A Review of Copy-Move Forgery Detection Techniques

Rajdeep Kaur/[1]Dept.of ECE(PG Student), Giani Zail Singh Campus College of Engineering and Technology Bathinda , India

Amandeep Kaur/[2]Dept.of ECE (Asst.Professor), Giani Zail Singh Campus College of Engineering and Technology, bathinda, India

***Abstract*— In today's digital world, authenticity and integrity of any image cannot be taken for granted. Gone are those days when image manipulation was limited to experts only. Digital photography, Photoshop and computer graphics have made image forgery both easier to commit and harder to detect. Amongst various image forgeries known, copy-move forgery stands as a serious threat to the society and image forensic experts. The success of this forgery is due to the fact that copied segment comes from the same image and hence, the properties such as color palette, dynamic range, noise level and texture remains compatible with the entire image, thus, making its detection difficult. Researchers have developed various techniques to counter this kind of attack based on exhaustive search and block matching approach. However, block matching is the most adopted approach due to its speed of operation and cost effectiveness as compared to exhaustive search. In this paper, we review some techniques based on Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT) Copy-Move forgery is a special type of image forgery. An image forgery is very easily performed due to extensive growth in software technologies. The purpose of Copy-Move forgery is to hide or conceal some region of the image with a copied portion of original image and pasted in same image in another area and as a result forged image is created. Copy-Move forgery detection techniques can be classified into two categories: 1) Block Based Methods 2) Key-Point Based Methods.**

Keywords- Image Forgery, PCA, SIFT

I. Introduction

Digital imaging has become fully developed to become the dominant technology for creating, processing, and storing pictorial memory and evidence. Though this technology has many advantages, it can be used as a misleading tool for hiding evidences. Because today digital image can be manipulated in such perfection that forgery cannot be detected visually. So, the security concern of the digital images content has arisen a long time ago and different techniques have been developed to check the authentication of the digital image. Copy- Move Forgery Detection techniques have been classified mainly into two approaches:

1) Block Based Methods
2) Key-Point based Methods

After that similar feature vector are matched to detect the forged region. In Key-point methods, image is divided into key-points and there is no image subdivision into blocks. Feature vector are computed for region having high entropy and after that matching is performed to detect the forged region. Firstly input image are converted into gray scale image and then the gray scale image is converted into overlapping blocks or key-points (according to the method) used for detecting forged region. Block based methods are able to detect forgery in flat regions and can handle multiple cloning. And block based methods are robust against JPEG compression and noise addition and gives exact location of tempered region. Key-point methods are invariant to geometric transformation such as scaling and rotation [12].

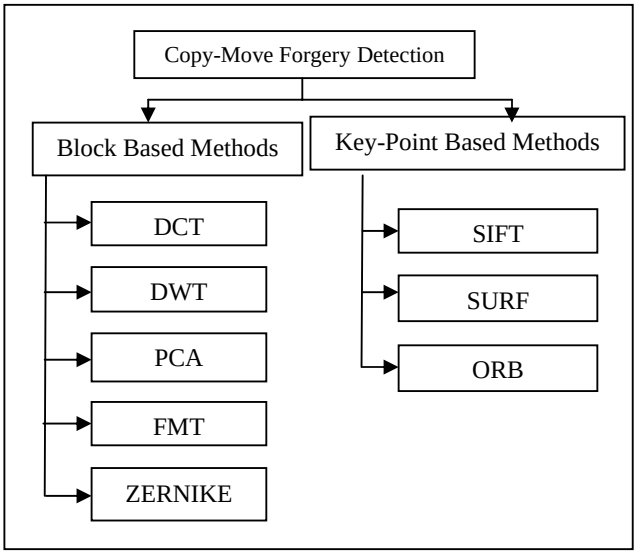

Figure 1.1 Classifications of Copy-Move Forgery detection Techniques

II. Framework for forgery detection system

Copy-Move image forgery detection can be done either by using block based or key-point based method or combination of both (as hybrid approach) in [12,15]. Figure 1.2 represents a general framework for copy-move image forgery detection.

