Detection of Digital Forgery Image using Different Techniques

Mehak[#1], Tarun Gulati[*2]

[#]Research Scholar, Deptt. of ECE, MMEC, MMU, Mullana, Ambala, Haryana, India
[*]Associate Professor, Deptt. of ECE, MMEC, MMU, Mullana, Ambala, Haryana, India

Abstract: *In present world, digital uprising made it very dominant technology to approach, share and store any pictorial information and evidences. Though digital technology has many rewards as it play a significant role in various fields like forensic investigation, medical imaging, courtrooms and journalism where digital image used as authenticated proofs, it can be used as misleading tool also. These misleading or say editing tools modify the images to make a forged image and there can be a many reasons behind this occurrence of forgery as to conceal something in an image in order to produce false proof referred as copy move forgery effect , to enhance image or to emphasize particular objects etc. So, there is a strong demand for robust and valid secured method to find out whether picture is forged or not. In this paper, review of various techniques related to block based and key-point based methods to find out the copy move forgery effect is presented.*

Keywords: *Image retouching. Image splicing, Copy-move forgery, Block Based, Key-point Based*

I. INTRODUCTION

Digital Image tampering has become so common these days because of large amount of digital images present all over the world. This success of forgery is due to revalorization of original images done by the intuitive software like Photo editing tools, computer graphics and Corel draw etc., [1] in such perfection that no one can easily visualized these forgery attacks. Such a will-fully modification in image can become a forgery if it changes the semantic of the original image which termed as digital image tampering. There are many techniques for image forging like image retouching, image splicing and copy move forgery etc. If we talk about image retouching here, some features such as background may be changed by adding some attractive colors. In image splicing, different fragments from multiple images are overlying into a single composite image where visual message of digital image may change more aggressively then image retouching ([2], [3]). But in Copy Move forgery, image is completely changed by copied one region of an image and pasted onto another region of the same image in order to produce false image and to hide something in image [3]. All have strong impact on original image and hard to depict. These techniques are image forgery type where detection is done at the pixel level [3] and comes under Passive/Blind approach where no prior information required instead of Active approach as shown in Fig.1.

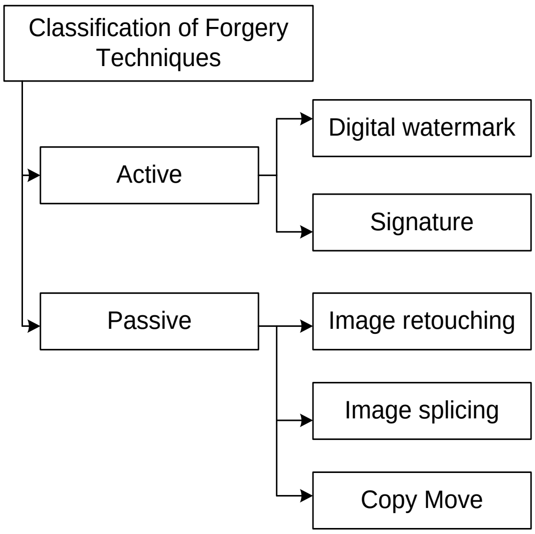

Fig 1: Classification of forgery Techniques

II. METHODOLOGY

In Copy-Move Forgery Detection Approach evidences are found only for detecting forged region when there exists a strong correlation between copied and pasted part. Intention behind this is either making an object copy from other part of the source image or to conceal object in image by covering it with small block from background of same image Also, to create an additional copy of an object already exiting in image by copied it into the desired location [4]. Since the copied region belongs to same image, properties of copied area like color palette, dynamic range, noise component and texture remains compatible with the rest of the image which make more challenging to detect copy move forgery attack ([5], [6]). Sometimes, forger may also use tools like retouching tool involve adding noise, compressed copied area and resampling tools include scaling and rotating the image which increases even more difficulties to detect forgery attack. This is a particular type of image manipulation technique [3] as shown in Fig. 2

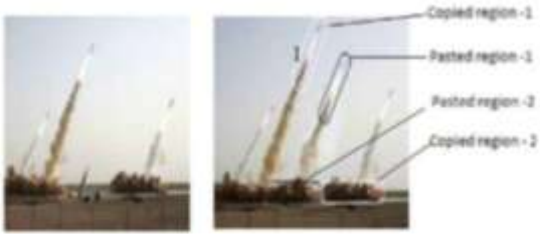

Fig 2: Example of image tampering which shown in press in July 2008 in which lower image display four successful missiles which are forge.

