Approaches for Detection of image forgery in Digital Images

[1]Vaishali Kulkarni, [2]Y. V. Chavan
[1,2]*Professors Department of E&TC*
[1,2]*RajarshiShahu College of Engineering, Pune University, Maharashtra*

Abstract: **The forgery in electronics and digital media is not new, which can be done actively or passively. Even digital images are forged and it is very difficult to identify the original one. Forgery is not new, it needs the details about the system in which the forgery is to be done. This paper discusses the forgery done in various types of images first and then the approach or the methodology adopted to detect this forgery. Various methods are adopted for different levels of forgery.**

Keywords: block based forgery, forgery detection, image forgery, key-point based forgery.

1. INTRODUCTION:

Digital image forgery is the process of changing some part or portion of the image so as to reflect the forged image as original one. Some of the digital image forgeries are copy-paste, region duplication, image splicing forgery. The software tools used for editing of images are used effectively for doing or making such changes in the original copy.This is very crucial needs to be detailed. Therefore there is need for detecting such doctored images.Digital image forensics or blind image forensics is capable of detecting digital image forgery.

1.1 Types of forgery

Broadly the type of images decides the type of forgery. So digital image forgery detection methods are divided into two categories i.e., active and passive. In Active methods watermarks and signatures are introduced in digital images to identify the authenticity of the images, but most of the images do not have this kind of added identity. So passive methods are used to verify the authenticity and integrity of the images. The copy-move forgery detection is one of the common types of digital forgery detection which tries to detect the tampering on the images

In Copy-Move forgery, a part of the image itself is copied and pasted into another part of the same image. This is usually performed with the intention to make an object “disappear” from the image by covering it with a segment copied from another part of the image. Textured areas, such as grass, foliage, gravel, orfabric with irregular patterns, are ideal. For this purpose, the copied areas will change with the background and the human eye cannot easily identify any suspicious artifacts. As the copied parts come from the same image, its noise component, color palette, dynamic range, and other important propertiesare compatible with the rest of the image. Thus these will not be detectable using methods that look for incompatibilities in statistical measures.

Copy-Move Forgery Detection (CMFD) are either block based or key-point based. In block based method it subdivides the method into rectangular region and for every such regions, feature vector is computed. These feature vectors are subsequently matched. (eg: PCA, KPCA, DWT, SVD method for feature extraction). In keypoint based method features are computed only on image regions of high entropy and the features are then matched within the image (eg: SIFT, SURF method for feature extraction) [16].

In this paper all such issues are organized as section. In section I an exhaustive discussion on various forgery detection method is done. In section II some of the forgery detection methods are compared for its efficient detection based on their application.

SECTION I

Aaron Langille et.al [1] proposed a detection method using Zero-Mean Normalized Cross Correlation (ZNCC). In this the input image is segmented into blocks. These blocks are sorted using a kd-tree based method which groups the blocks of identical and similar intensity patterns. Matching technique such as ZNCC is used to measure the similarity of neighbouring blocks from the sorted block array. The detected duplicated regions are encoded using a colour image.

Qiumin Wu etal [2] used Log Polar based scheme for revealing duplicated regions in digital images. Log Polar based approach is used to detect forgery even if copied area has been rotated and scaled. Log Polar fourier transform is computed on the image blocks to approximate DFT and interpolation operations. Log polar fast fourier transform (LPFFT) algorithm involves fractional fourier transform which is based on pseudo polar grids with computation complexity. Pseudo polar grid is converted to log polar grid and region duplication is detected. This method focuses on low complexity feature extraction. The optimized DSP can be better for giving good results in this algorithm

Alin C popescu et al [3] proposed a technique for detecting traces of digital tampering in the absence of any form of digital watermark or signature. Digital forgeries was exposed by detecting traces of resampling in which resampling introduces specific statistical correlations and these correlations can be automatically detected in portion of the images (uncompressed TIFF, JPEG AND GIF images with minimal compression). A broad range of resampling rates can be detected and simple counter attacks can be identified. Problem here is that this technique is not able to uniquely identify the specific resampling amount, as different samplings appear themselves with similar periodic patterns.

