Imperial Journal of Interdisciplinary Research (IJIR)
Vol-3, Issue-10, 2017
ISSN: 2454-1362, http://www.onlinejournal.in

Comparative Analysis of Feature Extraction Techniques in Keypoint based Image Forgery Detection

Pooja Patil , Namita Pulgam & Vanita Mane
Computer Engineering Department Ramrao Adik Institute of Technology, Mumbai, India

Abstract*—The role played by Digital image is important as far as information carrying is concerned which has also increased in last few decades. Increasing Image authentication demand need .Upcoming editing software Technology has emerged adding to this industry new techniques. Copy-Move forgery is most frequent among all the types of Image forgery. The same is achieved by copying the image from one location pasting the same at the target location in same image. Determining the originality authenticity of digital images irrespective of its history background . The same can be achieved in video as well. In this paper using key point based method different technique to detect Image forgery are presented.*

Keywords*: digital image; Image authentication; Image forgery; Keypoint based method*

1. Introduction

Authenticity of an image taken digitally suffers severe threats as a result of increase in various powerful digital image editing tools. The integrity of the images is checked for various forgeries by Digital Image forensics. Creation of a false written documents or alteration of original one with the intention to defraud can be called as Forgery. The main reason why images are forged so easily are due to low budget tools , software hardware which are easily available and easy to use as well for any alteration manipulation which are not easily traceable to human eyes. It is is difficult to identify if a given digital image is original or a forged one. Use of this kind of forgery is widely used in fields like Journalism ,media, publications, Investigations where the data is manipulated accordingly.

Active approach and Passive approach are basic two different ways for Digital image forgery. Active methods depend on watermarking and digital signature to authenticate where we have some background information available regarding the image which is one of the major drawback while working with these kind of images where the source are unknown and cannot be relied on.

The second way or technique which is passive technique where we don't have prior information or background available with respect to the concerned image. So it is called as blind images or passive image which are further divided in three sub categories which are as[1] Copy-move forgery, Image Splicing, Image Retouching

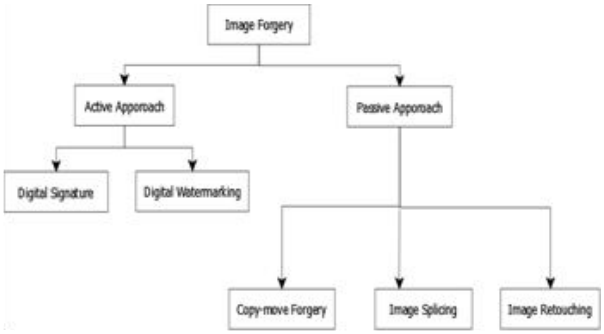


Figure 1. Image forgery techniques[2]

1. Copy-move forgery:

Copy-move forgery type is done by copying one part of image in same image hiding its necessary information. It very difficult to detect if the image provided is forged or original. This type can be further subdivided two groups as Keypoint and Block based method.

2. Image splicing:

In image splicing by combining two different images we can create a target image which is known as image splicing method. It is crucial to combine perfect object shape for forgery.

3. Image retouching:

Image retouching is third type of image forensic. Weather change, color change, make the background blurred etc are the main things in this type of Image forensic. Geometric transformation is yet another type in which image retouching can undergo scaling, rotation, stretching, etc. to create a new forged image.

In this research we work and study key point based image forgery detection methods. Processing pipeline of Copy- move forgery detection consists of Feature Extraction, Matching further followed by Filtering and Post-Processing as follows:

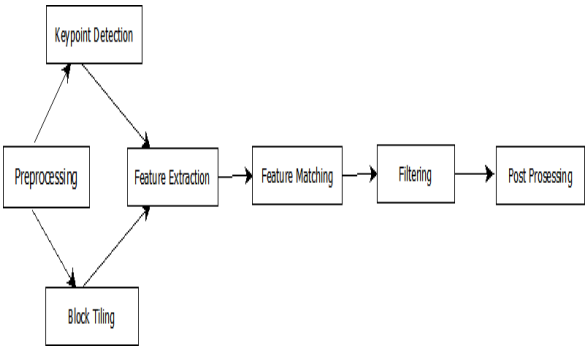


Figure 2.Processing pipeline of Copy-move forgery detection[3]

