IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol.-7, Issue-12, Dec 2019 E-ISSN: 2347-2693

# Latest Trends in Image Forgery Detection

**Kavita Rathi**

Dept. of Computer science and Engineering, DCRUST, Murthal, Sonipat, Haryana, India

*Author: kavita1217@gmail.com, Tel.: +00-8930220999*

DOI: https://doi.org/10.26438/ijcse/v7i12.4145 | Available online at: www.ijcseonline.org

Accepted: 16/Nov/2019, Published: 31/Dec/2019

***Abstract***— Digital image forensic is a part of multimedia security with the objective to expose the image forgery in digital images. Among different types of image forgeries available, copy–move forgery is the most popular and common forgery. In Copy-move forgery one part of the original digital image is copied and pasted at any other position in the same image. Several methods have been developed to detect the image forgery in digital images. This paper is focusing on pixel-based copy–move image forgery detection methods to detect forgery which later on includes the trending algorithms of Key point based techniques and Block based techniques. Various techniques have been mentioned in the paper from the literature which was used by different authors for feature extraction and forgery detection. Comparative study of key point and block based image forgery detection algorithms is also stated.

***Keywords:*** Image Forgery, Block based, Key point based

## I. INTRODUCTION

People switched from Analog camera to Digital cameras as it facilitates digital storage and do not require films. With advancement of technology, the ways to manipulate photographs to amuse the person in the picture is increasing. It helps in beautification of photograph or combines different photos of people like friends and relatives to revive people's memories. It may help in turning black and white photographs into colour photos. With time this technology is being misused by mischievous people to harass people by creating dirty picture or to create the wrong impression. Now days, a number of sophisticated software's are available for manipulating images to give them genuineness.

Alarming situation arose when these software's were misused by anti-social elements like criminals to change the pictures and misguide authorities. This may turn the situations in their favour by changing the images using software's like mat lab, adobe Photoshop, Microsoft power point and many others available in the market.

So, the need to detect image forgery arises. This paper focused mainly on key point and block based copy- move image forgery detection, as it is the most common forgery technique being used. In Copy-move technique one part of an image is copied and is pasted on some other part of the same image either to hide something or to add some extra information.[1][2][3][8].

The organization of the paper is as follows: **Section I** contains the introduction part of the paper which states the motivation for the paper and requirement for forgery detection. **Section II** contains the related work of image forgery detection to create a base knowledge for the readers so that they can understand the need of work carried out in the paper. **Section III** contains the methodology used by the author to present latest trends in Image Forgery, techniques used in key point and block based image forgery, their comparisons etc. **Section IV** contains Conclusion part which concludes the literature review carried out by the author on copy move image forgery, key point based techniques and block based techniques, their comparisons and why key point is better than block based technique.

## II. RELATED WORK

**Various ways to forge image: [1][6][7]**

Forgery used for better purpose created no problem, but when it was misused, the problem arises. So, for solving this problem methods to detect forgery are required.

 

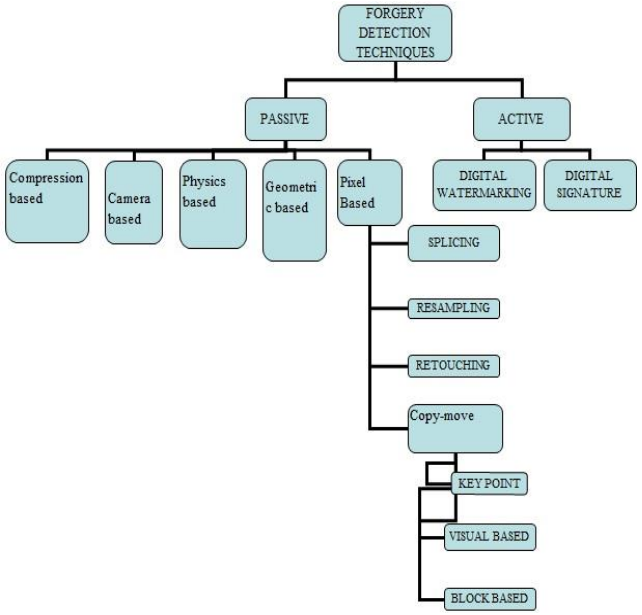


Fig.1

**Applications of Image Forgery Detection [10]**

i) Used in criminal and private investigation
ii) Used to check the genuinely of the images posted on various social sites
iii) To detect manipulated medical reports
iv) By journalist to check whether the images with them are tempered or not

