International Journal of Research in Advent Technology, Vol.6, No.6, June 2018
E-ISSN: 2321-9637
Available online at www.ijrat.org

Key Point Based Approaches for Copy-Move Image Tamper Detection-A Review

Dr.V.Thirunavukkarasu[1], Dr.J.SatheeshKumar[2]
School of Computer Science and Applications[1], REVA University, Bengaluru[1]
Department of Computer Applications[2], Bharathiar University, Tamil Nadu[2]
Email: arasu_mca3@yahoo.com[1]

Abstract: Block and key point based approaches are the two processing alternatives in blind copy-move image forensic detection. Tamper detection methods and algorithms discussed in the literature are primarily focused on image blocks. Both block and key point based methods exhibit the best performance to reveal the tampered region. Successes of these methods are limited owing to computational complexity and detection accuracy against various image distortions and post-processing operations such as flipping, blurring, noise, JPEG compression, scaling and rotation. This article introduces typical workflow of key point based tamper detection methods and its implementation issues. This article also evaluate the performance and robustness of SIFT (Scale Invariant Feature Transform) and SURF (Speed Up Robust Feature) descriptor based algorithms and their limitations in tamper detection.

Index Terms: Forensic detection, flipping, blurring, SIFT, SURF

1. INTRODUCTION

Copy-move is most frequently used image tampering method in which certain segment of an image is copied and pasted in different segment of the same image to conceal or reproduce certain part of an image[1]. In block based copy-move tamper detection the suspected input image is divided in to fixed size overlapping block of size b X b. Feature vectors are extracted from each block and matched its nearest neighbor to detect the tampered region. Unlike exhaustive search and auto correlation method the block based method does not require pixel by pixel comparison rather it make use of block by block comparison technique [2]. Even though block based methods are used to discover very small tampered regions and tamper regions with some image distortion, these methods are not appropriate to discover the tampered region which is rotated or scaled, comparing one block with all other blocks leads computational complexity. Finding an optimum block size is a challenging task in block based methods owing to the size of tampered region. Size of the image block should not exceed the size of the tampered region. To overcome the above shortcomings, key point based approaches have been given importance [3].

Organization of this paper includes section II which introduces key point based image tamper detection techniques, Section III presents a typical work flow of key point based image tamper detection, the SIFT based tamper detection algorithms are discussed in section IV. SURF based tamper detection algorithms are introduced in section V. Issues in key point based methods are discussed in section VI and section VII concludes the paper.

2. KEY POINT BASED IMAGE TAMPER DETECTION TECHNIQUES

Classification of various non-intrusive image tamper detection techniques are exposed in figure 1. A key point in an image is a point with well defined position and high entropy [4]. It can retain similar characteristics of an image region and detectable even after some image transformations or distortions. Good key-points are capable for discovering discrete locations in an image region and robust in detecting geometric transformations, illumination changes, noise and other image distortions [5][6] . Primary advantages of key-point based techniques include high detection rates in duplicated regions. However, it will produce false matches in uniform or flat image regions.

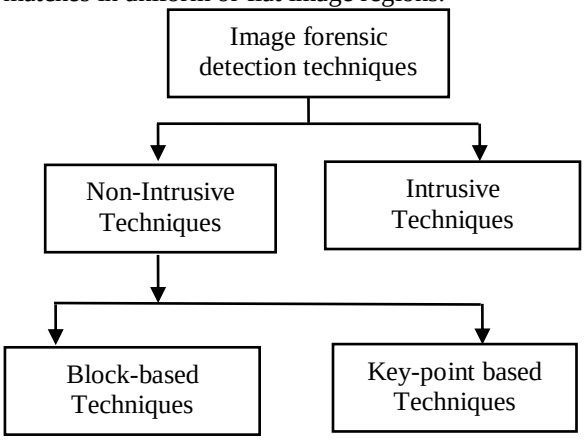


Fig 1: Classification tamper detection techniques

2.1 Characteristics of key point based algorithms

The robust and efficient key point based algorithms should include the following characteristics:

• *Repeatability*- Detection algorithm must discover the similar feature of the same scene repeatedly under different viewing condition.

•*Robustness*- The algorithm should detect the same feature locations irrespective of rotation, scaling, shifting, photometric deformations, compression artifacts and noise.