A. Pre-processing:
To enhance the important features for further detection preprocessing is vital. The grey-scale format of image wherever applicable. If necessary preprocessing can be applied at initial stages in both block-based and key-point based methods.
B. Feature Extraction:
Extraction of feature vectors for each block is carried out for block based algorithms whereas in key-point based methods the region with high entropy where feature vectors can be computed .
C. Feature Matching:
By searching similar featured blocks copy-move pairs can be identified after feature extraction. Regions can be interpreted as duplicate having high similarity between features. In block-based method sort similar features and in key-point based methods calculated approximate nearest neighbor which helps in the feature matching.
D. Filtering:
It is bit difficult on the basis of a single similarity criterion to predict presence and absence of forgery. To reduce probability of false prediction Filtering methods are used. To preserve matches that shows a similar behavior final post-processing can be applied.
E. Post-Processing:
Once the Image is identified as tempered, post processing find out type of transformation used. Various algorithms have been proposed in literature for the same such as RANSAC(Random Sample Consensus), Same Affine Transformation Selection(SATS

2. Related Work

Keypoint based methods detects the interest points that are use to produce set of features. various related work is done to this forgery detection as follows.
Fridrich [4] proposed Discrete cosine transform (DCT) of the image blocks to avoid the complexity using lex- ico- graphical sorting. In paper [5] the author introduced Scale Invariant Feature Transform (SIFT) algorithm to calculates the SIFT key points and then compares similar key points for detection of forgery. In Paper[6] the author proposed a method based on SIFT, combining BFSN clustering and CFA(color filter array) features to avoid obstruction in key points. In paper[7] adaptive over-segmentation and feature extraction is done in copy-move forgery detection. In Pa- per[8] to make copy-move forgery detection very fast author uses SIFT and SURF for finding keypoints. In Paper[9] Speeded-Up Robust Feature (SURF) in combination with Discrete Wavelet Transform (DWT), and Dyadic Wavelet Transform (DyWT) is proposed to reduce computational complexity. In Paper[10] author propose MIFT, which has properties of SIFT features and it is invariant to mirror reflection transformations which is an improved way for finding additional keypoint matches.

3. Key Point Based Techniques

In Copy-Move forgery technique the image can be tempered by using small part of same image. It is difficult task to detect manually, as various components like noise
,color, and some other properties will match the original image as its been extracted or copied from the base image. A clever forger achieve more finished image by rotating, scaling etc and before the region pasted may be some post processing on the copied region if required. So it is difficult to extract features in such a forgery detection techniques.

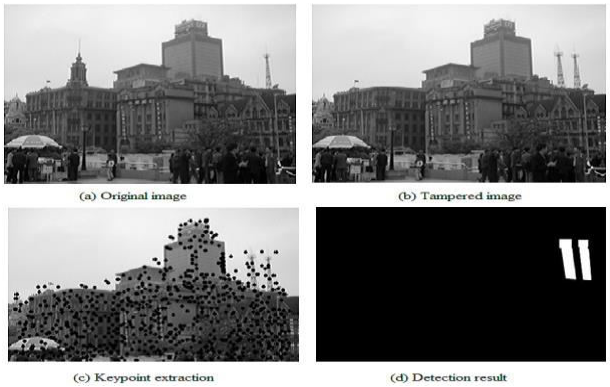


Figure 3. Keypoint based copy-move image forgery detection[11]

A. SIFT (Scale Invariant Feature Transform)[6]
SIFT is a digital image descriptor. Image-based matching, translations, rotations, scaling transformations and illumina- tion variation are invariant to SIFT and also robust making it easy in

practice. SIFT algorithm has four main steps: (a) Scaled-space Extrema Detection, (b) Localization of Key Point,(c) Orientation Assignment and (d) Generation of Descriptors.