**Image Forgery Detection Techniques: [2][3][4][5][6]**

Broadly they are classified in two categories:
Active and Passive [8][9]

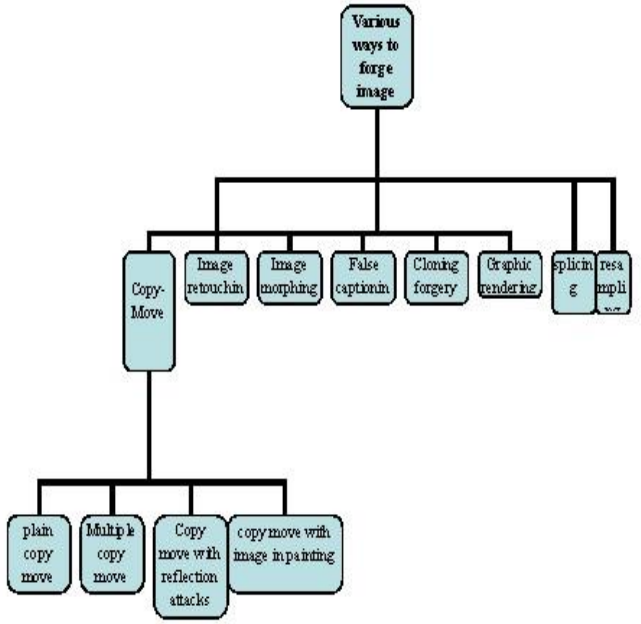


Fig. 2

Active Forgery Detection Method is not popular as the details like camera model, embedded digital signature are not always available with the concerned person. With the increase in virtual presence of society, content and pictures are posted on various social sites. So, it becomes indispensable to emphasize more on Passive Forgery Detection Techniques .This paper will pay attention to Passive Forgery detection method.

**Passive Method:**

This method is called passive because there is no involvement of the original image. Means, no prior information of the image like source of image, digital signature or watermark or any embedded digest is available to the forgery detector.

**There are a number of techniques used in passive methods**

a) **Pixel Based Technique**
Pixel being the fundamental unit of an image, it helps in forgery detection. In this technique statistical anomalies are checked at pixel level.

**b) Compression based technique**
Compression based technique is also known as Format Based Detection Technique. It is further divided into JPEG Quantization, JPEG Blocking.

**c) Camera based technique**
The forgery can be detected using its acquisition process which involves optics, camera components and image pipelining. The difference in chromatic aberration, color filter array, camera response, sensor noise is noticed.

**d) Physics based technique**
It relies on the concepts of Physics. The discrepancies in light sources between specific objects in the scene are used to reveal the traces of tinkering.

e) **Geometric based techniques**
Geometry-based techniques make measurement of objects in the world and their position relative to the camera.

**Further in pixel based technique we have various forgery detection techniques like,**

a) Copy-move: In this technique it highlights the areas of the image which are copied from the same image.
b) Splicing: In this technique the forged areas are highlighted if they are copied from some other image and are pasted on the image in question.
c) Resampling: Correlation between pixels is estimated as the bogus image so formed is manipulated either by rotation, resizing or by stretching, etc. which changes their pixel correlation.
d) Retouching: Small changes made to enrich the quality of the picture to make it more likable. Detecting these changes comes under this category.