• *Accuracy*- Feature detection algorithm should accurately locate the tampered region.

• *Generality*- Detection algorithm should be able to detect features that can be used in different applications.

• *Quantity*- Feature detection algorithm must detect all or most of the features in the image

3. TYPICAL WORKFLOW OF KEY POINT BASED COPY-MOVE IMAGE TAMPER DETECTION

Unlike block based methods, key point based methods merely rely on image regions with high entropy without any image sub division. Typical workflow of key point based image tamper detection is shown in figure 2.

3.1 Preprocessing

The suspected image is converted into gray scale image to improve the tamper detection performance, some methods use all three color channels for feature extraction.

3.2 Key point detection

The key points are detected in the image region with high entropy. Feature vector f_i is computed from the key points.

3.3 Matching

The similar feature vectors are matched to indicate the duplicate region. The KD-tree, Random Sample Consensus (RANSAC) algorithm and Best Bin First (BBF) method is used to match the feature descriptors.

3.4 Filtering

The neighboring regions in an image have similar feature vectors which will increase the probability of false matches. Different threshold values, distance measures and correlation coefficients were used for filtering.

3.5 Locating tampered region

The locating process is employed to identify the exact location in which tampering is made and highlighting the tampered region [7] [8].

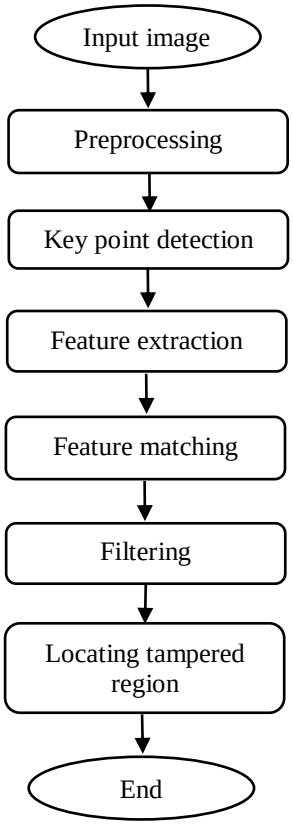


Fig 2: Flow of key point based image tamper detection

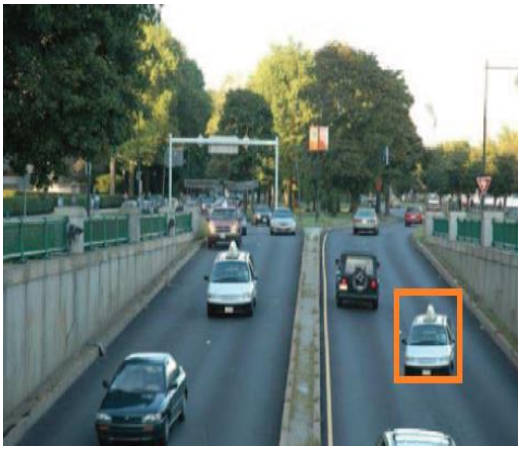
4. SIFT Based Tamper Detection Algorithms

The Scale Invariant Features Transform (SIFT) algorithm is largely used in image tamper detection because of its high accuracy and low computational cost. The key points K= $\{k_1, k_2, k_3 \ldots k_n\}$ and their SIFT descriptor D= $\{d_1, d_2, d_3 \ldots d_n\}$ are extracted by applying Laplacian of Gaussian (LoG) method. It approximate LoG by computing the difference between two nearby scales in the scale-space. The best matched key points are found by identifying the nearest neighbour from the remaining key points. To perform feature matching the key points with minimum Euclidean distance is chosen. Features extracted by SIFT algorithm is invariant to different geometric transformations like scaling, rotation and translation.

