliced images.

Chennamma and Rangarajan [13] proposes an approach in which the detection of splicing operation on images by estimating radial distortion from different portions of the image using line-based calibration. The detection of image splicing through the verification of consistency of lens radial distortion has been proposed for the detection of image splicing on both synthetic and real images.

Ke et al. [14] proposes an approach which is based on both the assumption that the shadow as well as main body is copied and pasted from another image during forgery and the property that the shadow will not obviously change the surface texture of object. In other words, the shadow areas with their adjacent non-shadow area should have the same or similar texture. So, the texture in the shadow area is Image Splicing Detection Based on Texture Consistency of Shadow not consistent with that in the original lit area in tamper image.

Rasse [15] proposes a method for efficient forgery detection particular for faces in images. The illuminant color is estimated using the physics based method as well as statistical edge method which make the use of inverse intensity-chromaticity color space. The estimate of illuminant color is extracted independently from the different mini regions. For the classification used the Support Vector Machine (SVM) approach. In this paper our main goal is to take review of different methods for digital image forgeries detection

Burvin and Esther [16] propose a machine-learning based technique. This technique is applicable to images containing two or more people and requires no expert interaction for the tampering decision. Physics-based and statistical-based illuminant estimators are used to incorporate information on the image regions. From these illuminant estimates, texture-based and edge-based features are extracted which are used to provide to an automatic decisions based on machine-learning approach.

Su et al. [17] propose an enhanced approach of Markov state selection is proposed, which matches coefficients to Markov states base on well-performed function model. Experiments and analysis show that the improved Markov model can employ more useful underlying information in transformed coefficients and can achieve a higher recognition rate as results.

Moghaddasi et al. [18] proposes the run length run number algorithm (RLRN), by applying two dimension reduction methods, namely, PCA and kernel PCA. Support vector machine is used to distinguish between authentic and spliced images. Results show that kernel PCA is a nonlinear dimension reduction method that has the best effect on R, G, B, and Y channels and gray-scale images.

Moghaddasi et al. [19] proposes an approach based on singular value decomposition (SVD) feature extraction method applied in steganalysis. SVD-based features are merged with DCT for image splicing detection. Support vector machine is used to distinguish between authentic and spliced images.

Ibrahim et al. [20] introduces a texture enhancement technique involving the use of fractional differential masks based on the Machado entropy. The masks slide over the tampered image, and each pixel of the tampered image is convolved with the fractional mask weight window on eight directions. Consequently, the fractional differential texture descriptors are extracted using the gray-level co-occurrence matrix for image splicing detection. The support vector machine is used as a classifier that distinguishes between authentic and spliced images.

Image splicing forgery detection algorithm divided into two categories: detection algorithm based on authenticity of the local area and detection algorithm based on source inconsistency. The former contains many detection algorithms. Approaches based on the consistency of imaging source are based on the fact that natural images are usually obtained through data acquisition devices, which introduce uniform characteristics to the entire image, and henceforth the variation in the local characteristics across the image can be used to detect tampering.

3 Image Retouching

"In Image Retouching, the images are less modified. It just enhances some features of the image. There are several subtypes of digital image retouching, mainly technical retouching and creative retouching." [21] Image is carried out to either reduce or improve certain features of the image. Retouching may require rotation, scaling, or stretching of an image before combining it with other image. Some contemporary methods proposed by various researchers for identifying image retouching forgeries are,

Stemm and Liu [22] present an iterative method to jointly estimate the contrast enhancement mapping used to modify an image as well as the image's pixel value histogram before contrast enhancement. Their method requires no side information and makes no assumptions on the form of the contrast enhancement mapping aside from monotonicity. This algorithm is more general, which assumes that the contrast enhancement mapping can be described by a parametric equation.

Cao et al. [23] propose a forensic scheme for identifying and reconstructing gamma correction operations in digital images. Statistical abnormity on image grayscale histograms, which is caused by the contrast enhancement, is analyzed theoretically and measured effectively. Gray level mapping functions involved in gamma correction can be estimated blindly.

Kee and Farid [24] have developed a metric that quantifies the perceptual impact of geometric and photometric modifications by modeling common photo retouching techniques. Geometric changes are modeled with a dense locally-linear, but globally smooth, motion field. Photometric changes are modeled with a locally-linear filter and a generic measure of local image similarity. These model parameters are automatically estimated from the original and retouched photos as described in Materials and Methods.

Again Cao et al. [25] propose two algorithms to detect the contrast enhancement involved manipulations in digital images. Firstly, they focus on the detection of global contrast enhancement applied to the previously JPEG-compressed images, which are widespread in real applications. 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. Secondly, they propose to identify the composite image created by enforcing contrast adjustment on either one or both source regions. 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.

Patil et al. [26] proposes the method for detecting global and local contrast enhancement is also called Intrinsic Fingerprint detection technique. After selecting test image that is color or grayscale image. If the image is RGB image, it is first separated into Red component, Green component and Blue component. The histogram of the image's pixel value is calculated for either Red or Green or Blue component. The magnitude of Discrete Fourier Transform (DFT) of the calculated histogram then calculated. The obtained magnitude is then plotted against the frequency to obtain the frequency plot. Sudden zeros or striking peaks present in the frequency plot are referred to as intrinsic finger prints. The intrinsic fingerprint if exists in the plot, then the image is said to be altered by contrast enhancement.