 

## III. METHODOLOGY

**Approaches to Passive Copy-move (image cloning) detection:**

Copy-move forgery detection technique has two main algorithms:

a) Block based algorithm
b) Key point based algorithm

**Following are the steps followed in block based algorithm:**

Step 1 convert colour image into gray-scale image
Step 2 divide the gray-scale image into overlapping blocks of size 8 x 8
Step 3 feature extraction
Step 4 use clustering algorithm
Step 4 apply sort for feature matching

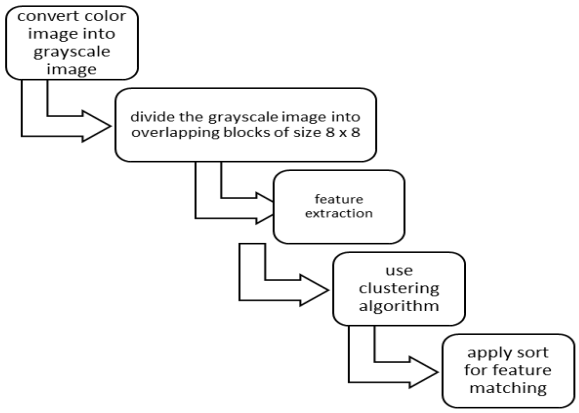


Fig. 3

**Following are the steps followed in Key point based algorithm:**

Step 1: Convert image into grey scale image.
Step 2: Instead of dividing the image into blocks compute the features only on image regions with high entropy.
Step 3: Match Similar feature vectors within the image.
Step 4: detection of large cluster formation.
Step 5: post processing is done such as filtering, edge detection etc.

**Latest Trends:**

i. Image Forgery Detection using BIRCH clustering based on Normalized mean and standard deviation.
ii. Detection using Homomorphic Image processing
iii. Region duplication detection based on hybrid feature and evaluation clustering
iv. Detection based on compact colour content descriptor and Delaunay triangle matching
v. Forgery detection using Segmentation and Swarm Intelligent Algorithm

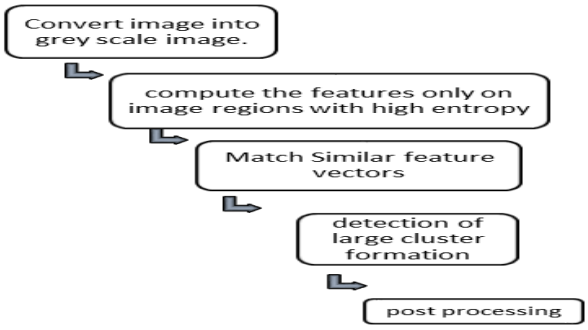


Fig. 4

**Different Key Point Based Algorithms:**

1. SIFT (Scale invariant Feature Transform) a robust and distinctive descriptor. It is an algorithm to detect and describe local features in an image.it is efficient in object recognition but it failed in real time applications.
2. SURF (Speeded up Robust Features) It consists of three steps namely, feature extraction, feature description and feature matching. It uses wavelet responses
3. ORB (Oriented FAST and Rotated BRIEF) it is combination of FAST and BRIEF descriptors. It is an alternative to SIFT as it more efficient.
4. Related BRIEF (Binary Robust Independent Elementary Features)
5. Wavelet Transform (as Discrete Wavelet Transform and Dyadic Wavelet Transform) and SURF
6. KAZE two dimensional feature detector. It helps in reducing noise and at the same time helps in maintaining boundaries. It uses nonlinear scale space.
7. Harris corner points: It is used for finding corner points by matching the difference in intensities for displacement in all directions.
8. BRISK (Binary Robust Invariant Scalable Key points). It relies on circular sampling pattern to compute brightness comparisons to construct a binary descriptor string. In plane rotation makes it unsuitable.
9. MIFT (Modified Iterative Fourier Transform)
10. JLinkage It is used in matching and generating multiple local homographic hypotheses.
11. SIFER (Scale Invariant Feature Detector with Error Resilience) It uses Cosine Modulated Gaussian filter
12. FAST (Features from accelerated segment test) It tells us about the presence of a corner by testing a circular area.

**Block Based Algorithms:**

1. DCT (Discrete Cosine Transform): It is used for converting the image into frequency domain.
2. DWT (Discrete Wavelet Transform): It allows both time and frequency analysis of images. It is used for images having discontinuous edges.
3. DSWT (Discrete stationary Wavelet transform) it is

 

used in combination with DCT to separate the colors.