M.K.Bashar et al [4] proposed a method for detecting forgery in the presence of flip and rotation. Initially an unknown color image is first converted into its gray scale version, which is then divided into small overlapping blocks. Each block is transformed by DWT or KPCA. In the first case, transform coefficients are arranged into a vector according to decreasing local variances of the wavelet coefficients. In the second case, KPCA based projected data is arranged into a vector. The whole image is then represented by a matrix, where each row vector corresponds to a block. Lexicographic sorting is then applied to the matrix, which is used to label similar block pairs for the duplication detection. This method extracts 'Translation', 'Flip' or 'Rotation' duplication but it cannot handle some other geometric operations, e.g., scaling and shearing. So the computationalload remains high.

Saiqa Khan, Arun Kulkarni [5] described the blind image forensics approach for detecting copy-move forgery. DWT (Discrete Wavelet Transform) is used to reduce the dimension of forged image.This compressed image is divided into overlapping blocks of fixed size. Lexicographic sorting is used to sort these blocks, using phase correlation duplicated blocks gaps are identified.Duplication map is used to display the detected forgery which gives count of pixels forged. This approach improves the accuracy of detection and also reduces the time needed for the detection process. This algorithm works even for the images with more noise and JPEG quality level changes. This algorithm has lower computational complexity but duplicated regions with rotation through angles and scaled regions cannot be detected.

DongmeiHou et al [6] proposed a new image division method to detect image copy-move forgery. First, discrete wavelet transforms (DWT) is applied to the input image which is forged to reduce the dimension. The reduced dimension representation is divided into nine sub-images by using "crossing shadow" division. Phase correlation and pulse are calculated to obtain spatial offset between the copied and the pasted part.Using this method the copy-move regions can be easily located by virtue of pixel matching. To improve the detection the mathematical morphological operations were used. This has advantage of low computational complexity and has wide implementation. Copy and pasted regions lie in different sub-images.

Irene Amerini et al [7] proposed SIFT features-baseddetection. Since they are robust to scaling, rotation and also to affine transformations, these properties are well-suited for the detection of forgeries in images. Its powerfulness to detect copy-move attack and to trace back the geometric transformation occurred has been witnessed by specific experimental results. Initially feature extraction matching is done by SIFT method.Then hierarchical clustering is applied and finally geometric transformation estimation is done and the tampered image is detected.

Preeti Yadav et al. [8] worked on Copy-Move Image Forgery Detection using the algorithm based on Discrete Wavelet Transform (DWT) which is used to detect such cloning forgery. In this technique DWT (Discrete Wavelet transform) is applied to the input image to yield a reduced dimensional representation. After that compressed image is divided into overlapping blocks. These blocks are then sorted and duplicated blocks are identified. Due to DWT usage, detection is first carried out on lowest level image representation so this Copy-Move detection process increases accuracy of detection process. This algorithm has lower computational complexity, since exhaustive search for identical blocks is performed only on the image at the lowest resolution. This algorithm gave best performance for detection of small size copy move forgery.

Xu Bo et al. [9] a fast method to detect image copy move forgery based on the SURF (Speed up Robust Features) descriptors, which are invariant to rotation, scaling etc. It involves key-point detector and descriptor. The key-point is detected using Fast-Hessian detector and the SURF descriptor are constructed by extracting the square regions around the interest points and the matching of keypoints are done and the duplication can be determined. This method can detect the copy-move forgery quickly, and can stand certain transformations and post processing such as, scaling, rotation, noise blurring etc.

Weihai Li et al [10] proposed forgery of JPEG image using Block artifact grid extraction. A new JPEG image forensics approach is proposed to detect copy-paste forgery based on the checking the mismatch of block artifact grid.The image is partitioned into blocks using
DCT grid which is the horizontal lines and the vertical lines. And a block artifact grid (BAG) is the grid embedded in an image where block artifact appears. The DCT grid and BAG are matched together in undoctor images. When an image slice is moved, the BAG within it also moves.This technique works well even if the copied area came from the same image or not but only if source image is JPEG compressed. it even works if the doctored image is truncated.

