A Proposed Work on Image Forgery Detection Technique

Manjima Mishra
Gyan Ganga Institute of Technology and Sciences
Jabalpur, India

Preeti Rai, PhD
Gyan Ganga Institute of Technology and Sciences
Jabalpur, India

ABSTRACT
Digital imaging has grown to become the prevalant technology for creating, processing, and storing digital memory and proof. Though this technology brings many leverage, it can be used as a ambiguous tool for covering details and evidences. This is because today digital images can be tampered in such supermacy that forgery cannot be find visually. In fact, the immunity concern of digital content has arisen a long time ago and different methods to verify the efficiency of digital images have been developed. Digital images offer many features for forgery detection algorithm to take precedence of specifically the colour and brightness of individual pixels as well as an image's resolution and format. These properties grant for analysis and similarity between the significance of digital forgeries in an attempt to develop an algorithm for detecting image tampering. This paper presents a technique for copy move image forgery detection using 2-Directional 2-Dimensional Principal Component Analysis $(2D)^2PCA$.

Keywords
Copy-move, Image forgery, Image forgery detection, Features extraction, Lexicographical sorting.

1. INTRODUCTION
Acquiring digital image as official document has become an accepted mode and the scope of low cost technology in which the image could be easily manipulated are two most denoting impression towards image forgery detection. There are many technologies to identify the digital image forgery their implementation is limited by the conditions imposed by many systems

Digital Image forgery techniques are divided in to two approaches presented in Fig.1. They are active approach and passive approach. In Active approach [1], the digital image desires some pre-processing such as watermark embedding or signature generation at the time of creating the image. There are many images in internet without water marking or digital signatures. In such case active approach could not be used to find the authentication of the image. So, the second approach is used.

The passive approach [2] does not need any digital signature generated or watermark embedded in advance. There are two techniques mainly used to manipulate digital images. 1: Splicing (Compositing) - Digitally manipulated combination of at least two source images to produce an integrated result 2: Cloning (Copy-Move) - a segment of the image is copied and pasted somewhere else within the image.

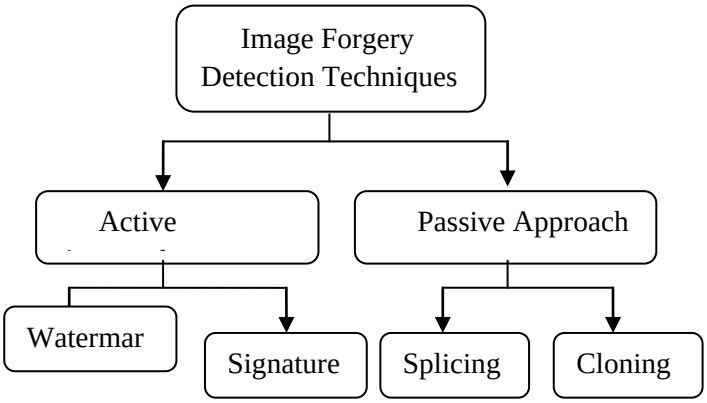

Fig.1. Categories of Image Forgery Techniques

2. COPY-MOVE
This paper considers a specific type of image forgery where a part of the image is copied and pasted on another part of the same image. An example for this type of forgery can be seen in Fig.2. This process can be done without any modifications on the duplicated regions. It is not always necessary that some additional post processing operations are often performed either on the copied region before pasting it or on the whole forged image, to make the forgery concealed.

(a) (b)

Fig.2. An example of copy-move forgery (a) Original Image With three different Lids. (b) Forged Image with two same Lids.

3. RELATED WORK
In most of the other approaches the suspicious image is divided into overlapping blocks. The aim is to detect blocks that are copied and moved. The copied region will contain overlapping blocks. The distance between each duplicate block pair will be similar since each block is carried with equal amount of shift. The next step would be extracting features form these blocks, which will give similar values for matching block. Different features can be used to perform the

image block. These blocks are vectorized and arranged in a matrix and the vectors are lexicographically sorted [3] for later detection. The computational time calculate by number of blocks, sorting techniques and the number of feature. In this an image size of size P x Q, it is divided into (P-b+1) (Q-b+1) overlapping blocks of size $b \times b$. The blocks are than sorted in a lexicographical order. Vectors related to blocks of matching content would be similar to each other in the list, so that same regions could be easily detected.

A. C. Popescu et. al.,[4] state that PCA is efficient to extract the image features. The method to produce each feature vector is called principle component analysis. The values are obtained by using the theorems of covariance matrix, eigenvectors and linear basis for each image block with the initial conditions of zero-mean. Then the vectors coefficients of each block are stored in a matrix S. These coefficients are then sorted lexicographically and the duplicated regions will be revealed by considering the offset of all pairs whose distances in S less than a specify threshold.

Ashima Gupta et. al.,[2] Work on an approach that can detect forged JPEG images and further locate the tampered parts, by examining the double quantization effect hidden among the Discrete Cosine Transform (DCT) coefficients. The image is divided into overlapping blocks (16x16) for feature extraction. Authors have used DCT coefficients for feature extraction and then find the matching blocks in the image.