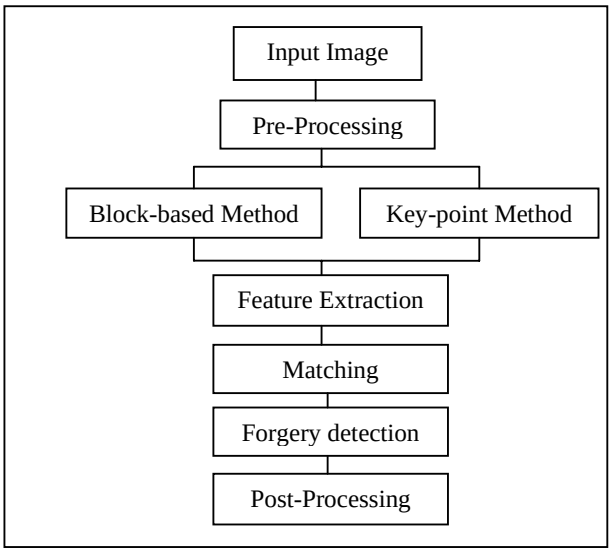

Figure 2.1 General Frame work for Copy-Move Forgey detection

- Pre-Processing**:** This process is application dependent. It involves image conversion from colored image to gray scale, image enhancement to remove the noise from input images.

- Feature Extraction**:** Feature extraction is the process to extract or finding features from input image for new representation of the image in good manner. Features should have two basic requirements: it should be avoid redundancy in the original image and reduce dimensionality of data.

- Matching: Matching is the process to find a high similarity or matching between feature descriptors and if similarity between feature descriptors is found than it is interpreted as a clue for duplicated regions. Various techniques of matching have developed for example Euclidean distance, KD tree, lexicographic sorting and g2NN (generalized 2 nearest neighbour).

- Post-Processing**:** When an image has been classified as non authentic; post processing helps to find out which transformation has been used between original area and its copy-moved version. Various algorithms have been proposed in literature for the same such as RANSAC (Random Sample Consensus), same Affine Transformation Selection (SATS).

III. Copy-Move Forgery Detection Techniques

Copy-Move forgery detection techniques are classified according to literature into two categories as Block based methods and Key-point methods.

A. Block Based Method

In block based methods, input image is firstly divided into overlapping blocks and then feature extraction of each block are done and then matching is performed between each block to detect the forged region[15]. Copy–Move forgery detection using Discrete Cosine Transformation (DCT) technique, firstly the color image was converted from RGB color space to YCbCr color space and then the R,G,B and Y-component was splitted into fixed-size overlapping blocks and, features extracted from the DCT representation of R,G,B and Y-components image block. The feature vectors obtained then lexicographically sorted to make similar image blocks neighbours and duplicated image blocks identified using Euclidean distance as similarity criterion [10]. Using DCT was better than using PCA for detecting Copy- Move forgery into highly textured images [6].

Later on, discrete wavelet transformation used to detect copy-move forgery in digital images. In DWT, instead of dividing the input images into overlapping blocks; input image was divided into four sub-bands. The lower frequency band was further subdivided into overlapping blocks to reduce the no. of blocks which speeded up the process and more energy concentrated to lower sub-band [7]. The discrete wavelet transformation was used to reduce the dimensionality and advantage of DWT over Fourier transforms is temporal resolution. It captured both frequency and location information (in time).It is combined with SVD and SIFT [15].

In PCA (Principal component analysis) was a block based method and PCA was used to reduce the dimension of image. Firstly, test image and its dimensions were reduced using PCA. PCA returns the principal component coefficients of a matrix (say X). Rows and column of this matrix represents coefficients for one principal component. And number of principal component columns was taken according to work. PCA is combined with SIFT (scale invariant feature transform) or SURF (speeded up robust feature) to combine advantages of both block based and Key-Point based techniques to enhance the speed and evaluation metrics to detect the Copy-Move forged region.[12].

FMT is a Fourier Millen transform. In mathematics, the Mellin transform is an integral transform that may be regarded as the multiplicative version of the two sided Laplace transform. In this technique, extraction of features from the image blocks would not only be robust to lossy JPEG compression, blurring, or noise addition, but also known to be scaling and translation invariant [2].

Zernike moment was used to localize the Copy-Move forgery region in digital images. The magnitude of Zernike moment was algebraically invariant against rotation and the proposed method was detecting forged region even though rotated. This scheme was also appropriate to detect forged region by Copy-Rotate-Move forgery and resistive to international distortion such as additive white Gaussian Noise (AWGN), JPEG compression and blurring [4]. In this proposed scheme Copy-Rotate-Move forgery was performed rotations in the range 0° to 90°.The proposed scheme

theoretically invariant against rotation but actual results had lower performance than expected. Seung Jin et. al [4] had evaluated that there might be a two reasons for the performance degradation. At first, the Zernike moment calculated on discrete domain had inherent quantization error since the moment was originally defined on the continuous domain. Secondly interpolation caused by the rotation step increased the error rate.