Yi-Lei Chen et al [11] discovered new traces caused by recompression and use these traces to detect the recompression forgeries. Quantization is the critical step in lossy compression which maps the DCT coefficients in an irreversible way under the quantization constraint set (QCS) theorem. Initially it is derived that a doubly compressed image no longer follows the QCS theorem and then proposed a novel quantization noise model to characterize single and doubly compressed images. In order to detect double compression forgery, the uncompressed ground truth image using image restoration techniques is proposed. The proposed approach can successfully locate the forged region as small as 8x8 blocks, either with aligned or misaligned block boundary cases

Zhang Ting et al [12] proposed Singular value decomposition method to detect and locate duplication regions in tampered images. Image feature extraction and block similarity matching are the two major steps in detection which involves dividing an image into small overlapped blocks, then comparing the similarity of these blocks and finally identifying the duplicated regions. Steps involved in this method are

Step1: partitioning the image into small overlapping blocks

Step2: for each block SVD is applied and singular feature vector is extracted.

Step3: Block similarity matching is done.

Step4: identifying the tampered regions and mapping by a region map which shows duplicated regions.

This method has low computational complexity and is more robust to scaling, rotation, noise contamination and gaussian blurring etc but it has weak performance to resist JPEG compression and fails to say which is copied and which is pasted in duplication region.

Mehdi Ghorbani et al [13] proposed an algorithm based on Discrete Wavelet Transform
(DWT) and Discrete Cosine Transform Quantization Coefficients Decomposition (DCT-QCD) to detect cloning forgery. Initially gray scale is considered and the image is resolved into its discrete wavelet transform in which the image is approximated by extracting the low frequency sub band only. Discrete CosineTransformQuantizationCoefficient decomposition (DCT-QCD) is performed on each of the row vectors to reduce vector length. The rows of the matrix are lexicographicallysorted. For each pair of adjacent rows associated normalized shift vector is computed. Finally, the shift vectors with a count greater than some thresholds are examined, the corresponding pair of positions in the image are found.This work preserves the application of Discrete Cosine Transform Quantization Coefficient Decomposition (DCT-QCD) in reducing the dimension of the feature vector while reducing the dimension of the image using DWT.

A. N. Myna et al. [14] worked on copy move forgery detection by using wavelets and log polar mapping method. Wavelet transform is first applied to the input image to get a reduced dimension representation. Then exhaustive search is made to identify the similar blocks in the image by mapping them to log polar coordinates and using phase correlation as the similarity criterion. Only the matched blocks are carried for comparison to the next level. This reduces the time needed for the detection process. Since exhaustive search for identical blocks is performed only on the images at the lowest resolution so this algorithm has lower computational complexity.The algorithm also works for images in which pasted regions have undergone any transformation such as rotation, scaling, etc., The approach works well on all the basic image formats (JPEG, BMP, PNG etc.).

X. Kang et al. [15] proposed Singular value decomposition technique which provides a new way for extracting algebraic and geometric features from the image. Reduced rank approximation theorem is used which reduces the dimensionality, decreases the effect of noise and enhances the desired signal. In SVD and reduced rank approximation of a matrix, the largest singular values composes feature vector and then image block similarity matching is made. Steps involved are

Step 1: An image is partitioned into small overlapping blocks

Step2: SVD is applied for each block and reduced rank approximation is obtained and singular values feature vector is extracted. All feature vectors are stored in matrix.

Step3: Lexicographically the rows of a matrix are sorted.

Step 4: Block similarity or identification matching by Euclidean distance is made. After the two blocks with the required similarity threshold have been found, the tampered image is detected.

Compared with [11] this method gives liableness and robustness against retouching details like JPEG compression, Gaussian noise addition etc.

Yang Wang et al. [16] used wavelet-based method for forgery detection. Here DWT coefficients are extracted.

S1: Initially the colour image is converted into gray scale images by calculating a weighted average of the red, green and blue components. If the original image is compressed such as JPEG image, decompression is applied before converting the colour.

Step 2: The image is then divided into overlapped blocks.

Step 3: Feature extraction is done by applying

2-D DWT to each block for two levels. For each level, features are extracted from the coefficients of low frequency approximation, horizontal and vertical high frequency subimages, which mainly contains noise is not used.

Step 4: Lexicographically sorting is applied and each feature vector is then compared with each of its following vectors until a vectors first feature is different with that of the current vector.