Zhang et. al., [5] proposed an approach for detecting copy-move forgery detection in digital images. Authors used Discrete Wavelet Transform (DWT) and divided low-frequency band into four non-overlapping sub-images and phase correlation is used to compute the spatial offset between the copy-move regions. Then, they applied pixel matching for detecting the duplicate region. This algorithm works well in the highly compressed image. This is an effective algorithm with lower computational time compared with other algorithms.

Xiao Bing Kang et. al., [6] introduce an algorithm named Singular Value Decomposition (SVD) was used to extract the algebraic and geometric features from small overlapping image blocks and to produce a singular value feature vectors which are saved in a matrix. This matrix is then reduced rank by reduced-rank approximation before detecting the similarity of vectors.

M. K. Bashar et. al.,[7] given Kernel Principle Component Analysis (KPCA) or wavelet transform to extract the features of the small blocks split from a given image which are then lexicographically sort to suggest the similarity of corresponding blocks. The paper proposes algorithms to detect forged areas with translation, flip and rotation based on the global. The results also examine cases of addition noise and lossy JPEG compression. KPCA is the best in case of noisy and rotation of any degree compared with PCA and wavelet based.

Kakar and Sudha et. al.,[8] developed a new technique based on transform-invariant features which detecting copy-paste forgeries but need some post processing based on the MPEG image signature tools. Feature matching that uses the inherent constraints in matched feature pairs so as to improve the detection of tampered regions is used which results in a feature matching.

Muhammad et. al.,[9] proposed a copy-move forgery detection method based on dyadic wavelet transform (DyWT). DyWT being shift invariant is more suitable than DWT. Image is decomposed into approximate and detail sub bands which are further divided into overlapping blocks and the similarity between blocks is calculated. Based on high similarity and dissimilarity pairs are sorted. Using thresholding, matched pairs are obtained from the sorted list.

Sutthiwan et. al.,[10] presented a method for passive-blind colour image forgery detection which is a combination of image features extracted from image luminance by applying a rake – transform and from image by using edge statistics.

Huang et al.,[11] proposed a copy move forgery detection method based on Scale Invariant Feature Transform (SIFT) descriptors. After extracting the descriptors of different regions, they match them with each other to find manipulated area in images.

Fridrich et. al.,[12] used Discrete Cosine Transform (2D-DCT). They use lexicographic sorting after extracting 2D-DCT coefficients of each block in an image. Then find the equivalent distance between each block. If distance is less than the image is forged.

Ghorbani et. al.,[13] proposed DWT-DCT (QCD)-based copy-move image forgery detection in 2011. Authors used DWT and resolved the image into sub-bands and then performed DCT-QCD (quantization coefficient decomposition) in row vectors to reduce vector length. After lexicographically sorting the row vectors, shift vector is computed. Finally, the shift vector is compared with threshold and the forged region is highlighted.

Lin et. al.,[14] proposed an combined technique for splicing and copy-move image forgery detection in 2011. First, the authors converted an image into the grey. For splicing detection, the image is divided into sub-blocks and DCT is used for feature extraction and SURF is used for copy-move detection. The algorithm works in both splicing and copy move image forgery detection.

Leida Li et. al.,[15] this paper presents a method for detecting image forgery based on circular pattern matching. The tampered image is filtered and divided into circular blocks. Using Polar Harmonic Transform (PHT) rotation and scaling feature is extracted from each block. The feature vectors are lexicographically sorted and the manipulated regions are detected by finding the similar block pairs after applying post-processing.

4. PROPOSED APPROACH

The primary purpose of copy-move forgery is to detect similar regions in an image the duplicated regions are unknown both in size and shape. It is not easy to compare every pairs pixel by pixel, as well as it guides to higher computational complexity. In order to make efficient forgery detection an image window is used. Some appropriate and robust features are extracted from the image window, an efficient features extraction not only represent the whole image window, but also lower the dimension of feature vector, and due to less dimension of feature matrix, forgery detection algorithm has less computational complexity.

This paper propose copy-move forgery detection method based on the $(2D)^2PCA$. Firstly, a sliding window centred on every pixel of the forged image, then each window is passed through $(2D)^2PCA$ to obtain the $(2D)^2PCA$ coefficient matrix. The low dimensional statistical feature vector of each $(2D)^2PCA$ matrix is obtained and arranged in a feature matrix. In order to make similar windows adjacent, the feature matrix is lexicographically sorted. Finally, copy-move forgery

detection is performed using the adjacent pairs of feature vectors.

4.1 Pre-processing of the image

The proposed method operates in the luminance domain. Therefore, the colour image is first converted into gray scale by

$$I = 0.228R + 0.587G + 0.114B \quad (1)$$

where R, G, B denote the red, green and blue components of the image.

4.2 Feature extraction

(2D)²PCA is employed to extract features from the circular blocks. A feature vector is extracted from a block, so $(P - n + 1) \times (Q - n + 1)$ features can be obtained. Then they are arranged in a matrix F. It is straightforward to know that similar blocks should have similar feature vectors. However, if the matrix F is directly used to perform the block matching, the computation cost will be extremely high. In order to enhance the computational efficiency, the matrix is lexicographically sorted. In this way, similar features will be rearranged in the neighbouring rows, which facilitate fast block matching.

