COPY MOVE FORGERY DETECTION BASED ON DENSITY BASED CLUSTERING.

B. Manikanth[1], I. Sridhar[2], A. Kishan Chandra[3], E.B.V.S.D. Siva Kumar[4], B.V.S. Naga Yashwanth[5]

[1] *Assistant Professor, ECE, Vasireddy Venkatadri Institute of Technology, Andhra Pradesh, India*
[2] *Student, ECE, Vasireddy Venkatadri Institute of Technology, Andhra Pradesh, India*
[3] *Student, ECE, Vasireddy Venkatadri Institute of Technology, Andhra Pradesh, India*
[4] *Student, ECE, Vasireddy Venkatadri Institute of Technology, Andhra Pradesh, India*
[5] *Student, ECE, Vasireddy Venkatadri Institute of Technology, Andhra Pradesh, India*

ABSTRACT

Copy-move is one of the most commonly used methods of tampering with digital images. It has become a significant research subject in digital forensics and security due to its widespread use and its hard detection. In this type of image forging, a region of the image is copied and pasted elsewhere in the same image. The performance of keypoint based methods is not very efficient when the duplicated regions are near to each other and while handling highly textured areas. The clustering algorithm that is mostly used in keypoint based methods suffer from high complexity. In this project, an improved approach for keypoint based copy-move forgery detection is proposed via SIFT method. The proposed method is based on density-based clustering (DBSCAN). The proposed method will be superior to existing state-of-arts methods in terms of time complexity, and forgery location accuracy.

Keyword: - *Density Based Clustering, Copy Move forgery, SIFT, CLAHE, Key point Mapping etc.….*

1. Introduction

In the last few years due to presence of low-cost and high-resolution digital cameras, there is large amount of digital images all over the world. Also with help of very easy to use Photo editing tools, any non-expert can modify image. Any image manipulation can become a forgery, if it changes semantic of original image. . There can be many reasons for a forgery to be occurred by a forger like: To cover objects in an image in order to either produce false proof, to make the image more pleasant for appearance, to hide something in image, to emphasize particular objects etc. There are many ways to categorize the digital image forgery, but main categories of Digital image Forgery are Enhancing, Retouching, Splicing, Morphing and Copy/Move . Following is brief description of different types of digital image forgery:

1.1 Copy-Move

In copy-move forgery one region is copied from an image and pasted onto another region of the same image. Therefore, source and the destination both are same . Copy Move involves copying regions of the original image and pasting into other areas.

1.2 Copy-Move Forgery

Copy-Move is a type of forgery in which a part of image is copied and then pasted on to another portion of the same image. The main intention of Copy-Move forgery is to hide some information from the original image. Since the copied area belongs to the same image, the properties of copied area like the color palette, noise components, dynamic range and the other properties too will be compatible with the rest of the image

Passive detection methods can utilize the advantages of the detective strategy to find the tampering regions. Hence, a large majority of image forgery detection methods adopt a passive-based strategy to perform the type of tampering identification discussed in the present study. Passive detection technology can be categorized into block based methods and keypoint-based methods

FIg1.1:Example for Copy Move Forgery

Fig 1.2:(a) Original image of Iranian Missile Test (b) Forged image of Iranian Missile Test Among the image manipulation technique

2. Related Work

As discussed earlier, there are two methods for detecting copymove forgery: block-based and keypoint-based. Block-based methods are also known as dense field methods because all the pixels go through the phase of feature extraction. Unfortunately, blockbased methods are known to result in high computational complexity because all features are searched exhaustively in the matching phase. In the literature, various enhancements techniques based on block-based approaches can be found Of all block based methods, DCT is one of the most vastly used methods in CMFD (Bakiah et al., 2016)[1].However, when applying high levels of post-processing operations, such as blurring and geomet ric transformations, DCT-based approaches fail to detect copy move forgery (Asghar et al., 2017; Christlein et al., 2012)[2]. Detection based on DCT was first proposed by (Fridrich et al., 2003)[3]. Detection method presented by (Cozzolino et al., 2015)[4] attempted to reduce the complexity of the matching phase by utilizing Patch Match algorithm.