Step 5: Two vectors are compared in the matching step to find the similarity of the corresponding blocks.

Step 6: filtering is done to remove the detected duplicated regions if they are too small. After filtering, all duplicated regions are found. An output is then created to mark all of the duplicated regions

This method gives higher performance compared to DCT based detection method.

SevincBayram et.al [17] proposed a new approach for detection of digital images. Features are extracted from image blocks by using Fourier-MellinTransform (FMT).These features are not only robust to lossy JPEG compression ,blurry or noise addition but also to scaling and invariant transform. Lexicographic sorting is performed to find the similar blocks. To reduce the detection time counting blooming filter is used instead of lexicographic sorting method. FMT features can detect the duplicated region even if severe image manipulation is done.

B.L.Shivakumar et.al [18] proposed a technique to detect copy-move forgery detection using SURF and Kd-tree for multidimensional data matching. Initially the features are extracted using SURF and keypoint matching is done using KD-tree algorithm instead of lexicographical sorting .Then verification is performed and the duplicated region is detected. using this method forgery detection can be made with minimum false match for images with high resolution.

SECTION II

Fig [1] below shows the result of using the singular value decomposition method to identify the tampered image. To check the robustness of the algorithm,a copy-move tampering was done on a database of 100 images of size 256*256 pixels. Each image was either JPEG compressed, processed guassian blur filter or corrupted with guassian white noise.[15].

Fig 1 shows the results of 100 JPEG images with quality factor. JPEG quality factor are 50, 60, 70,80,90,100in (a) and (b). Guassian blur filter radius are 0,0.4,0.8,1.2,1.6,2.For these is shown (c) and (d) and guassian white noise is 25,30,35,40,45,50 in (e) and (f) [15].

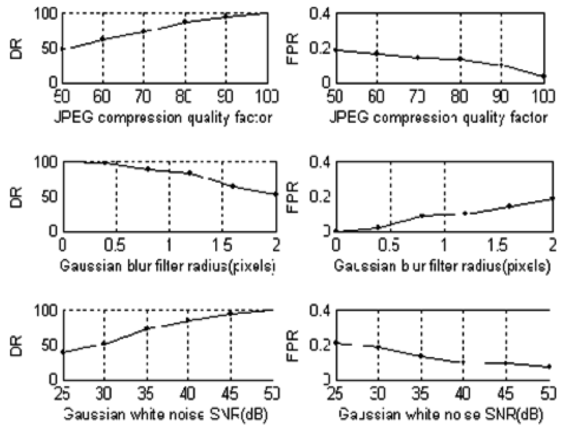

Fig 1 shows the results over 100 images.fig 1(a), 1(c), 1(e) shows the average detection rates and fig 1(b), 1(d), 1(f) shows the average no of false positive rates (FPR).

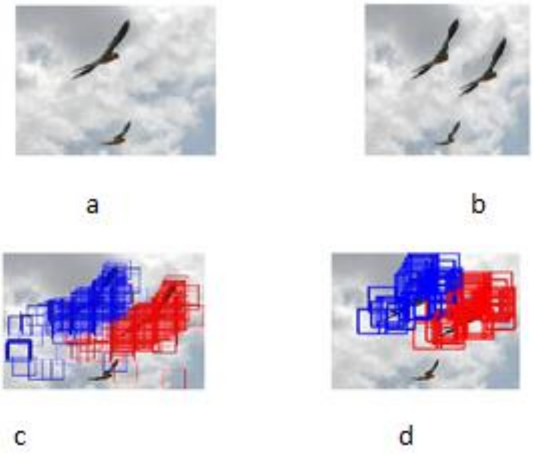

fig 2: forgery detection result (a) original bird image (b) tampered image (c)detection result for PCA method (d) detection result for DWT method

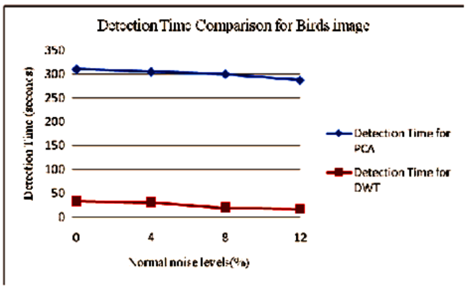

Fig 3:Detection time comparison under different normal noise(Nn) levels

Fig 3 shows the time detection under different noise values in which the noise are varied from 0%-12% .[4]