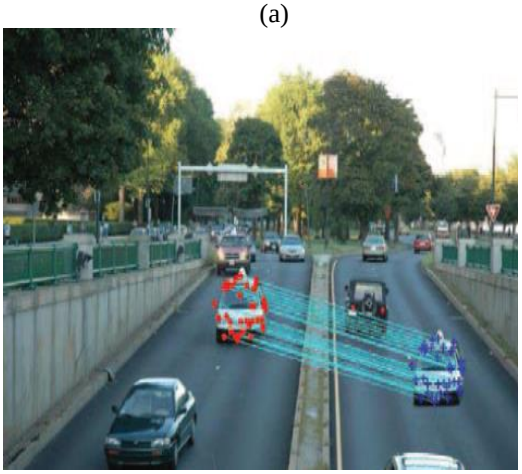
4.1 Geometric transformation estimation method with SIFT features

The block based region duplication detection algorithms are not appropriate when the tamperd region is translated, sclled or rotated. SIFT key

points and features are extracted from the suspected input image and extracted features are matched to discover forged region by estimating the geometric transformation among different image region. This method effectively detect copy-move tampered region with different post processing operations such as rotation and scaling. Performance of this method is efficient when the tampered region is rotated up to 90^0 and scaled up to 50%. Detection result of this method is shown in figure 3 [9].



(a)



(b)

Fig 3: (a) Tampered image (b) Detection result using SIFT

4.2 SIFT based region duplication detection method

The geometric transformation estimation method fails to detect the tampered region with JPEG compresssion and additive noise. The SIFT based region duplication detection method employs SIFT, Best Bin First(BBF) algorithm to detect and match the image features. Correlation map is used to locate the duplicate regions. Detection accuracy and false positive rate of the algorithm demonstrate that the method is efficient when the tampered region is distressed with translation, scaling and rotation. Robustness of this algorithm is tested against additive noise with various Signal to Noise Ratio(SNR) and different JPEG compression quality factors. Experimental results reveals the effectiveness of this method. Accuracy of this method is reduced when the signal to noise ratio (SNR) is above 40db and JPEG compression quality factor is below 60%. This method is inefficient when the tampered regionis distorted by illumination or linear transform [10].

4.3 Image feature matching technique based on key points

The SIFT based region duplication detection method is not appropriate when the tampered region is illuminated or linear transformed. Key point based image feature matching method is used to overcome this drawback. First the method convert the suspected image into grayscale using standard color space conversion method then key points are extracted using SIFT algorithm. At each key point, a 128-feature dimensional vector is generated and detected feature points are matched with the Best Bin First search (BBF) algorithm. Affine transformation is used between the matched key points to estimate the geometric transformation in the duplicated region. The Random Sample Consensus (RANSAC) algorithm is applied to reduce false matches and region correlation map is employed to locate the tampered region. This method is efficient while handling copy-move tampering with rotation, scaling, free-form linear transform and illumination distortion. However, the method fails to detect tampering when the image region contains fewer key points and images that inherently contain identical regions [11].

4.4 Automatic image similarity assessment method

In automatic image similarity assessment method, the feature points and descriptors are extracted from the input image using SIFT algorithm. Learning dictionary basis method is used to interpret the SIFT features. To find similarity between two image regions based on dictionary features, the sparse coding is performed and reconstruction error for each SIFT descriptor is calculated. This method is applied in image copy-move tamper detection, image retrieval and recognition [12].

4.5 Local invariant feature method

This method locate the tampered region by matching its feature points, first the key points are detected and feature vectors are extracted using SIFT method, then KD-tree and Best-Bin-First (BBF) methods are used to match the feature points. This method is effective even when the tampered regions are distorted by scaling, rotation,

JPEG compression and blurring. Computational complexity of this method is similar to block based approaches but locating accuracy of forged region is more. This method fails to detect the tampered regions in smooth areas .

5. Methods based on SURF features

Discovering the point similarity among two images of the same scene or object is a primary task of various computer vision applications such as image retrieval, object recognition and image registration. Key points are detected at different image locations specifically at corners, blobs and T-junctions. The major role of any key point detector is detecting same interest points under different viewing conditions. Neighbourhood of each key point is characterized by a feature vector. This feature vector or descriptor has to be distinct and invariant against noise, translation, geometric distortion and some image deformations. Finally, the descriptors are matched among different images or within the same image by means of distance measures like city block, Euclidean and minkowski distance.

A wide variety of descriptors such as SIFT, FAST, PCA-SIFT, Gaussian derivatives, Harris corner points are proposed and compared in the literature. However, Speeded up Robust Feature (SURF) descriptor proposed by Bay et al. is fast, robust and invariant against scale, rotation and noise. SURF descriptors make use of Hessian matrix approximation and integral image concept in order to reduce computational complexity.