All the proposed algorithms work on analyzing image histogram to identity contrast enhancement. Irregularities from the histogram can be considered as the evidence of image retouching forgery. With histogram analysis algorithm can also localize the forgery area.

4 Lighting Condition

Now days the image forgery is very common where two movie stars are shown romantically involved. This type of forgery can be easily done by splicing two different images together. Often such spliced images are from different scene and having different lightning conditions and so it is very difficult for image forger to match exact lightning condition of one image with other. Some contemporary methods proposed by various researchers for identifying lighting condition forgeries are,

Kee and Farid [27] describe how to model complex lighting environments with a nine-parameter spherical harmonic model. As 3-D surface normals usually cannot be determined from a single image, we considered the 2-D surface normals at occluding boundaries, from which only five of the nine model parameters could be estimated.

Johnson and Farid [28] show that under some simplifying assumptions, arbitrarily complex lighting environments can be approximated with a low-dimensional model. We show how the parameters of a reduced version of this model can be estimated from a single image, and how this model can be used to detect consistencies and inconsistencies in an image.

Johnson and Farid [29] describe a technique for estimating the direction (within one degree of freedom) of an illuminating light source. They extended basic formulation by relaxing some of the simplifying assumptions that were necessary to make the problem tractable, and by generalizing the approach to work under a local light source.

Johnson and Farid [30] describe a computational technique for automatically estimating lateral chromatic aberration. Although we eventually plan to incorporate longitudinal chromatic aberration, only lateral chromatic aberration is considered here. We show the efficacy of this approach for detecting digital tampering in synthetic and real images.

Remya [31] propose method deals with peak/gap bins detection method and peak/gap similarity measurement method which contains Peak/Gap bins detection, Peak/Gap bins similarity measurement, Histogram, Detection of Globally Applied Contrast Enhancement, and Detection of Locally Applied Contrast Enhancement.

Lightning inconsistency is one of the obvious technique to identify image forgery. Johnson and Farid have suggested many algorithms which uses 2-D surface normals, and lateral chromatic aberration. Latest algorithm

suggested by Remya uses Peak/Gap bin detection method for identifying lighting inconsistencies.

III CONCLUSION

Image forgeries can be categorized into either copy-move forgery or image splicing or image retouching or lightning condition forgery. From this maximum research work is being done on copy-move forgery, while very less research work is done on image retouching and lightning condition forgery. It is also evident that copy-move forgery, image splicing, image retouching and lightning condition forgery are done with malafide intentions, while image retouching is done to enhance certain features, like brightness or contract of the image.

Moreover, there is no unified algorithm with ability of detection of any type of forgery and future research is to be done in that direction.

REFERENCES

[1] HWEI-JEN LIN, CHUN-WEI WANG, and YANG-TA KAO, "Fast Copy-Move Forgery Detection," *WSEAS TRANSACTIONS on SIGNAL PROCESSING*, vol. 5, no. 5, pp. 188-197, May 2009.

[2] Tehseen Shahid and Atif Bin Mansoor, "Copy-Move Forgery Detection Algorithm for Digital Images and a New Accuracy Metric," *International Journal of Recent Trends in Engineering*, vol. 2, no. 2, pp. 159-161, November 2009.

[3] Li Jing and Chao Shao, "Image Copy-Move Forgery Detecting Based on Local Invariant Feature," *JOURNAL OF MULTIMEDIA*, vol. 7, no. 1, pp. 90-97, February 2012.

[4] Pradyumna Deshpande and Prashasti Kanikar, "Pixel Based Digital Image Forgery Detection Techniques," *International Journal of Engineering Research and Applications*, vol. 2, no. 3, pp. 539-543, May 2012.

[5] Irene Amerinia et al., "Copy-Move Forgery Detection and Localization by Means of Robust Clustering with J-Linkage," *Signal Processing: Image Communication*, March 2013.

[6] Ashima Gupta, Nisheeth Saxena, and S K Vasistha, "Detecting Copy move Forgery using DCT," *International Journal of Scientific and Research Publications*, vol. 3, no. 5, May 2013.

[7] Shraddha R Asati and P R Pardhi, "Exposing Digital Image Forgeries by Illumination Color Classification," *International Journal of Engineering Trends and Technology (IJETT)*, vol. 18, no. 6, pp. 269-271, December 2014.

[8] Tushant A Kohale, S D Chede, and P R Lakhe, "Forgery Detection Technique Based on Block and Feature Based Method," *International Journal of Advanced Research in Computer and Communication Engineering*, vol. 3, no. 6, pp. 7334-7335, June 2014.

[9] Rohini A Maind, Alka Khade, and D K Chitre, "Image Copy Move Forgery Detection using Block Representing Method," *International Journal of Soft Computing and Engineering (IJSCE)*, vol. 4, no. 2, pp. 49-53, May 2014.