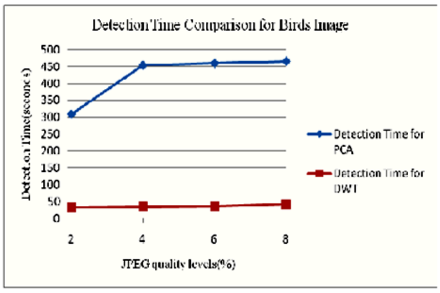

Fig 4**:** Detection time comparison under different JPEG quality (Jq) levels.

Fig 4 shows the comparative performance of the algorithm for tampered image under different JPEG quality levels [4].

Table 1: Performance results

Manipulation type	FMT	DCT	Eigenvalues
JPEG	20	40	50
Rotation	10^0	5^0	0^0
Scaling	10%	10%	0%

From the table 1 [18] it is seen that FMT is very robust to JPEG compression and forgeries can be detected even if the image is saved at JPEG quality factor of 20.It can also detect rotations upto 10^0 and is insensitive to scaling upto 10% compared to DCT and eigenvalues.

CONCLUSION

The purpose of this paper was to get acquainted with work done for detection of image forgery time to time. As technological support improves, these approaches need to modify for optimized results. Therefore wide and exhaustive survey have been done for this and are listed which will be useful for researchers working in forgery detection application of various digital images. This will also help to decide approach /method for application under the researchers preview. This gives the idea of using the approach based on the application such as digital images, photographs, satellite images and biomedical images.

ACKNOWLEDGEMENT

I would like to thank my guide, Dr. Prof.Y.V.Chavan for his great guidance and support. I am thankful to Principal Dr. R.K.Jain and post graduate faculty members of RajarshiShahu College of Engg, Tathawade, Pune.

REFERENCES

[1]. Aaron Langille ,"An efficient Match based Duplication Detection Algorithm", Proceedings of the 3rd Canadian Conference on Computer and Robot Vision (CRV'06) IEEE 2006, pp 1-8.

[2]. QiuminWu,Shuozhong Wang, and XinpengZhang,"Log Polar based scheme for revealing duplicated regions in digital images. IEEE Signal Processing 2011,pp 559-562

[3]. A.C. Popescu and H. Farid, "Exposing digital forgeries by detecting traces of resampling ", IEEE Transactions on Signal Processing, vol. 53, no. 2, pp. 758-767,2005.

[4]. M.K.Bashar, K. Noda, N. Ohnishi, K.Mori,"Exploring duplicated regions in Natural Images", IEEE Transactions on Image Process.,vol 99, 2011.

[5]. Saiqa Khan, Arun Kulkarni," Robust method for Detection of Copy-Move Forgery in Digital Images", 2010 IEEE International Conference on Signal and Image Processing, pp 69-73.

[6]. DongmeiHou, Zhengyao Bai, ShuchunLiu,"Image Copy-Move Forgery Detection based on "Crossing Shadow"Division"2011 IEEE, pp 978-981.

[7]. Irene Amerini, Lamberto Ballan, Roberto Caldelli, Alberto Del Bimbo and Giuseppe Serra, "GeometricnTampering Estimation by Means of A SIFT-Based Forensic Analysis", 2010 IEEE, ICASSP 2010, pp 1072-1705.

[8]. Preeti Yadav ,Yogesh Rathore ,Aarti Yadu," Detection of Copy-Move Forgery of Images Using Discrete Wavelet Transform", International Journal on Computer Science and Engineering (IJCSE), pp 56-58.

[9]. Xu Bo, Wang Junwen, Liu Guangjie and Dai Yuewei," Image Copy-Move Forgery Detection based on SURF Division IEEE 2010 International Conference on Multimedia Information Networking and Security, pp 889-892.