In proposed scheme to detect the Copy-Rotate-Move region, firstly to extract the feature vectors of the given block, magnitude of Zernike moment calculated and then vectors were lexicographically sorted and measure the similarity between adjacent vectors. Finally, the suspected region was measured by Precision, Recall and F1-measure. Zernike moments had rotational invariance, and made scale and translational invariant, making them suitable for many applications. Zernike moments are accurate descriptors even with relatively few data and points. Reconstruction of Zernike moments can be used to determine the amount of moments necessary to make an accurate descriptor.

B. Key-Point Based Methods

In Key-Point based methods, input or test image is firstly divided into corner or isolated points to provide local features description of the image. The Key-Point algorithm for detecting of copy-move forgery starts by extracting high entropy regions i.e. Key-points. Feature descriptors are extracted from these features. These feature descriptor are compared with each other to detect the matched Key-Points and hence forgery detected [12]. The well known Key-Point descriptors are SIFT (Scale Invariant Feature Transform) and SURF (Speed-Up Robust Feature) and ORB (Oriented Rotation and BRIEF) has been discussed as follows:

1) Scale Invariant Features Transform (SIFT):

SIFT is very efficient method to detect duplication region. It is not only just scale invariant but also provides good detection results for rotation, illumination and invariant viewpoint changes. The Key-Point extracted by SIFT are invariant to rotation and scaling because magnitude of each Key-point is different [1]. The descriptors are assigned to local interest points as Key-points. After that each descriptors are compared with each other and matched descriptors are used to detect the Copy-Move forged region. SIFT matching-based detection method can locate matched Key-point with rotating and scaling. The extraction of Features using SIFT algorithm applies into four stage filtering. The applications of SIFT algorithm are object recognition using SIFT Features, Robot localization and mapping is used to determine 3D estimates for Key-point locations. As the robot moves, it localizes itself using feature matches to the existing 3D map. This provides a robust and accurate solution of the problem of robot localization in unknown environments. SIFT features are used in Panorama stitching or image stitching (Panorama is any wide –angle view or representation of the physical space or a three-dimensional model) for a fully automated Panorama reconstruction from non-panoramic images. SIFT features are used for 3D object recognition and 3D modeling in context of augmented reality. Block diagram of object recognition using SIFT as shown in figure given below:

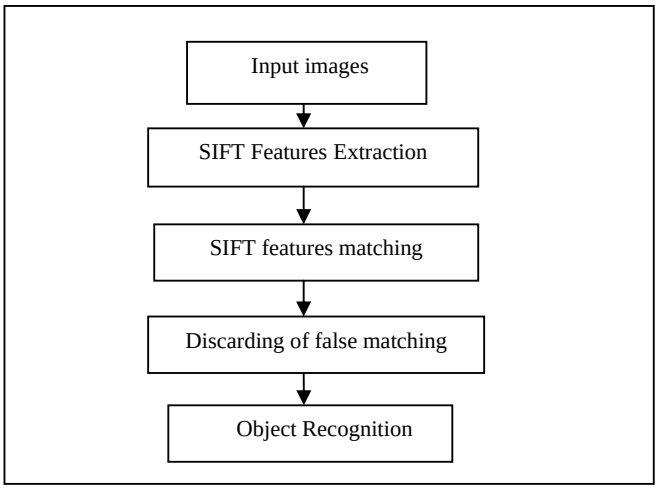

Figure 3.1 Block diagram of Object Recognition using SIFT

SIFT algorithm mainly consist four types of filtering to extract the sift features from the test image [7, 12, 16].
1. Scale-Space Extrema detection
2. Key-Point localization
3. Orientation Assignment
4. Key-Point Descriptor

Scale- Space Extrema Detection: This stage of filtering used to identify those locations and scales that were identifiable from different view of the same image [16]. This was based on scale-spaced function. And this must be further based on Gaussian function. The scale spaced function was defined as:

$$L(x, y, \sigma) = G(x, y, \sigma) * I(x, y) \quad (1)$$

#

Where * was a convolution operator and G(x, y, σ) was Gaussian operator and I(x, y) is input images. Difference of Gaussian was used to find out the Scale-Space Extrema and difference of Gaussian was calculated by difference of input images, one with k time the scale of other, as given follow:

$$D(x, y, \sigma) = L(x, y, k\sigma) - L(x, y, \sigma) \quad (2)\#$$

To detect the local minima and local maxima D(x, y,σ) each point was compared with its eight neighbours at the same scale and 9 neighbours were up and down one scale.