5.1 Integral images

It is an intermediate image representation that is used for high-speed computation of box type convolution filters. The integral image $I^M(x, y)$ at location (x, y) stand for sum of all pixels inside a rectangular region formed by the origin and the location (x, y) in the input image I. It is calculated using the formula,

$$I^M(x, y) = \sum_{i=0}^{i \le x} \sum_{j=0}^{j \le y} I(i, j)$$

For computing integral image three additions and four memory access are required to calculate sum of the intensities over the any rectangular area consequently the calculation time is independent of its size (refer figure 4).

5.2 Hessian matrix-based interest points

Hessian matrix is used to detect interest points owing to its accuracy and good performance. Given a point X=(x, y) in an image I, the Hessian matrix H(x, σ) in X at scale σ is defined as follows,

$$H(x, \sigma) = \begin{bmatrix} L_{xx}(x, \sigma) & L_{xy}(x, \sigma) \\ L_{yx}(x, \sigma) & L_{yy}(x, \sigma) \end{bmatrix}$$

Where, $L_{xx}(x, \sigma)$ is the convolution of the Gaussian second order derivative $\frac{d^2}{dx^2} g(\sigma)$ with the image I at point X, similarly for $L_{xy}(x, \sigma)$ and $L_{yy}(x, \sigma)$. The above derivatives are called as Laplacian of Gaussians. SURF key points are calculated using determinant value of Hessian matrix for each pixel in the image. Box filters are used to approximate Gaussian second order derivatives, the approximated Gaussian second order derivates are evaluated with very low computational cost through integral image concept

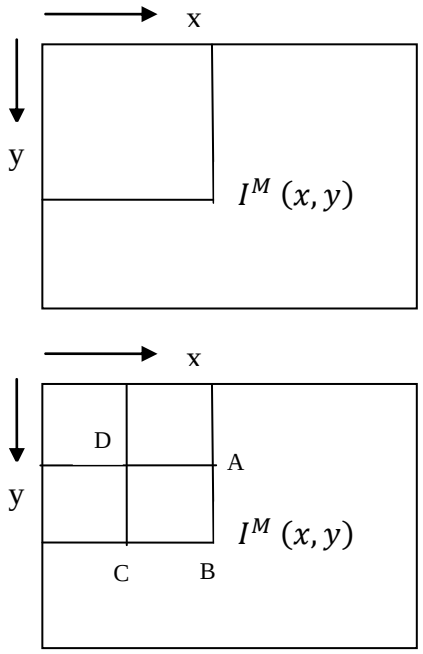


Fig 4: Integral image representation

Bo et al. introduced Speed up Robust Features (SURF) to detect copy-move region which is rotated, scaled or blurred. In the first step, the key points are detected by means of integral image and Hessian matrix then a circular region around each key point is created to assign unique orientation and gain invariance against image rotation. Key point matching is done by calculating Euclidean distance between every pair of interest points. This method is inappropriate to detect boundary of tampered region [13].

Zhang et al. employed SURF algorithm to detect copy-move tampered region. SURF key points are extracted and square region is estimated around each key points. Morphological operations are used to fill small holes in the square region. Image blocking method is introduced in flat region and Fourier Mellin Transform (FMT) features are

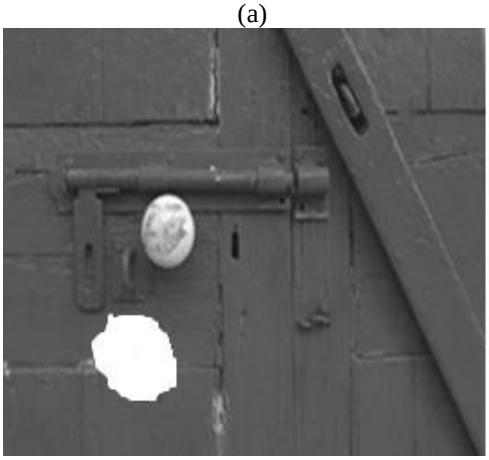
extracted from each block and finally, radix sort is used to match the similar regions. This method is efficient to detect the tampered region in flat and non-flat image regions but inappropriate to detect tampered region with various image distortions. Result of this method is shown in figure 5 [14].