(a) Scaled-space Extrema Detection

Building Scale Space model can be considered as an initial preparation for finding interesting points. Here original image is considered as creating blurred out images to create a scale space. This way several octaves of original images are obtained. The size of each octaves image is half the previous one. In each octave, using Gaussian Blur operator images are blurred. Gaussian blur is applied to each pixel of each octave. It has mathematical expression given as

$L(x; y; \sigma) = G(x; y; \sigma) * I(x; y)$

Where, L is a blurred image, G is Gaussian Blur operator,

I is an image, x, y are location coordinates, is the scale parameter, The * is the convolution operation in x and y. Key points in SIFT framework is first stage in finding interest points. The Laplacian of Gaussian (LoG) can be used to find interesting points in an image. It makes use of second points. But it is expensive calculating second order derivative as it is sensitive to noise. Difference of Gaussian is used to calculate difference between two consecutive scales. As it is fast and efficient. Local minima/maxima of the DoG images across scales are considered as key points. In DoG images Each pixel is compared to its eight neighbors at the same scale and nine corresponding neighboring pixels. Candidate keypoint is selected on basis that if the pixel value is highest or lowest comparatively to all other pixels.

(b) Localization of Key Point

Key points are produced in earlier stage which are there throughout an edge or they lack in contrast. In either cases, features are not effective. Intensities are checked for low contrast features. If the intensity is less than a particular value of magnitude, it gets rejected. This is the reason behind localizing keypoints which are further refined by removing the low contrast key points.

(c) Orientation Assignment

Key point orientation is performed as it provides rotation invariance. Using pixel differences Gradient magnitude orientation can be precomputed. Where these Equations can be applied for calculating gradient magnitude orientation:

$$m(x,y) = \sqrt{(L(x+1,y) - L(x-1,y))^2 + (L(x,y+1), -L(x,y-1))^2}$$

$$\theta(x,y) = \tan^{-1} \frac{L(x,y+1) - L(x,y-1)}{L(x+1,y) - L(x-1,y)}$$

After the computation, formation of histogram takes place where 36 bins combine to form 360 degrees of orientation. This type of orientation histogram is computed for all pixels around the key point. In SIFT, the magnitude gradient of an image has to be blurred by an amount of 1.5

* σ and the window size has to be equal to an amount of

1.5 * σ

(d) Generation of Descriptors

Each key point is formulated using gradient magnitude along with orientation of earlier stage.

In order to get local image descriptor, a 4x4 sample region around a key point is considered. This 4x4 window is broken into four 4x4 window as shown in the right side

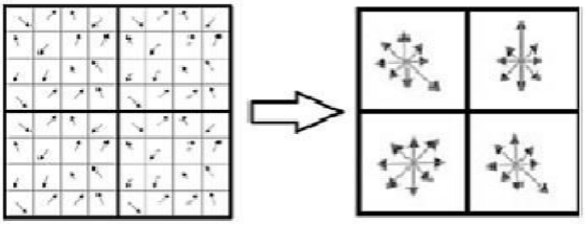


Figure 4. SIFT Descriptor Generation[12]

of the image. For each 4x4 window a histogram of 8 bins are generated. Gradient orientations from 44 are put into respective bins. This is done for all blocks. We get a total of 128 numbers (4x4x8) which are normalized forming feature vector. For identify a particular key point these feature vector can be uniquely used.

B. SURF(Speed up Robust Feature)[9]

SURF is a speeded-up version of SIFT. SURF approximates LoG with Box Filter. Laplacian of Gaussian method can be incorporated for distinguishing between background and foreground features of SURF. SURF uses only 64 dimensional vector instead of 128 dimensional vector for SIFT which are two major advantage of SURF over SIFT helping in quick matching compatibility fast feature computation . The algorithm is divided into three parts (a)Extracting Features,(b)Description of the Features, (c)Features Matching.

(a) Extracting Features

Hessian matrix is an approach for detecting of extracting features. Given a point x= (x,y) of an image I the Hessian matrix defined at scale σ is

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

Where, Lxx(x,σ), Lxy(x,σ) and Lyy(x,σ) shows the convolution of the Gaussian second order derivative image L in point x. Then integral images are calculate from the original image using,

x = (x; y) is a location in the integral image, than in the integral image IΣ(x)equals the sum of all pixels in the input image I of a rectangular region formed by that point x and the origin.