On the other hand, keypoint-based methods try to address these issues for both computation complexity and robustness to post-processing operations. The most popular and reliable keypoint features technique in CMFD is Scale Invariant Feature Transform (SIFT) (Bakiah et al., 2016)[1]. The generalized 2-nearest neighbor (G2NN) procedure for SIFT descriptor matching was first introduced in (Amerini et al., 2011) to detect multiple copy-move forgeries. Their method is based on SIFT and Agglomerative Hierarchical Clustering (AHC). Later, they improved their work in (Amerini et al., 2013)[5] by intro ducing a method based on J-linkage algorithm for clustering.A CMFD based on Multi-Level Dense Descriptor (MLDD) and a hierarchical feature matching is presented in (Bi et al., 2016). (Wang et al., 2016)[6] introduced a detection method for small smooth regions based on superpixel segmentation and Speed up Robust Feature (SURF). Although this method recorded a good detection accuracy, it cannot be used in real-time applications due to its high computational complexity. In (Jin and Wan, 2017[7]), presented SIFT-based method using non maximum value suppression and optimized J-Linkage.

2.1 Block Based Detection

Firstly the image is preprocessed i.e. Converted to grayscale.Preprocessing is optional. Then the image is subdivided into overlapping blocks of pixels. For an image size of M × N and a block n size of bxb, the number of overlapped blocks is given by (M-b+1) x (N-b+1).

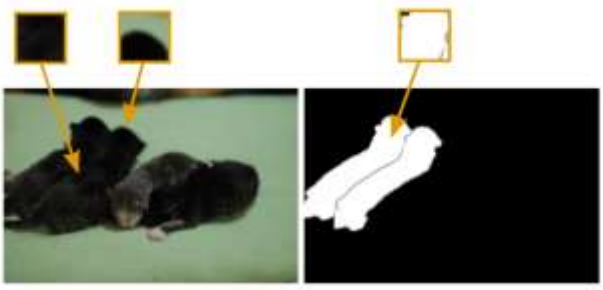


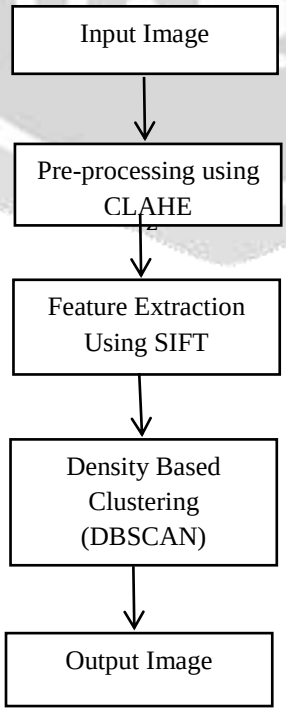
Fig -2.1 Block-based method

Following Steps are performed in block-based for Copy Move forgery detection:

A. ***Preprocessing*** Preprocessing is the very first step. Also it is optional. Some images required to be pre-processed and some not. Colored image can be converted into grey-scale image to reduce size of image. So, that processing become fast.
B. ***Feature Extraction*** In case of Block based method image is firstly divided into several over lapping blocks and this process is known as block tiling. For an image size of M × N and a block n size of bxb, the number of overlapped blocks is given by (M-b+1) x (Nb+1). After block tiling features are extracted from each block. Features like Local binary pattern, discrete cosine transform, discreet wavelet transform Principle Component Analysis etc. are used in block based method.
C. ***Matching Matching*** is done to detect the duplicated regions. High similarity between two feature descriptors is interpreted as a cue for a duplicated region. Methods used for matching can be lexicographic sorting, Best-Bin-First search etc.
D. ***Forgery*** detected After matching forged regions are detected. Forged regions are marked so that user can see the forged areas.

3. Proposed Method

In this project, a keypoint-based copy-move forgery detection method is proposed. It effectively reduces the false positive rate and improves time and space complexity. The contributions of the proposed method include by utilizing the (DBSCAN) clustering algorithm, the forged patch can be detected more accurately while reducing time and space complexity.



3.1 DBSCAN (DENSITY BASED CLUSTERING):

Clustering analysis is an unsupervised learning method that separates the data points into several specific bunches or groups. Centrally, all clustering methods use the same approach i.e. first we calculate similarities and then we use it to cluster the data points into groups or batches. Here we will focus on the Density-based spatial clustering of applications with noise (DBSCAN) clustering method.If you are unfamiliar with the clustering algorithms, I advise you to read the Introduction to Image Segmentation with K-Means clustering. You may also read the article on Hierarchical Clustering.