[10] Mohammad Farukh Hashmia, Vijay Anand, and Avinas G Keskar, "Copy-move Image Forgery Detection Using an Efficient and Robust Method Combining Un-decimated Wavelet Transform and Scale Invariant Feature Transform," in *AASRI Conference on Circuit and Signal Processing*, 2014, pp. 84-91.

[11] V S Kulkarni and Y V Chavan, "Comparison of methods for detection of Copy-Move Forgery in Digital Images," *Spvryan's International Journal of Engineering Sciences & Technology*, vol. 1, no. 1, October 2014.

[12] K Anusudha, Samuel Abraham Koshie, S Sankar Ganesh, and K Mohanaprasad, "Image Splicing Detection involving Moment-based Feature Extraction and Classification using Artificial Neural Networks," *International Journal on Signal & Image Processing*, vol. 1, no. 3, pp. 9-13, December 2010.

[13] H R Chennamma and Lalitha Rangarajan, "Image Splicing Detection Using Inherent Lens Radial Distortion," *International Journal of Computer Science Issues*, vol. 7, no. 6, pp. 149-458, November 2010.

[14] Yongzhen Ke, Weidong Min, Xiuping Du, and Dandan Li, "Image Splicing Detection Based on Texture Consistency of Shadow," *Journal of Convergence Information Technology*, vol. 8, no. 4, February 2013.

[15] Sushama G Rasse, "Review of Detection of Digital Image Splicing Forgeries with illumination color Estimation," *International Journal of Emerging Research in Management &Technology*, vol. 3, no. 3, pp. 27-30, March 2014.

[16] P Sabeena Burvin and J Monica Esther, "Detection of Digital Image Splicing Using Luminance," *International Journal of Engineering Research and Applications*, pp. 29-33, March 2014.

[17] Bo Su, Quanqiao Yuan, Shilin Wang, Chenglin Zhao, and Shenghong Li, "Enhanced state selection Markov model for image splicing detection," *EURASIP Journal on Wireless Communications and Networking*, pp. 1-10, July 2014.

[18] Zahra Moghaddasi, Hamid A Jalab, and Rafidah Md Noor, "SVD-based Image Splicing Detection," in *International Conference on Information Technology and Multimedia*, Putrajaya, Malaysia, November 2014, pp. 27-30.

[19] Zahra Moghaddasi, Hamid A Jalab, RafidahMd Noor, and Saeed Aghabozorgi, "Improving RLRN Image Splicing Detection with the Use of PCA and Kernel PCA," *The Scientific World Journal*, 2014.

[20] Rabha W Ibrahim, Zahra Moghaddasi, Hamid A Jalab, and Rafidah Md Noor, "Fractional Differential Texture Descriptors Based on the Machado Entropy for Image Splicing Detection," *Entropy*, pp. 4775-4786, July 2015.

[21] P. Sabeena Burvin and J. Monica Esther, "Analysis of Digital Image Splicing Detection," *IOSR Journal of Computer Engineering*, vol. 16, no. 2, pp. 10-13, Mar-Apr 2014.

[22] M. Stamm and K.J.R. Liu, "Blind forensics of contrast enhancement in digital images," in *15th IEEE International Conference on Image Processing*, San Diego, CA, 2008.

[23] Gang Cao, Yao Zhao, and Rongrong Ni, "Forensic estimation of gamma correction in digital images," in *17th IEEE International Conference on Image Processing*, Hong Kong, 2010, pp. 3112 - 3115.

[24] Eric Kee and Hany Farid, "A perceptual metric for photo retouching," *Proceedings of the National Academy of Sciences of United States of America*, vol. 108, no. 50, pp. 19907-19912, October 2011.

[25] Gang Cao, Yao Zhao, Rongrong Ni, and Xuelong Li, "Contrast Enhancement-Based Forensics in Digital Images," *IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY*, vol. 9, no. 3, pp. 515-525, March 2014.

[26] Mahesh Mahipati Patil, S P Rangdale, and S A Nalawade, "Digital Image Alteration Detection using Advance Processing," *International Journal of Computer Applications*, vol. 116, no. 18, pp. 18-21, April 2015.

[27] Eric Kee and Hany Farid, "Exposing Digital Forgeries From 3-D Lighting Environments," in *IEEE Workshop on Information Forensics and Security*, Seattle, 2010.

[28] Micah K Johnson and Hany Farid, "Exposing Digital Forgeries in Complex Lighting Environments," *IEEE Transactions on Information Forensics and Security*, vol. 2, no. 3, pp. 450-461, August 2007.

[29] Micah K Johnson and Hany Farid, "Exposing Digital Forgeries by Detecting Inconsistencies in Lighting," in *ACM Multimedia and Security Workshop*, New York, USA, 2005.

[30] Micah K Johnson and Hany Farid, "Exposing Digital Forgeries Through Chromatic Aberration," in *Multimedia and Security Workshop*, Geneva, Switzerland, 2006.

[31] S Remya, "Digital Image Forgery Detection by Contrast Enhancement," *IOSR Journal of Computer Engineering*, vol. 16, no. 5, pp. 1-7, September 2014.