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

(b) Description of the Features

The primary step should be fixing up the reproducible orientation. Secondly extraction of a SURF descriptor by constructing a square region. Haar-wavelet responses in x-y direction are calculate in a circular neighborhood of radius 6s around the interest point, in order to make it invariant to rotation where s denotes the scale where detecting of the interest point takes place. The Haar-wavelet responses are denoted in vectors form. Thereafter sliding orientation window covering all responses within an angle of 60 degree are added up. Both responses in x and y direction of sliding window are added up generating all together a new vector.

$$v = \left(\sum dx, \sum dy, \sum |dx|, \sum |dy|\right)$$

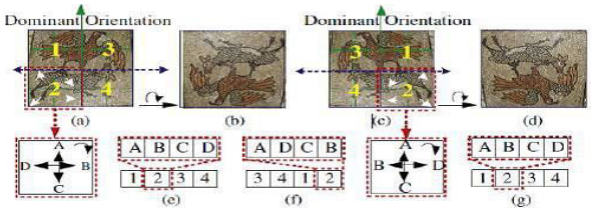
Sum of the absolute values of the responses |dx|; |dy| are extracted for achieving information about the polarity of intensity changes.

(c) Features Matching:

Integral image has been used for speeding up descriptor and detector steps which requires only four array references to calculate the sum of intensities of any rectangular area in the image.

C. MIFT(Mirror Reflection Invariant Feature)[10]

The SIFT algorithm extracts features invariant to scale, rotation, and brightness. But these are not invariant to mirror reflection. MIFT is local feature detector rest on SIFT, which is invariant to mirror reflection. Image with mirror reflection can be obtained by reverting the axis of image. Hence, in a horizontally reflected image the column order of pixel changes remains same row order,as in Fig 5.



A simplified SIFTdescriptor with 22 cells and 4 oriented bins in each cell is used for illustration. (a) The original image. (b) The combined reflection of (a). (c) The horizontal reflection of (a).(d) The vertical reflection of (a). (e) The original and MIFT descriptor for (a). (f) The descriptor of original version for (c). (g) The MIFT descriptor for (c).

Figure 5. Different mirror refelections and the concept of MIFT[13]

mirror reflection situations for the same feature, as shown in Fig.5 (e) and (f). In MIFT simple descriptor reorganization is used for achieving mirror invariance. And further it is used for organizing cell order arrangement. This is done by checking the values of total left pointing (ml) and right pointing (mr) orientations. Based on the winning orientation, column order may change (ml>mr) or not. Second, for each cell, it checks whether the order of orientation bins to follow clockwise or anticlockwise direction. Thus a descriptor which is similar to all mirror reflections is given by MIFT. Another similar process is restructuring orientation of bins order in each cell. After comparing mr/ml, correct order to encode properties in each cell can be selected. For instance, if mr> ml we encode them in clockwise order, or anticlockwise order otherwise for the similar keypoint, we obtain identical descriptors.

4. Comparative Analysis

SIFT,SURF,MIFT are different keypoint based methods For extracting feature points. Table. 4.1 shows the comparison of keypoint based forgery detection techniques using five parameters. 1) Keypoint based technique, 2) feature matching method, 3) pre-processing method,

4) Detection region and 5) Performance. Keypoint based technique used to extract features of image. feature matching method match features. Pre-processing gives idea about the process which is been used at the initial stage. Single or multiple regions are detected on basis of detection region. Finally performance gives the performance of keypoint based forgery methods.

Table1. Comparison of Keypoint based techniques for image forgery detection

Keypoint based tech-nique	Feature matching method	Pre-processing method	Detection region	Performance
SIFT[6]	BFSN clus-tering	No	Multiple	Effective detection of forgery for multiple tampered region
SIFT and MIFT[7]	Coefficient map and threshold	DWT and segmen-tation	Multiple	Give better result for different translations and when duplicate forged region is small
SIFT and SURF[8]	G2NN matching	No	single	SIFT and SURF gives quick and better per-formance in case of geometrical transfor-mation
SURF[9]	Use descrip-tor vector	DyWT and DWT	Single	Method detects copy move forgeries with high accuracy and Robustness against rotation and scaling
MIFT[10]	RANSAC and hysteresis thresholding	Apply geo- metric con-straints	single	High accuracy and ro-bustness in detection of forged region

A. Keypoint based image forgery detection in video:

In paper [14] author proposed passive forensic scheme for copy move forgery detection in spatial and temporal domain of video. For detecting copy move forgery in spatial domain SIFT can be used which gives appropriate results in comparison with other features. Detection of performance for forgery in spatial domain different scales and angles are taken into consideration. We get better performance in spatial domain under different transformations using SIFT features.