4. PCA It is sensitive to noise. It is an efficient method and gives low false positives.
5. FMT: An efficient algorithm which can work with noise, compressions, scaling but is unable to work properly if image is highly rotated.
6. Zernike Moments: They represent images without repetition or commonality of information between the moments. It is also used for feature extraction.
7. CCV (Color Coherence Vector) it is used for fast multi resolution image querying with increased speed of the image retrieval.
8. LBP (Local Binary Pattern): It describes each pixel by relative grey scale levels of its neighbor's pixels. It has faster computational power and is invariant to monotonic illumination variations.
9. SVD (Singular Value Decomposition)
10. DCT Phase
11. FMT (Fourier Melin Transform)
12. Kernel Principal Component Analysis
13. Blur Moment Invariant: It is robust against blur/noise and compressions.
14. MDS (Multidimensional Scaling) It extracts a rotation invariant DFT feature matrix with log polar transform and is impervious to angle rotations.
15. LFD (Local Fractal Dimension)
16. DFT (Direction Filter Technique): It works for both compressed and uncompressed images.

**Key Based techniques**

| Paper | Technique | Advantages |
|---|---|---|
| Mohammad Hashmi and Avinash Keskar,Fast and Robust Copy-Move Forgery Detection Using Wavelet Transforms and SURF(2019) | Wavelet Transforms and SURF | ● It focuses on Blind detection of copy move forgery<br>● These techniques are applied on the whole image rather than dividing it into blocks<br>● It reduces the false positives<br>● Detection time reduces by the use of SURF.<br>● Performance using this technique was better than block based techniques but was a bit lower than other key point based techniques.<br>● Improved computational power as compared to both other block as well as key point techniques.<br>● More robust algorithm as the precision and recall of the detector remain reasonably unchanged even after exposing the image to various attacks.<br>● Computationally inexpensive |
| | CMFD-PSO | ● |
| Mohamed Abdel Basset,Gunasekaran Manogaran, Ahmed E. Fakhry, Ibrahim El-Henawy, 2-Levels of clustering strategy to detect and locate copy-move forgery in digital images (June,2018) | SIFT+2 level clustering | Efficient in dealing with multiple cloning. |
| | KAZE | KAZE is better than BRISK and Harris corner and SURF |
| Zhao Fei, Shi Wenchang†, Qin Bo,Liang Bin,Image Forgery Detection Using Segmentation and Swarm Intelligent Algorithm (2017) | SIFT+SI | Effective to identify image with a small or smooth cloned region |

**Block Based techniques**

| Paper | technique | Advantages |
|---|---|---|
| Malti Puri,Dr. Vinay Chopra ,A Review: Block-Based Copy-Move Forgery Detection Methods(Oct 2016) | DCT | Can detect the forged part even after retouching and enhancement. |
| | PCA | ● Can work in the presence of noise<br>● Low false positive |
| | LBP | Robust against blurring, noise, flipping |
| | SVD | Lower computational complexity |
| | Blur Moment Invariant | ● Capable of detecting lossy JPEG format images<br>● Can detect blurring |
| Amanjot Kaur Lamba, Neeru Jindal,Sanjay Sharma,Digital image copy-move forgery detection based on discrete fractional wavelet Transform(Jan 2017) | DWT | ● Takes less time and is robust<br>● Can detect single and multiple duplicated regions<br>● Can detect tampering areas even in the presence of distortions due to Gaussian blurring and JPEG compression.<br>● Exact copy move |

 

| | | |
|---|---|---|
| | | region detected |
| Malti Puri,Dr. Vinay Chopra ,A Review: Block-Based Copy-Move Forgery Detection Methods(Oct 2016) | Zernike Moments | Robust against JPEG compression and blurring |
| | CCV | Capable of detecting Gaussian blurred images |
| | DCT Phase | ● Can determine threshold value automatically<br>● Gives lower false negatives |
| | Double Quantisation DCT | Forged region detected precisely |
| Er.Isha1, Er.Vikas Goyal2A literature review of Image Forgery Detection | HU | Capable of detecting noise,blur and lossy compression |
| Er.Isha1, Er.Vikas Goyal2A literature review of Image Forgery Detection | CURVELET | Gives precise result |
| Er.Isha1, Er.Vikas Goyal2A literature review of Image Forgery Detection | Circular block with DCT | Accurate results provided for uniform background image and high resolution image |
| Er.Isha1, Er.Vikas Goyal2A literature review of Image Forgery Detection | Polar Harmonic Transform | Can deal with affine transformation |