So, to overcome these difficulties Copy-Move Forgery Detection approach has been classified in two methods:

i. Block Based Method
ii. Key-Point based Method

In block based method, digital input image is firstly changed into gray scale and then divided up into overlapping or non-overlapping rectangular or circular blocks. For an digital image of size $M \times N$ and a block of n size $b \times b$, the number of overlapped blocks is given by $(M - b + 1) \times (N - b + 1)$from where the feature vector is computed [7]. In Key-point based method, key-points are computed by scanned the image for selected high entropy image region. Here, image is divided into key-points instead of blocks and feature vector is computed for every key-point [8]. Performance of these techniques at pixel level evaluate by parameters like complexity, Precision and Recall rate which are described as:

Precision = $Tp/(Tp + Fp)$

Recall rate = $Tp/(Tp + Fn)$

Where, Tp (True Positive) = Forged image declared as same as forged, Fp (False Positive) = Genuine image declared as similar to forged and Fn (False Negative) = Forged image declared as similar to genuine.

General framework for Copy-Move Forgery Detection: The typical work flow of copy-move forgery detection as shown in Fig.3 is almost same for both block based and key-point based approach by left over the step of feature extraction which is different for both methods [7].

Pre-Processing: The motive of this step is to improve the image by suppressing unwanted distortions or enhance some important features. This step is application dependent and optional. According to the requirement of application different type of processes like color conversion, low power filtering, dimension reduction are used.

Feature Extraction: In Block based method, feature vector is computed for each rectangular block but in case of Key-Point feature vector is computed for each key-point in high entropy region of an image. During feature extraction, features must nullify or avoid repetition in the original image.

Matching: The aim of matching is to identify the forged region by searching the blocks or key points with high similarity in features. Method used here such as Euclidean distance, K-d tree, g2nn, Best-bin first search.

Filtering: This scheme is used to reduce certain probability of false matches to claim the presence or absence of tampered region because dependence on single similarity criteria is not good.

Post-processing: This is the final step where matches show a common behaviour are preserved.

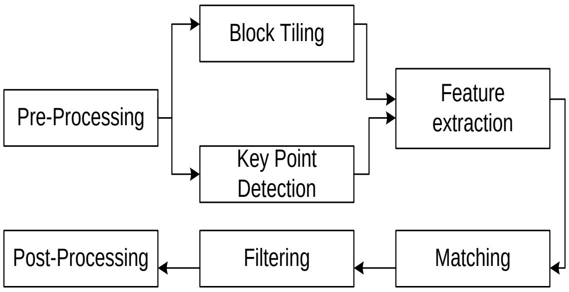

Fig 3: Basic process for detection of copy move forgery

III. Related work

Many researchers have performed work in this field. A review of few of them is presented here:

J. Fridrich et al. proposed an exhaustive search method based on DCT coefficients to localize tampered region. In this DCT coefficients are taken out from the blocks and put into an array which was lexicographically sorted to reduce computational cost. Then matching was performed by using quantized values of DCT coefficients and assuming neighbouring block pairs to be possibly forged. In this way method successfully calculated the forged part even when forged region is modified to combine it with background or saved in lossy JPEG format. But failed in noisy image and time taken which is not acceptable for matching [9]. Young-Dal Shin et al. proposed a fast exploration approach of copy move forgery image and it is the improved version of method defined in [9]. This method reduced the computational complexity more than conventional algorithm because in this author used a half block size in the spatial domain instead of 8×8 pixel block exhaustive search method and frequency domain for copy move forger image detection [1]. N.D.Wandji et al. proposed frequency based technique, in which firstly the RGB color image is converted into YC_bC_r color space and after that the RGB and Y components separated into fixed size block. The computed feature vectors was lexicographically sorted to search similar block pairs and output the duplicated region using Euclidean distance which act as a similarity criterion. Well performed in detecting copy move forgery into highly textured image robust to multiple copy move forgery, noise contamination, rotation up to 5 degrees and scaling but failed in produced accurate results in case of image blurring ([10], [11]). Beste Ustubioglu et al. proposed a method to calculate a threshold automatically. Threshold is a value that is used to compare similarity between feature vectors. Author utilized DCT-phase terms to restrict the range of the feature vector elements. They used element by element equality between feature vectors instead of cross-correlation or Euclidean distance and use compression history by Benford’s generalized law to determine the threshold value for the current test image automatically. Result of this method shows that it can detect the copied region under different scenarios and give high accuracy ratio with low false negative compared to similar work [12]. Alin C Popescu et al. presented a technique based on PCA to reduce the size of feature vector extracted from blocks of the image with high discriminated power, less computational cost and memory. This reduced representation help in predict small variations in image due to noise or losssy JPEG compression with less false positive. In this duplicated regions are detected by noting offsets with highest occurrence. But accuracy rate is lower for small size bocks and JPEG quality level less than 50 [13]. Harpreet Kaur et al. proposed dimensionality reduction based technique. In this technique after reducing the dimensions, PCA returns the principal component coefficient which represented by the rows and column of the matrix and the number of principle component was taken according to desired work. PCA technique gives good result when it was applied in area of Image Color Reduction and object orientation but also shown it’s insensitivity to relative scaling of original variables. Experimental results also shows that when PCA technique combined with key point based techniques (SIFT or SURF) improved the efficiency of speed [8]. Babak Mahdian et al. introduced an improved method of [1] based on Blur moment invariant to automatically localize tampered region. Firstly image is divided into blocks from which 24 blur invariants features are computed. Then feature set dimension was reduced by applying principle component transformation. Matching was done by using k-d tree to execute range queries in multidimensional data and after that created a duplicated image region map. Result shows the ability to localize tampered region even when copied image changes due to blur degradation, additional noise or arbitrary contrast but having high computational cost due to similarity threshold [14]. Kang et al. presented a novel scheme based on SVD for identifying the tampered region. It worked by first applied SVD on each block to obtain reduced-rank dimension and extract singular value SV feature having some properties of algebraic, geometric invariance and higher noise immunity. Then features were lexicographically sorted and matching done by Euclidean distance to find out similarity between blocks is higher than fixed value or not. Compared with ([9], [13], [14]) proposed result shows lower computational complexity and reliability against blur filtering, Gaussian noise and JPEG compression [15]. Saiqa khan et al. proposed a blind forensic passive approach related to DWT. In this technique discrete wavelet transform is used to return a reduced dimension representation which further separated into overlapping blocks. These blocks were sorted and matching performed on lowest level blocks by using Phase correlation criteria. Result shows that this technique good at detecting forged region in less time but not good in detection of copied region changed by rotation and scaling [16]. Jin Ryu et al. proposed a method based on Zernike moment to localize copy move forgery in tampered digital image. In this method firstly magnitude of Zernike moment was calculated from each overlapping block and then extracted feature was lexicographically sorted .After that Euclidean distance between pairs estimated and blocks with distance smaller than threshold are become candidate for forgery. The magnitude of Zernike moment is robust to rotation and resilient to international distortion like AWGN, blurring and JPEG compression. But result shows that invariances against rotation when practically performed had low performance due to the increased error rate during the interpolation step of rotation [17]. Sevinc et al. presented a new technique where features were based on FMT and counting bloom filter to give an effective and robust method for detecting copy move forgery effect. Counting bloom filter replaces the Lexicographic sorting and in this hashes or index values of features are compared instead of feature themselves. Experimental results shows the improvement in computational complexity because forged part detected accurately in less time as it reduced time from 25 sec (lexicographic) to 2 sec but at the expense of slightly reduction in robustness toward scaling and rotation [18]. Leida Li et al. proposed a technique that is LBP. It works by firstly divided the image into overlapping circular blocks from which feature vectors are computed using rotation invariant LBP. Then feature vectors compared and forged region located by tracking the corresponding blocks. Experimental result shows that the motive of author to solve the problem of detection forged region when copied region is rotated or flipped was successfully achieved. Also, demonstrate the robustness of method against blurring, JPEG compression and noise [19]. Guzin Ulutas et al. proposed a CCV method to detect copy move forgery by determining the similarity among the blocks. In this method, vector designates the coherence of color in a region and use spatial relationship in color information. When similarity between CCV designated to pixels in forged image region and original image found, forged area accurately detected. Author demonstrated that this method robust to only Gaussian blurring affects not all other post-processing effects [20]. Haung et al. proposed SIFT technique. This author used this technique for evaluated local statistical features of an image. Then for matching key-points best-bin-first search method used as similarity criteria. Experimental result shows that it is invariant to rotation and scale but lack in performance [21]. Himanshu Goyal et al. presented an approach to guide image forensic investigation based on SIFT. Author used photos of different contrast and improved the False Positive rate by checked intensity value of region of interest manually [22]. Amerini et al. presented two steps method. First is SIFT feature extraction and similar feature matching performed by generalized 2NN test. Last is estimation of geometric transformation. Result shows the success in detecting the multiple cloned regions but failure in localize the copied region accurately. This method also failed in detecting tampering image patch having maximum uniform texture such as salient key-points not covered by SIFT [23]. G.Zhang et al. presented a new technique based on SURF to detect copy move forgery effect into flat regions. This technique firstly extracted the key-points from the integral image and then feature matching and pruning is done. Then estimate region transforms and duplicated region identify using correlations adjustment by estimated transforms. This method invariant to rotation and detect region duplication in non-flat region also [24].