4.3 Block matching

Block matching is to find the similar block pairs by estimating the Euclidean distances of the feature vectors. Let Fi and Fj denote the ith row and jth row of F, then the Euclidean distance is computed as follows:

$$d(f_i, f_{i+1}) = \sqrt{\sum_{k=1}^{l} (f_i - f_{i+1})^2} \quad (2)$$

Where l is the dimension of the feature vector. Block matching starts from the first row of the matrix S.

4.4 Post-processing

It is easy to obtain the detection result by marking the block pairs. Most of the proposed methods generate the detection map in a block manner, namely the blocks are completely marked to generate the detection map. This may produce coarse boundary of the detected regions. In order to obtain finer boundaries, we propose to mark only the innermost pixels for each block.

5. CONCLUSION

The copy-move forgery detection is one of the emerging problems in the field of digital image forensics. In the last decade many forgery detection techniques have been proposed. An attempt is made to bring in various potential algorithms that signify improvement in image authentication techniques. The techniques which have been developed till now are mostly cable of detecting the forgery and only a few can localize the tampered area. There are many drawbacks with the presently available technologies. Firstly all systems require human interpretation and thus cannot be automated. Second being the problem of localizing the forgery. Since an image forgery analyst may not be able to know which forgery technique is used to tamper the image, using a specific authentication technique may not be reasonable. Hence there is still an utmost need of a forgery detection technique that could detect any type of forgery. An image forgery detection technique should detect any type of forgery with lesser computational complexity and high robustness.

6. REFERENCES

[1] Mohd Dilshad Ansari, S. P. Ghrera & Vipin Tyagi 2014 Pixel-Based Image Forgery Detection: A Review. IETE Journal of Education.

[2] Ashima Gupta, Nisheeth Saxena, S.K Vasistha 2013 Detecting Copy Move using DCT, International Journal of Scientific and Research Publications.

[3] Vivek Kumar Singh and R.C. Tripathi 2011 Fast and Efficient Region Duplication Detection in Digital Images Using Sub-Blocking Method. International Journal of Advanced Science and Technology

[4] A. C. Popescu, and H. Farid 2004 Exposing digital forgeries by detecting duplicated image regions. Dept. Comput. Sci., Dartmouth College.

[5] J. Zhang, Z. Feng, and Y. Su 2008 A new approach for detecting copy-move forgery in digital images. In IEEE International Conference on Communication Systems, China.

[6] XiaoBing KANG, ShengMin WEI 2008 Identifying Tampered Regions Using Singular Value Decomposition in Digital Image Forensics. IEEE International Conference on Computer Science and Software Engineering, Wuhan, Hubei.

[7] M. K. Bashar, K. Noda, N. Ohnishi, and K. Mori 2010 Exploring Duplicated Regions in Natural Images", IEEE Transactions on Image Processing.

[8] P. Kakar and N. Sudha 2012Exposing post processed copy-paste forgeries through transform-invariant features. IEEE Trans Inf Forensics Security.

[9] Muhammad, M. Hussain and G. Bebis 2012 Passive copy move image forgery detection using undecimated dyadic wavelet transform. Digital Investigation.

[10] P. Sutthiwan, Y. Q. Shi, S. Wei and N. Tian-Tsong 2010 Rake transform and edge statistics for image forgery detection. Proc. IEEE International conference on multimedia and Expo.

[11] Huang H, Guo W, Zhang Y 2008 Detection of copy-move forgery in digital images using SIFT algorithm. In: Proc. IEEE Pacific-Asia workshop on Computational Intelligence and Industrial Application.

[12] Fridrich J, Soukal D, Lukas J 2003 Detection of copy-move forgery in digital images. In: Proceedings of Digital Forensic Research Workshop.

[13] M. Ghorbani, M. Firouzmand, and A. Faraahi 2004 DWT-DCT (QCD) based copy-move image forgery detection. In 18thIEEE International Conference on Systems, Signals and Image Processing.

[14] S. D. Lin 2011 An integrated technique for splicing and copy move forgery image detection. In IEEE 4th International Congress on Image and Signal Processing.

[15] Leida Li, Shushang Li, Hancheng Zhu, Xiaoyue Wu 2014 Detecting copy-move forgery under affine transforms for image Forensics. Elsevier Computers and Electrical Engineering.

[16] Saba Mushtaq and Ajaz Hussain Mir 2014 Digital Image Forgeries and Passive Image Authentication Techniques: A Survey. International Journal of Advanced Science and Technology.

[17] Tu K.Huynh, Khoa V.Huynh, Thuong Le-Tien, Sy C.Nguyen 2015A Survey on Image Forgery Detection Techniques. IEEE RIVF International Conference on Computing & Communication Technologies, Research, Innovation, and Vision for Future (RIVF).

[18] Video Communication Laboratory. http://www.vcl.fer.hr/comofod/