What's nice about DBSCAN is that you don't have to specify the number of clusters to use it. All you need is a function to calculate the distance between values and some guidance for what amount of distance is considered "close". DBSCAN also produces more reasonable results than k-means across a variety of different distributions. Below figure illustrates the fact:

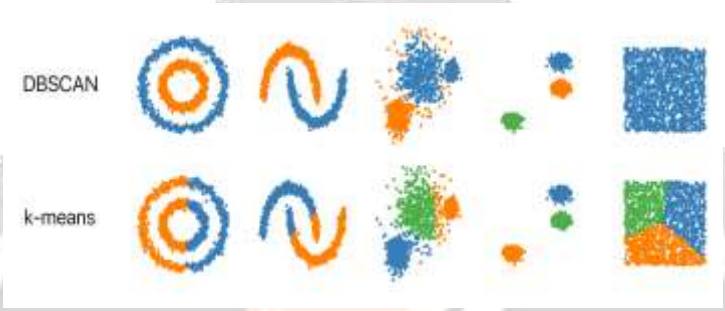


Fig -2 DBSCAN clustering comparison with k-means clustering

Density-Based Spatial Clustering of Applications with Noise (DBSCAN) is a base algorithm for density-based clustering. It can discover clusters of different shapes and sizes from a large amount of data, which is containing noise and outliers.

The DBSCAN algorithm uses two parameters:

- minPts: The minimum number of points (a threshold) clustered together for a region to be considered dense.
- eps (ε): A distance measure that will be used to locate the points in the neighborhood of any point.

4. EXPERIMENTAL RESULTS

We evaluate the proposed copy-move forgery detection method. The detection performance is measured in terms of the True Positive Rate (TPR) and False Positive Rate (FPR), which are defined as

$$\text{TPR}=\frac{\text{detected forged images}}{\text{forged images}}$$ (Correctly detected forged images)

$$\text{FPR}=\frac{\text{wrongly detected original images}}{\text{original images}}$$ (authentic images that detected incorrectly as forged images.)

4.1 RESULTS ON MICC-F220 DATASET

MICC-F220 dataset consists of 110 tempered images and 110 untempered images.Resolution of images range from 722 x 480 to 800 x 600 pixels, on average, the size of forged region covers 1.2% of whole image.

methods	MICC F220	
	TPR	FPR
Amerini2011[6]	98.18%	9.09%
Cozzolino2015[4]	84.55	17.27%
Li2015	70.91%	17.27%
Proposed	95.45%	11.81%

5.CONCLUSION

A SIFT features based copy move forgery method used for forgery detection. The main contribution of this work are introducing a density based clustering algorithm to increase the accuracy and time complexity.Various data set images are tested containing different scaling and rotation techniques .Experimental results exhibit that proposed method performs well in the existence of various attacks like rotation and scaling

6.REFERENCES

[1] Bakiah, Nor, Warif, Abd, Wahid, Ainuddin, Wahab, Abdul, Yamani, Mohd, Idris, Idna, Ramli, Roziana, Salleh, Rosli, Shamshirband, Shahaboddin, 2016. Copy-move forgery detection : survey, challenges and future directions. J. Netwk. Computer Appl. 75, 259–278. https://doi.org/10.1016/j.jnca.2016.09.008.

[2] Christlein, Vincent, Riess, Christian, Jordan, Johannes, Riess, Corinna, Angelopoulou, Elli, 2012. An evaluation of popular copy-move forgery detection approaches. IEEE Trans. Inf. Forensics Secur. 7 (6), 1841–1854. https://doi.org/10.1109/ TIFS.2012.2218597

[3] Fridrich, Jessica, Soukal, David, Lukáš, Jan, 2003. Detection of copy-move forgery in digital images. Digital Forensic Res. Workshop 3 (2), 652–663. https://doi.org/ 10.1109/PACIIA.2008.240.

[4] Cozzolino, Davide, Poggi, Giovanni, Verdoliva, Luisa, 2015. Efficient dense-field copy-move forgery detection. IEEE Trans. Inf. Forensics Secur. 10 (11), 2284– 2297. https://doi.org/10.1109/TIFS.2015.2455334.

[5] Amerini, I., Ballan, L., Caldelli, R., Del Bimbo, A., Serra, G., 2011. A SIFT-based forensic method for copy–move attack detection and transformation recovery. IEEE Trans. Inform. Forensic Secur. 6 (3), 1099–1110. https://doi.org/10.1109/ TIFS.2011.2129512.

[6] Wang, Xiang-yang, Li, Shuo, Liu, Yu-nan, Niu, Ying, Yang, Hong-Ying, Zhou, Zhi-li, 2016. A new keypoint-based copy-move forgery detection for small smooth regions. Multimedia Tools Appl. 76 (22), 23353–23382. https://doi.org/10.1007/ s11042-016-4140-5.

[7] in, Guonian, Wan, Xiaoxia, 2017. An improved method for SIFT-based copy-move forgery detection using non-maximum value suppression and optimized J linkage. Signal Process. Image Commun. 57, 113–125. https://doi.org/10.1016/j. image.2017.05.010.