DOI: https://doi.org/10.53555/nncse.v2i6.445 **Publication URL: http://nnpub.org/index.php/CSE/article/view/445**

COMPARATIVE STUDY AND SURVEY ON COPY MOVE IMAGE FORGERY DETECTION APPROACHES

Naincy[1]*, Ashok Kumar Bathla[2]
*[1]*Research scholar, CE Deptt. YCOE, Punjabi University, Patiala, India*
[2]*Assistant Professor, CE Deptt. YCOE, Punjabi University, Patiala, India*
*[1]*Email: naincyaneja2k9@gmail.com*, [2]ashokashok81@gmail.com

Corresponding Author: -
Email ID - naincyaneja2k9@gmail.com

Abstract: -

Nowadays the demand of digital images in various application areas is increasing and thus it is becoming important to ensure the authenticity of images. Due to easy availability of various image editing tools, continuous manipulations are done to create fake or forged images. Although various techniques like copy-move, splicing, resampling etc. for image forgery are present but copy move image forgery has received significant attention these days. Thus the focus of this paper is on copy-move image forgery detection techniques. We have presented a review of commonly used copy move image forgery detection techniques and the comparison of same is also showed to evaluate their performance on basis of various parameters.

Keywords: - *Image forgery, Image forgery detection, Copy-move, Splicing, Resampling, Block based, Key-point based*

1. INTRODUCTION

It is easy to access and share information in this era of digital revolution. Now there are various tools available by which we can manipulate digital images and makes it difficult to differentiate between an authentic picture and its manipulated version. Thus, to verify integrity and authenticity of images in various application areas like in document authentication, forensic investigation, criminal investigation, fingerprint recognition etc. their arisetheneed of images forgery detection techniques. Digital image forensics is the field that deals with forgery and provides various detection techniques. Although various techniques hadmadefor forgery detectionbut the work is still in a flourishing state. Image tampering (image forgery) is defined as any type of manipulation in image by adding, removing or changing some elements of image without leaving any obvious traces. The tampering is basically done either to hide some important features or to create misleading images. Image forgeryor tampering can be classified into three categories,namely copy-move, splicing and resampling.

1.1 Copy-move

Copy-move image forgery is the most commonly used manipulationsin which, part of image is copied and pasted to different location in same image. It is also possible to do some post processing operations like scaling, rotation, translation, compression etc. onthecopied part before pasting it to some other location. This forgery is mainly done for two purposes,either to create duplicate regions or to hide some region. As the copied region came from same image,thus no change occur in its properties like noise, texture , color etc. and hence makes the detection process difficult for humans [1].(Refer Figure 1.1)

(a) (b)

(a) Original image (with two cats) (b) Forged image (with four cats)

Figure1.1:- An example of copy-move forgery.

1.2 Splicing

Splicing is also a commonly used forgery, but instead of using a single image as in copy-move image forgery, the fake images are created by using more than one image. As the higher order Fourier statistics does not remains same after forgery, thus it providesa great help in detection of forgery done using splicing [1]. Fig 1.2 shows image forgery using splicing in which first two images are original images are fused to make forged image

Figure1.2:-An example of image forgery using splicing.

1.3 Resampling

It is the type of forgery that involves geometric transformations like rotation, scaling, stretching, skewing, flipping etc. on selected portions of images, which are fused to make fake image. But it introduces specific periodic correlations into an image that help in its detection [1]. (Refer Figure 1.3)

(a) Original image (b) Forged image

Figure1.3:- An example of image forgery using resampling.

2.COPY-MOVE IMAGE FORGERY DETECTION METHODS

Generally, copy move image forgery detection methods are classified into two categories that are block based methods and key-point based methods

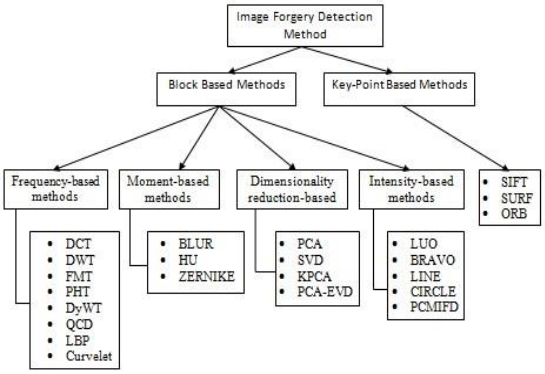

Figure 2.1: -Classification of image forgery detection methods.