Key-Point Localisation: This step used to eliminate the key-points those had low contrast or poorly localized at on edge. This was calculated by Laplacian. If the location of extremum as below the threshold value then key-point with low contrast was discarded.

Orientation Assignment: This step was used to assign orientation to key-point based on local image properties. The approach taken to find the orientation of the key-point involves some steps as follow:

- Use the Key-points scale to detect the Gaussian smoothed image L.
- Compute m, which was a gradient magnitude.
- Compute θ, orientation.
- Form an orientation histogram from gradient orientations of the sample points.
- Now locate the highest peak of histogram. Use this peak and any other local peak of 80% height of this peak to create a local key-point with that orientation.
- Some points will be assigned multiple orientation points.
- After that fit a parabola to the 3 histogram values closest to each peak to interpolate the peaks position.

Key-point Descriptor: The local gradient data was used to create key-point descriptor. The gradient information was rotated to line up with orientation of key-point and then weighted by Gaussian with variance 1.5*Key-point scale. The data was used to create set of histograms over a window centered on the key-points.

2) Speeded-up Robust Features (SURF)

SURF is used to extract features and it is a robust local feature detector. SURF is based on sums of 2D Haar Wavelet responses. It make an efficient use of Integral images [8].SURF's detector and descriptor is said to be faster and at same time robust to noise, detection displacements and geometric and photometric deformations. SURF is invariant to geometric transformation such as scaling and rotation. It is able to detect multiple cloning and has high computational efficiency. SURF detector is not suitable for detecting image tempering in case of highly compressed JPEG image and flat duplicates regions. It does not give good results when tempered region is small [3, 8].
SURF features can be extracted using the following steps:

- Integral Image
- Key-point detection
- Orientation Assignment
- Feature Descriptor Generation

Integral Image: Integral images was used to increase the computation speed and performance, its value was calculated from an upright rectangular area, the sum of all pixel intensities was calculated by the formula,

$$\Sigma = A + D - (C + B) \quad (3)\#$$

A, B, C and D were vertices of rectangular area. The integral image I∑ calculated by the sum of the values between the point and origin.

$$I\Sigma(x,y) = \Sigma\Sigma I(x,y) \quad (4)\#$$

Key-Point Detection: The key-points were blob like structure and located at where determinant was maximum. The extraction of the key-points using SURF include some steps. Firstly, Laplacian of Gaussian was approximated with a box filter. To creating the scale-space of the image, convolution applied to an image with varying size box filter. Secondly, determinant of hessian matrix was calculated for detection the extreme points. If determinant of the hessian matrix was positive that means, both the Eigen values were of the same sign either both were negative or both were positive. Hessian matrix was represented by,

$$H(x,\sigma) = \begin{bmatrix} Lxy(x,\sigma) & Lxy(x,\sigma) \\ Lxy(x,\sigma) & Lyy(x,\sigma) \end{bmatrix} \quad (5)$$

Where Lxy (x,σ) was the convolution of the Gaussian second order derivative with the image I in point x, and similarly Lxy (x ,σ) and Lyy (x,σ).

Orientation Assignment: The key-point orientation in SURF algorithm was done by creating a circular area around the key-points. Then Haar wavelets were used for the orientation assignment. It also increases the robustness and decreases the computational cost. After calculated key-points or interest points using Haar wavelet then calculate key-point descriptor.

Feature Descriptor Generation: In this step, the SURF descriptors were constructed by extracting square regions around the interest points. These were oriented in the directions assigned in orientation assignment. Now window was split up in 4*4 sub-regions to retain some spatial information. And then Haar wavelets are extracted at regularly spaced sample points. In this step order to increase robustness to geometric deformations, the Haar wavelets were weighted with a Gaussian, centered at the interest point. The wavelet responses in horizontal directions d_x and d_y (vertical directions) are summed [3].

$$V = (\Sigma Dx, \Sigma Dy, \Sigma|Dx|, \Sigma|Dy|) \quad (6)$$

3) Oriented FAST and Rotated Brief (ORB):

ORB is based on FAST detector and recently developed BRIEF descriptor. Due to this reason, it is called ORB (Oriented Fast and Rotated Brief). Both these techniques are attractive due to good performance and low cost. Fast and its variants [9, 13] were the method of choice to finding the key-points in real time systems. SIFT and SURF detectors include key-point orientation but FAST detector does not include key-point orientation. There were many ways to determine the key-point orientation, histogram of gradient and approximation by block patterns. ORB is rotation invariance and resistive to noise. The efficiency ORB was experimentally determined on several real-world applications i.e. object detection and patch tracking on smart phone. Experimental result shows that ORB

is two order faster than SIFT, while performing as well as in many situations.