5. Future Work and Conclusion

future work will be concerned with applying SURF algorithm instead of SIFT for copy move forgery detection in video in spatial domain as SURF gives faster result than SIFT and having similar performance to SIFT. Various other forms are examined to overcome this issues but the major concern in these techniques is to detect the duplicated image regions without been disturbed by the general image processing operations. So by the help different keypoint based method we can find out if the given image is forged or original. So we conclude that SIFT method gives better result in this type which is invariant to translation, scale and rotation but comparatively SURF gives faster result than SIFT and have similar performance to SIFT also MIFT is use in case of mirror reflections and have similar result as SIFT in absence mirror reflection.

References

[1] Maryam Jaberi, George Bebis, Muhammad Hussain, Ghulam Muham- mad.”Accurate and robust localization of duplicated regionin copy- move image forgery.” Springer-Verlag Berlin Heidelberg,2013.

[2] Devanshi Chauhan, Dipali Kasatb, Sanjeev Jain, Vilas Thakare.”Survey On Keypoint Based Copy-move Forgery Detection Methods On Image.” International Conference on Computational Modeling and Security(CMS 2016).

[3] Kshipra Ashok Tatkare.”Fusion of SIFT and Hue Moments Features for Cloning Tamper Detection.” International Conference on Ap- plied and Theoretical Computing and Communication Technology (iCATccT),IEEE,2015.

[4] J. Fridrich, D. Soukalm and J. Lukas.”Detection of Copy-Move Forgery in Digital Images.” Digital Forensic Research Workshop, Cleveland, (2003), pp. 1923.

[5] Huang, H., Guo W., Zhang Y.”Detection of copy-move forgery in digital images using SIFT algorithm.” Computational Intelligence and Industrial Application, 2008. PACIIA’08.

[6] Lu Liu, Rongrong Ni, Yao Zhao, Siran Li.”Improved SIFT-Based Copy-Move Detection Using BFSN Clustering and CFA Features.” Tenth International Conference on Intelligent Information Hiding and Multimedia Signal Processing, IEEE, 2014.

[7] Dhania V. S., Harish Binu K. P.”Exposing Digital Image Forgeries Using Feature Extraction and Adaptive Over Segmentation.” Inter- national Journal of Innovative Research in Science, Engineering and Technology, Vol. 5, Issue 8, August 2016.

[8] Ramesh Chand Pandey,Sanjay Kumar Singh, K. K. Shukla and Rishabh Agrawal.”Fast and Robust Passive Copy-Move Forgery De- tection Using SURF and SIFT Image Features.” 5th International Con- ference on Computer and Communication Technology,IEEE, 2014.

[9] Mohammad Farukh Hashmia , Vijay Anandb , Avinas G. Keskarc.”Copy-move Image Forgery Detection Using an Efficient and Robust Method Combining Un-decimated Wavelet Transform and Scale Invariant Feature Transform.” AASRI Conference on Circuit and Signal Processing (CSP 2014).

[10] Maryam Jaberi, George Bebis, Muhammad Hussain, Ghulam Muham- mad.”Accurate and robust localization of duplicated regionin copy- move image forgery.” Springer-Verlag Berlin Heidelberg,2013.

[11] Guang-qun Zhang, Hang-jun Wang.”SURF-based Detection of Copy- Move Forgery in Flat Region.”International Journal of Advancements in Computing Technology(IJACT), Volume4, Number17,September 2012.

[12] Neetu Yadav and Rupal Kapdi.”Copy Move Forgery Detection Using SIFT Features- An Analysis.”Nirma University journal of engineering and Technology, VOL. 4, NO. 1, JAN-JUN 2015.

[13] Xiaojie Guo, Xiaochun Cao.”MIFT: A framework for feature descrip- tors to be mirror reflection invariant.”Image and Vision Computing 30 (2012) 546556.

[14] Ramesh Chand Pandey, Sanjay Kumar Singh and K.K.Shukla.”Passive Copy- Move Forgery Detection in Videos.”5th International Conference on Computer and Communication Technology, IEEE 2014.