2.1 Block based methods

Block based methods come into existence due to various drawbacks of exhaustive search method like its high computational time. Block based method work by dividing the image into small overlapping or non- overlapping blocks by sliding a window of particular size over the image. Then the features for each block are calculated which help in matching similar blocks. Thus, it leads to detection of forged region. Block based methods are robust against various intermediate or post processing operations like compression, blurring, noise addition etc. But they are not able to detect forgery in regions having operations like scaling or rotations done over them. Block based forgery detection techniques can be classify into four categories.

- Frequency-based methods (DCT, DWT, FMT, PHT, DyWT, QCD, LBP, and Curvelet)
- Moment-based methods (BLUR, HU, and ZERNIKE)
- Dimensionality reduction-based methods (PCA, SVD, KPCA, and PCA-EVD)
- Intensity-based methods (LUO, BRAVO, LIN, CIRCLE and PCMIFD) [12].

2.2 Key-point based methods

Key-point based forgery detection methods are proved great beneficial in dealing with the shortcomings of block-based methods. These methods are proven robust against scaling and rotations attack. The key-point based methods start work by scanning the image. Then key-points are extracted from whole image and feature vectors are computed for these key-points. These feature vectors are placed in feature matrix where they are sorted lexicographically. Thus, the similar feature vectors come closer and are suspected to be forged. Thus, by following some threshold criteria forged region are detected. Major drawback that remains there is inability of key-point based methods in dealing with flat duplicate region detection [12]. Examples of commonly known key-point methods used for copy move image forgery detection are SIFT, SURF and ORB.

3. RELATED WORK

Fridrich et al. [6] proposed the use of 256 discrete cosine transform coefficients (DCT) as features. They used block matching and developed two types of algorithms. The first algorithm is based on exact match and started by dividing the image into various blocks. Then a window of fixed size is used to perform sliding over blocks. Then pixel value for each block is calculated and put into an array. Then with the help of lexicographic sorting of these arrays forged regions are detected. Second algorithm is based on robust match. Instead of matching the pixel representation of blocks, as done in exact match, it calculates the DCT transform for each block. Thus, DCT coefficients are quantized and stored in matrix. Rest of the procedure of robust match is same as for exact match. To avoid false match, it uses shift vector count. Zhang et al. [16] proposed an efficient and robust algorithm for copy-move forgery detection using DWT (Discrete Wavelet Transform) and pixel-matching. At first DWT transform was applied on whole image to reduce the dimensions of image at each level. Thus, the image in its compressed form was divided into fixed size overlapping blocks. These blocks were then lexicographically sorted and duplicated blocks are identified using Phase correlation as a similarity checking criterion. This algorithm worked well even in the presence of noise and JPEG compression.

Popescu et al. [9] proposed an efficient technique for automatic detection of duplicated region. This technique worked by applying block-based detection method principal component analysis (PCA) on blocks. The main advantage of using this technique was to reduce the dimension of feature vector of each block. The method was found robust against noise and lossy compression.

Bayram et al. [3] proposed a technique that used Fourier Mellin Transform (FMT) for extracting features. They proposed the use of counting blooming filters instead of lexicographic sorting. The technique proposed was found more robust against various attacks like lossy compression, scaling and rotation. The technique was also compared with previous technique which uses DCT method of forgery detection and found better robustness in various cases. Bashar et al. [2] proposed methods by using Discrete Wavelet Transform (DWT) and Kernel Principal Component Analysis (KPCA) which is the improved version of linear PCA for copy-move forgery detection. They worked by dividing the image into blocks. Then the feature vectors for blocks are computed. The vectors are then sorted lexicographically. These sorted vectors are used to find similar points. The concept of threshold value was used to improve accuracy by removing false matches. They

also designed a new algorithm to deal with Translation-flipping and Translation-rotation duplications. This technique was found robust against additive noise and lossy JPEG compression also.