IV. Error Measures and Evaluation Metrics

The performance of the Copy-Move forgery detection methods were also measured by detection error at two levels, namely image level and pixel level [11].

Table 1 Evaluation Metrics

Sr. no.	Image level	Mathematical Expression	Pixel level	Mathematical Expression
1.	False Positive Rate(F_P)	$FP/FP+TN$	Precision	TP/(TP+FN)
2.	False Negative Rate(F_N)	$FN/FN+TP$	Recall	TN/(TN+FP)
3.	–	–	F_1	$2.\frac{precision*recall}{precision+recall}$

REFERENCES

[1] David G. Lowe., (2004), "Distinctive Image Features from Scale-Invariant Key-Points", International Journal of Computer Vision 60(2), pp.91-110.

[2] Sevince Byram, Husrev Taha Sencar, Nasir Mamoon., (2009), "An efficient and Robust Method for Detecting Copy-Move forgery", IEEE International Conference on Acoustic, Speech and Signal Processing, pp. 1053-1056.

[3] Xu Bo, Wang Junwen, Liu Guangie and Dai Yuewei., (2010), "Image Copy-Move forgery Detection Based on Surf", International Conference on Multi-media Information Networking and Security, pp.889-892.

[4] Seung Jin Ryu, Min Jeong Lee, Heung-Kyuulee., (2010), "Detection of Copy-Rotate-Move Forgery Using Zernike moments", International Conference on Information, vol.387, pp. 51-65.

[5] Ethan Rublee Willow Garage, Menlo Park, (2011), "ORB: An efficient alternative to SIFT or SURF", IEEE International Conference on Computer Vision, pp. 2564-2571.

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

[7] Mohammad Farukh Hashmi, Aaditya Hambarde., (2013), "Copy move forgery detection using DWT and SIFT", International Conference on Intelligent System Design and applications, pp.188-193.

[8] K. Kiruthika, S. Devi Mahalakshmi, K. Vijayallakshmi., (2014), "Detecting Multiple Copies of Copy-Move Forgery Based on SURF, International Journal of Innovative Research in Science, Engineering and Technology, vol. 3, pp. 2276-2281.

[9] Mohan Ramakrishna, Shylaja SS., (2014),"Is ORB efficient Over Surf for Object Recognition?", International Journal of Advanced Research in Computer Engineering and Technology, 3(8), pp. 2783-2788.

[10] Nathalie Diane Wandji, Sun Xingming, Moise Fah Kue., "Detection of Copy-Move forgery in digital images based on DCT", International Journal of Computer Sciene Issues, 10(2).

[11] Jian Li, Xiaolong Li, Nin Yang, Xingming., (2015), "Segmentation Based Image Copy-Move Forgery Detection Scheme", IEEE Transactions on Information Forensics and Security,10(1) , pp. 507-518.

[12] Harpreet Kaur, Jyoti Saxena, and Sukhjinder Singh., (2015), "Simulative Comparision of Copy –Move Forgery Detection Methods for Digital Images" International Conference on Journal of Electronics, Electrical & Computational, vol.4, pp. 62-66.

[13] Prashant Aglave, Vijaykumar., (2015), "Implementation of High Performance Feature Extraction Method Using Oriented Fast and Rotated Brief Algorithm", International Journal of Research in Engineering and Technology, 4(2).

[14] Emre Gurbuz., (2015), "Rotation Invariant Copy Move forgery Detection Method", International conference on Electrical and Electronics Engineering, pp.202-206.

[15] Toqeer Mahmood., (2015), "A Survey on Block based Copy Move Image Forgery Detection Techniques", International Conference on Emerging Technologies, pp.1-6.

[16] Rajeev Rajkumar., (2015), "Digital Image Forgery Detection Using SIFT Feature", IEEE International Sympsium advanced Computing & Communication, pp. 186-191.