Ref. No.	Techniques used	Pro's	Con's
[10], [11]	DCT frequency based	Performed better in highly textured image.	Not accurate in case of image blurring, Uniform area lead to false matches.
[13]	PCA dimensionality reduction based	Reduced computational cost, reliable in lossy JPEG compression with less false positive.	Lower accuracy rate for smaller sized blocks, Not work well if SNR is small.
[14]	Blur moment invariant based	Well performed against blur degradation, additive noise, and arbitrary contrast.	Lack of efficiency in time and have high computational cost.
[15]	SVD dimensionality reduction based	Low computational complexity and Invariant to Retouching effect, higher noise immunity.	Failed to specify which part is copied and which is pasted.
[16]	DWT dimensionality reduction based	Excel in computational speed.	Not invariant towards affine transformation like rotation and scaling.
[17]	ZERNIKE Moment Based	Resistive to international distortion like AWGN, blurring and JPEG compression.	Lower performance towards geometrical transformation like scaling and rotation.
[19]	LBP block based	Invariant to rotation, flipping, noise blurring and JPEG compression.	Difficult to detect forgeries when region is rotated by general angles.
[20]	CCV block based	High accuracy ratio, Work well even when image is processed by Gaussian Blurring.	Cannot detect forgeries if other post-processing is done.
[18]	FMT block based	High accuracy and Less computational Time.	Expense of reduction in robustness toward scaling and rotation.
[23], [24]	SIFT, SURF Key-point based	Excellent speed, Robust to scaling and rotation, Detect multiple cloned regions, immune to noise.	Failed only in localize copy region accurately.

IV. Conclusions

In this era as one of the main challenging task in digital image forensic is to detect copy-move forgery effect. So, this paper mainly concerned how to detect image forgeries and how to compute performance of different techniques. There are various methods described for image forgery detection and showing limitations related to them. It can be seen that key-point based method seems more appropriate in large size images because of its excel in computational time and robustness towards geometric transformation, JPEG compression, noise blurring and good detection towards multiple cloned region as compared to block based which excel only in detect forged region accurately.

References

[1] Y. D Shin, "Fast Exploration of Copy-Move Forgery Image," Advanced Science and Technology Letters, vol. 123, pp.1-5, 2016.

[2] H. Goyal and T. Gulati, "A Review on Forensic analysis of digital image tampering," IJRIT International Journal of

Research in Information Technology, vol. 2, pp. 364-367, May 2014.

[3] M. D. Ansari, S. P. Ghrera and V. Tyagi, "Pixel-Based Image Forgery Detection: A Review," IETE Journal of Education, vol. 55:1, pp. 40-46.

[4] S. Sharmila, S. Prajakta and S. Hiral, "Image Forgery Detection Techniques for Forensic Sciences," International journals, ISSN-No: 2347-4890, vol. 2, Aug. 2014.

[5] M. Puri and V. Chopra, "A survey: Copy-Move forgery detection methods," International journal of computer systems, vol. 3, Sept. 2016.