[10]. Weihai Li, Yuan Yuan, and Nenghai Yu," Detecting Copy-Paste forgery of JPEG Image via Block Artifact Grid extraction"

[11]. Yi-Lei Chen and Chiou-Ting Hsu," Detecting Doubly Compressed Images based on Quantization Noise Model and Image Restoration",2009 IEEE.

[12]. Zhang Ting, Wang Rang-ding," Copy Move Forgery Detection based on SVD in Digital Image", 2009 IEEE.

[13]. Mehdi Ghorbani, Mohammad Firouzmand, Ahmad Faraahi, "DWT-DCT (QCD) Based Copy-move Image Forgery Detection".

[14]. A. N. Myna, M. G. Venkateshmurthy, and C. G. Patil, "Detection of Region Duplication Forgery in Digital Images Using Wavelets and Log-Polar Mapping," in IEEE International Conference on Computational Intelligence and Multimedia Applications, Dec. 2007, pp. 371–377.

[15]. X. Kang and S. Wei, "Identifying Tampered Regions Using Singular Value Decomposition in Digital Image Forensics," in International Conference on Computer Science and Software Engineering, vol. 3, 2008, pp. 926–930.

[16]. Yang Wang, Kaitlyn Gurule, Jacqueline Wise, Jun Zheng, Wavelet Based region Duplication Forgery Detection 2012 Ninth International Conference on Information Technology- New Generations , pp 30-35.

[17]. Vincent Christlein, Christian Riess ,Johannes Jordan, Student Member Corinna Riess, and Elli Angelopoulou, "An Evaluation of Popular Copy-Move Forgery Detection Approaches", IEEE Transactions on Information Forensics and Security.pp 1-25.

[18]. S.Bayram, H. T. Sencar, and N. Memon, "An efficient and robust method for detecting copy-move forgery," in Proc. IEEE ICASSP, Washington, DC, 2009. Pp 1053-1056.

[19]. B.L.Shivakumar and S.SanthoshBaboo, "Detection of Region Duplication Forgery in Digital Images Using SURF", International Journal of Computer Science Issues, Vol. 8, Issue 4, No 1, July 2011, pp. 199-205.

………..

1. Vaishali Kulkarni have completed B.E. Electronics in June 2001 from Karnataka University, Dharwar. She is at present working as Lecturer in Electronics and telecommunication Engg at RajarshiShahu College of Engg, Pune and has experience in teaching of 5-years. She is now pursuing her Master of Engineering in Digital System from Pune University, MS, India. Her area of interest is digital image processing. She is a member of IEEE.

2.Dr. Y. V. Chavan has completed his Bachelor of Engineering in Electronics and Master of technology in 1989 and 1999 respectively from Nagpur University. He has completed his Ph D (Sep 2011) from RGPV, a state technological University, Bhopal. Previously he worked as Lecturer in Electronics at Pravara Rural Engineeing College Loni, Ahmednagar, (M.S.). He worked as Assistant Professor and Head of Department for Dept of E&TC at Amrutvahini College of Engineering, Sangamner, Ahmednagar (M.S.)-India. He also worked as Assistant Professor at Maharashtra Academy of Engineeing, Alandi, Pune.

He is at presently working as Vice-Principal at RSCOE,Tathawade,Pune. His area of interest is Modeling and Simulation and its implementation using VLSI.

He has interest in Computer Network and published 3/e on the same topic with Umesh Publications, New Delhi (India). He is actively involved in IEEE Student oriented activities. He is instrumental in starting 4-5 IEEE student branches under Pune University. He is senior member of IEEE life member of ISTE, Member of IETE. He is Exe-com member for IEEE Pune Section. He has published 13Journal Papers in National/International Journals and 15-papers in National/International Conferences.

3. Dr. D. S. Boramaneworking as Principal at RSCOE, Tathawade, Pune. He has done his B.E. (EC), M.E. (CSE) and PhD in Electronics and Telecommunication in 2003 respectively. He has guided four PhD students and eight students are pursuing PhD. He has experience of 25 years. He has guided 15 post graduate dissertations in the field of electronics. He is the life member of ISTE, member of ISCEE Roorkee, member of CSI, fellow member of IETE, senior member of IACSIT, Singapore. He has published about 60 papers in various national, international journals and conference. He is the key person for framing various curriculums at university of Pune.