6. Issues in key point based methods

Even though Key-point based methods are able to detect tampered region which is scaled, rotated and deformed by different image distortions, the following issues needs to be resolved.

- High False Positive Rate (FPR) of detection results is most important issue and need to be resolved
- Key-point based methods are unable to distinguish tampered area in the in the flat region.
- Feature dimensions and time taken to detect the key points are the primary issues in this method.
- Key point based methods unable to handle mirror reflection transformation.
- It is not appropriate for the images with fewer key points.

(a)



(b)

Fig 5: Detection result of SURF method (a) Tampered image (b) Detection result

7. CONCLUSION

In order to overcome the above drawbacks, a robust hybrid approach needs to be developed. Many key point based techniques have been proposed without rely on pre-embedded code or signature. However, success of these techniques is based on accuracy, false positive rate and time. This article introduced typical workflow of key point based tamper detection techniques and different key point based tamper detection methods. It also focuses SIFT and SURF based tamper detection methods and their robustness against various post processing operations such as rotation, scaling, noise, JPEG compression, flipping , blurring and illumination distortion.

REFERENCES

[1] Donghui Hu, Xiaotian Zhang, Yuqi Fan, Zhong-Qiu Zhao, Lina Wang, Xintao Wu, Xindong Wu, "On digital image trustworthiness", Applied Soft Computing, Vol.4(8), pp:240–253, 2016.

[2] Thirunavukkarsu V, Satheesh Kumar J, "A novel method to detect copy-move tampering in digital images", IND-JST, 9(8), pp:1–4, 2016.

[3] V.Thirunavukkarasu, J.Satheeshkumar, "Passive Image Tamper Detection Based on Fast Retina Key point Descriptor", IEEE-ICACA, pp.279-285, 2016.

[4] L. Wang, X. Jiang, S. Lian, D. Hu, D. Ye, "Image authentication based on perceptual hash using Gabor filters", Journal of Soft Computing, Vol.15 (3), pp: 493–504, 2011.

[5] Babak Mahdian, Stanislav Saic, "A bibliography on blind methods for identifying image forgery", Signal Processing: Image Communication, Vol.25(6), pp:389–399, 2010.

[6] V. Thirunavukkarasu, J Satheesh Kumar, Gyoo Soo Chae, J. Kishorkumar,| "Non-intrusive Forensic Detection Method Using DSWT with Reduced Feature Set for Copy-Move ImageTampering", Wireless Personal Communications, Springer, pp:1-19.

[7] Thirunavukkarasu V, Satheesh Kumar J, "Evolution of blind methods for image tamper detection-A review", International Journal of Applied Engineering Research, Vol.9 (21), pp: 5069–76, 2014.

[8] V.Thirunavukkarasu, J.Satheeshkumar, "Passive Image Tamper Detection Technique Based on Moment Invariants", IJCTA, Vol.9 (10), pp: 4705-4714, 2016.

[9] Irene Amerini, Mauro barni, Roberto caldelli, Andrea costanzo, "counter-forensic of SIFT-based copy-move detection by means of key

point classification", EURASIP Journal on Image and video processing, Vol.18(1), pp:1-17, Springer, 2013.

[10] Pan, Xunyu, and Siwei Lyu, "Detecting image region duplication using SIFT features" , Acoustics Speech and Signal Processing (ICASSP), IEEE International Conference, 2010.

[11] Xunyu Pan, Siwei Lyu, "Region duplication detection using image feature matching", IEEE Transactions on information forensic and security, VOL. 5, NO. 4, December 2010

[12] Irene Amerini, Lamberto Ballan, Roberto Caldelli, Alberto Del Bimbo, Giuseppe Serra, "A SIFT-based forensic method for copy-move attack detection and transformation recovery", IEEE Transactions on information forensic and security, 2011.

[13] X. Bo, W. Junwen, L. Guangjie, D. Yuewei, "Image Copy-Move Forgery Detection Based on SURF", Multimedia Information Networking and Security(MINES), pp: 889–892, 2010.

[14]Guang-qun Zhang, Hang-jun Wang, "SURF-based Detection of Copy-Move Forgery in Flat Region", International Journal of Advancements in Computing Technology (IJACT), Vol.4(17), pp:159-171, 2012.