[6] V. Christlein and J. Jordan, "An Evaluation of Popular Copy-Move Forgery Detection Approaches," IEEE Transactions on information forensics and security, pp. 1-26, 2012.

[7] Kusam, P. Abrol and Devanand, "Digital Tampering Detection Techniques: A Review," BVICAM's International Journal of Information Technology, vol. 1, pp. 125-132, 2009.

[8] H. Kaur, J. Saxena, and S. Singh, "Simulative Comparison of Copy –Move Forgery Detection Methods for Digital Images," International Conference on Journal of Electronics, Electrical & Computational, vol.4, pp. 62-66, 2015.

[9] J. Fridrich, D. Soukal and J. Lukas, "Detection of copy–move forgery in digital images," Proceedings of Digital Forensic Research Workshop, IEEE Computer Society, pp. 55– 61, Aug. 2003.

[10] N. D Wandji, S. Xingming and M. FahKue, "Detection of Copy-Move forgery in digital images based on DCT," International Journal of Computer Science Issues, vol. 10(2).

[11] A. Gupta, N. Saxena and S.K Vasistha, "Detecting a Copy move Forgery using DCT," International Journal of Scientific and Research Publications, vol. 3(5), pp. 1-4, 2013.

[12] B. Ustubioglu, G. Ulutas, M. Ulutas and V. V. Nabiyev, "A new copy move forgery detection technique with automatic threshold determination," Elsevier - International Journal of Electronics and Communications vol. 70, pp. 1076–1087, Aug. 2016.

[13] A. C Popescu and H. Farid, "Exposing digital forgeries by detecting duplicated image regions," Department of Computer Science, Dartmouth College, Tech. Rep. TR2004-515, 2004, pp. 1-11.

[14] B. Mahdian and S. Saic, "Detection of copy–move forgery using a method based on blur moment invariants", Forensic Science International, an international journal dedicated to the applications of medicine and science in the administration of justice, vol. 171, pp. 181-189, Sept. 2007.

[15] X. Kang and S. Wei, "Identifying tampered regions using singular value decomposition in digital image forensics," in Proc. Int. Conf. Computer Science and Software Engineering, 2008, vol. 3, pp. 926–930.

[16] S. Khan and A. Kulkarni, "An Efficient Method for Detection of Copy-Move Forgery Using Discrete Wavelet Transform," International Journal on Computer Science and Engineering, vol. 2, pp.1801-1806, 2010.

[17] S. J Ryu, M. J Lee and H. K Lee, "Detection of Copy-Rotate-Move Forgery Using Zernike Moments," Springer Proc. Int. Workshop Information Hiding, 2010, pp. 51–65.

[18] S. Bayram, H. T Sencar and N. Memon, "An Efficient and robust method for detecting copy move forgery," IEEE Trans. Image Processing, 2009.

[19] L. Li1, S. Li and H. Zhu, "An Efficient Scheme for Detecting Copy-move Forged Images by Local Binary Patterns," Journal of Information Hiding and Multimedia Signal Processing, vol. 4, pp. 46-56, 2013.

[20] G. Ulutas and M. Ulutas, "Image forgery detection using Color Coherence Vector," Electronics, Computer and Computation (ICECCO), pp. 107 – 110, Nov. 2013.

[21] Huang H, Guo W and Zhang Y, "Detection of copy-move forgery in digital images using SIFT algorithm,'' In: Computational Intelligence and Industrial Application, 2008 PACIIA'08 Pacific-Asia Workshop on IEEE, pp. 272–6, 2008.

[22] H. Goyal and T. Gulati, "Robust Copy-move Image Forgery Detection using SIFT," International Journal of Computer Science and Application, vol. 97, pp. 14-19, July 2014.

[23] Amerini I, Ballan L, Caldelli R, Del Bimbo A and Serra G, "A sift-based forensic method for copy–move attack detection and transformation recovery," Inf Forensics Secure IEEE Trans On. 2011; 6(3):1099–110.

[24] G. Zhang and H.Wang, "SURF based Detection of Copy-Move Forgery in Flat Region," International Journal of Advancements in Computing Technology (IJACT), vol. 4, September. 2012 doi:10.4156/ijact.vol4.issue17.61S.