Ryu et al. [11] proposed a block based method for copy move image forgery detection based on Zernike moments. The method gave better results in comparison to previous block based methods in case of robustness against rotation. The method was found robust against various operations like Gaussian noise, JPEG compression and blurring done on cloned area.

Huang et al. [7] introduced a key-point method using SIFT (Scale Invariant Feature Transform) for detection of copy move image forgeries in tempered images. The technique worked by extracting SIFT descriptors for key-points of an image. These descriptors were then matched with each other. This method has increased the computational complexity in the case of high dimensional vectors. Thus the BBF (Best-BinFirst) derived from a k-d tree algorithm was developed to decrease the computations for matching. The results obtained from experiment shows the technique is robust against additive noise and lossy JPEG compression, rotation, noise, scaling compound image processing.

Due to the relatively slow speed of SIFT, a new technique named Speeded Up Robust Feature (SURF) which is basically the improved version of SIFT. Bo et al. [4] proposed an algorithm for copy move image forgery detection using SURF. It also worked by extracting interest point from image and matching descriptor vectors of interest points to find forged regions. The experimental results have shown its efficiency in dealing with various post processing like scaling, rotation, noise and blurring etc. But it was not able in automatic detecting tampered region and its boundaries.

Zheng et al. [17] proposed a method to detect region duplication forgery based on binary descriptors and was known as ORB (Oriented FAST and rotated BRIEF). The method proposed was an alternative to SIFT or SURF and it reduced the matching time and storage space required. To deal with problem of scaling and false matching, a new method called scaled ORB was proposed by Zhu et al. [18]. The method first established a Gaussian space and then extracted oriented FAST key-points and ORB features from each scale space. These features are then matched with each other using hamming distance to detect copied regions. It then used RANSAC to remove false matches.

4. COMPARATIVE ANALYSIS

This section has shown differences that exist between various copy-move image forgery detection techniques. The comparison is made on basis of various characteristics like according to their robustness against various attacks done on images.

Table 4.1 represented the comparison of various copymove image forgery detection algorithms.

Detection technique	Robustness against scaling	Robustness against rotation	Robustness against noise	Robustness against compression	Robustness against blur	Feature length	Advantage
DCT[1,6]	Don't work	Don't work	Robust	Robust	Robust	256	Gives exact location of forged region.
PCA [1,9]	Don't work	Don't work	work well	work well	Don't work	Depends upon image size	Detect forged region automatically
KPCA [2,14]	Don't work	Don't work	work well	work well	Don't work	192	Detect forged region automatically
DWT [1,5,13]	Don't work well	Don't work well	Robust	Robust	Don't work	256	Gives exact location
FMT [3,15]	Robust	Can't handle rotation above 10 degrees	Robust	Robust	Robust	45	Able to detect forgery in flat regions
ZERNIKE [11,14]	Don't work	work well for small degree of rotation	Robust	Robust	Robust	12	Able to detect forgery in flat regions
ORB [8,17,18]	Don't work	Robust	Robust	Robust	Robust	256	Able to detect hidden forgery
Scaled ORB[18]	Robust	Robust	Robust	Robust	Robust	256	Able to detect hidden forgery
SIFT [1,8,10]	Robust	Robust	Don't work efficiently	Don't work efficiently	Don't work efficiently	128	Robust against illumination changes
SURF [5,10]	Robust	Robust	Robust	Don't work efficiently for high value	Don't work efficiently for high value	64	Robust against illumination changes

4. CONCLUSION

As many blocks based and key-point based methods for detection of copy move image forgery available. But as it is clear from comparison presented in the above table that none of them efficient in dealing with all types of attacks like compression, blurring, scaling, rotation etc. and each has its own advantages and drawbacks. Thus, to develop robust methods for copy move image forgery detection it is advisable to make hybrid techniques by combining different techniques on the basis of their advantages.