## IV. CONCLUSION

**Comparison of Key Point Method and Block Based Method**

| **Key Point** | **Block Based** |
|---|---|
| Have high computational efficiency, robustness against geometric transformations like scaling, rotation, illumination, etc. | Efficiency decreases with the increase in size, as block size increases resulting in increase in complexity. |
| Not able to detect forgery in flat copied/uniform texture regions. | Can detect forgery even with the smooth background |
| Gives high false rate | Comparatively less |
| Usually cannot deal with few key-points | Divided into blocks |
| Requires less memory | |
| Less computational cost | |
| Lower accuracy because of poor local image feature computation | |

:

## REFERENCES


[1] A. Kashyap, R. S. Parmar, M. Agarwal, and H. Gupta, "An evaluation of digital image forgery detection approaches," *Int. J. Appl. Eng. Res.*, vol. 12, no. 15, pp. 4747–4758, 2017.

[2] M. Ismail and N. Kanwal, "a Review Block Based Copy Move Forgery Detection Techniques," *Int. J. Comput. Sci. Mob. Comput.*, vol. 7, no. 4, pp. 205–212, 2018.

[3] X. Cun and C. M. Pun, "Image splicing localization via semi-global network and fully connected conditional random fields," *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 11130 LNCS, pp. 252–266, 2019.

[4] V. Christlein, C. Riess, J. Jordan, C. Riess, and E. Angelopoulou, "An evaluation of popular copy-move forgery detection approaches," *IEEE Trans. Inf. Forensics Secur.*, vol. 7, no. 6, pp. 1841–1854, 2012.

[5] M. hak and T. Gulati, "Detection of Digital Forgery Image using Different Techniques," *Int. J. Eng. Trends Technol.*, vol. 46, no. 8, pp. 457–461, 2017.

[6] S. Mushtaq and A. H. Mir, "Image Copy Move Forgery Detection: A Review," *Int. J. Futur. Gener. Commun. Netw.*, vol. 11, no. 2, pp. 11–22, 2018.

[7] S. Walia and K. Kumar, "Digital image forgery detection: a systematic scrutiny," *Aust. J. Forensic Sci.*, vol. 51, no. 5, pp. 488–526, 2019.

[8] S. Sadeghi, S. Dadkhah, H. A. Jalab, G. Mazzola, and D. Uliyan, "State of the art in passive digital image forgery detection: copy-move image forgery," *Pattern Anal. Appl.*, vol. 21, no. 2, pp. 291–306, 2018.

[9] E. Isha and E. V. Goyal, "A literature review of Image Forgery Detection," *Int. J. Res. Appl. Sci. Eng. Technol.*, vol. 4, no. IX, pp. 75–80, 2016.

[10] T. Dalal, "Survey of Image Forgery Detection Technique Based on Color Illumination Using Machine Learning Approach," *Int. J. Adv. Res. Ideas Innov. Technol.*, vol. 2, no. 3, pp. 1–7, 2016.

[11] Z. Zhang, C. Wang, and X. Zhou, "A survey on passive image copy-move forgery detection," *J. Inf. Process. Syst.*, vol. 14, no. 1, pp. 6–31, 2018.

[12] S. Panda and M. Mishra, "Passive techniques of digital image forgery detection: Developments and challenges," *Lect. Notes Electr. Eng.*, vol. 443, pp. 281–290, 2018.

[13] A. Sahay and A. Gautam, "Comparison between SIFT and SURF image forgery Algorithms," *Int. J. Comput. Appl.*, vol. 164, no. 2, pp. 9–11, 2017.


 