REFERENCES

[1].Ansari M. D., Ghrera S. P., Tyagi V., "Pixel-Based Image Forgery Detection: A Review", IETE Journal of Education, vol. 55, no. 1, pp.40-46, 2014.

[2].Bashar M. K., Noda K., Ohnishi N., Mori K., "Exploring duplicated regions in natural images", IEEE transactions on image processing: a publication of the IEEE Signal Processing Society, pp.1-40, no.99, 2010.

[3].Bayram S., Sencar H. T., Memon N., "An Efficient and Robust Method for Detecting Copy-Move Forgery", IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), Taipei, pp.1053-1056, 2009.

[4].Bo X., Junwen W., Guangjie L., Yuewei D., "Image copy move forgery detection based on SURF", IEEE International Conference on Multimedia Information Networking and Security (MINES), Jiangsu, pp.889892, 2010.

[5].Christleinl V., Riess C., Jordan J., Riess C.,Angelopoulou E., "An Evaluation of Popular CopyMove Forgery Detection Approaches", IEEE Transactions on Information Forensics and Security, vol.7, no.6, pp.1841-1854, 2012.

[6].Fridrich J., Soukal D., Lukas J., "Detection of copymove forgery in digital images", Proceedings of Digital Forensic Research Workshop, Citeseer, 2003.

[7].Huang H., Guo W., Zhang Y., "Detection of CopyMove Forgery in Digital Images Using SIFT Algorithm", IEEE Pacific-Asia Workshop on Computational Intelligence and Industrial Application, Wuhan, pp.272-276, 2008.

[8].Isik S., Ozkan K., "A Comparative Evaluation of Well-known Feature Detectors and Descriptors", International Journal of Applied Mathematics, Electronics and Computers (IJAMEC), pp.1-6, 2014.

[9].Popescu A.C., Faridy H., "Exposing digital forgeries by detecting duplicated image regions", Dartmouth College, Tech. Rep. TR2004-515, pp.1-11, 2004.

[10]. Qureshi M. A., Deriche M., "A Review on Copy Move Image Forgery Detection Techniques", IEEE 11th International Multi Conference on System, Signal and Devices, Barcelona, pp.1-5, 2014.

[11]. Ryu S. J, Lee M. J., Lee H. K., "Detection of CopyRotate-Move Forgery Using Zernike Moments", Springer-Verlag Berlin Heidelberg, pp. 51–65, 2010.

[12]. Sekhar R., Matha L., "Recent Block-based Methods of Copy-Move Forgery Detection in Digital Images", International Journal of Computer Applications, vol. 89, no. 8, pp.28-33, March 2014.

[13]. Sridevi M., Mala C., Sanyam S., "Comparative Study of Image Forgery and Copy-Move Techniques" Springer-Verlag Berlin Heidelberg, vol.166, pp. 715– 723, 2012.

[14]. Thajeel S. A., Sulong G., "A Survey of Copy-Move Forgery Detection Techniques", Journal of Theoretical and Applied Information Technology, vol.70, no.1, 2014.

[15]. Zhang G. Q., Hang-jun Wang H. J., "SURF-based Detection of Copy-Move Forgery in Flat Region", International Journal of Advancements in Computing Technology (IJACT), vol.4, no.17, 2012.

[16]. Zhang J., Feng Z., Su Y., "A new approach for detecting copy-move forgery in digital images", 11th IEEE Singapore International Conference on Communication Systems (ICCS), Guangzhou, pp.362366, 2008.

[17]. Zheng J., Chang L., "Detection of Region-duplication Forgery in Image Based on Key Points Binary Descriptors", Journal of Information & Computational Science, pp.3959-3966, 2014.

[18]. Zhu Y., Shen X., Chen H., "Copy-move forgery detection based on scaled ORB", Springer Science+Business Media New York, pp.51-65, 2015.