Bachelor of Science in Computer Science and Engineering

Copy Move Forgery Detection Based on Scaled ORB and K-means++

Mohammad Asiuzzaman
ID: 1304006

December, 2018

Department of Computer Science &Engineering
Chittagong University of Engineering & Technology
Chittagong-4349, Bangladesh.

Copy Move Forgery Detection Based on Scaled ORB and K-means++

This thesis is submitted in partial fulfillment of the requirement for the degree of Bachelor of Science in Computer Science & Engineering.

Mohammad Asiuzzaman

1304006

Supervised by
Dr. Pranab Kumar Dhar
Professor
Department of Computer Science &Engineering (CSE)
Chittagong University of Engineering &Technology (CUET)

Department of Computer Science & Engineering

Chittagong University of Engineering & Technology

Chittagong-4349, Bangladesh.

December, 2018

The thesis titled **“Copy Move Forgery Detection Based on Scaled ORB and K-means++”** submitted by ID No. 1304006, Session 2016-2017 has been accepted as satisfactory in fulfillment of the requirement for the degree of Bachelor of Science in Computer Science & Engineering (CSE) as B.Sc. Engineering to be awarded by the Chittagong University of Engineering & Technology (CUET).

Board of Examiners

1.____ Chairman
(Supervisor)

Dr. Pranab Kumar Dhar
Professor
Department of Computer Science & Engineering (CSE)
Chittagong University of Engineering & Technology (CUET)

2.____ Member
Professor Dr. Mohammad Shamsul Arefin (Ex-officio)
Head of the Department
Department of Computer Science & Engineering (CSE)
Chittagong University of Engineering & Technology (CUET)

3.____ Member
Muhammad Kamal Hossen (External)
Associate Professor
Department of Computer Science & Engineering (CSE)
Chittagong University of Engineering & Technology (CUET)

Statement of Originality

It is hereby declared that the contents of this project are original and any part of it has not been submitted elsewhere for the award if any degree or diploma.

Signature of the Candidate

Date:

Acknowledgment

First and foremost, I would like to thank Allah for the good health and giving necessary energy to complete this work. I would also like to express my sincere gratitude to my honorable project Supervisor **Dr. Pranab Kumar Dhar**, **Professor**, Department of Computer Science and Engineering, Chittagong University of Engineering and Technology for providing me the perfect guidance, encouragement, instructive suggestions with all the necessary facilities for the research and preparation for the project. Also, I want to show my respect to **Dr. Mohammad Shamsul Arefin**, Head of the Department, Department of Computer Science and Engineering, Chittagong University of Engineering and Technology for the kind encouragement.I also grateful to my external, **Muhammad Kamal Hossen**, Department of Computer Science and Engineering, Chittagong University of Engineering and Technology, for his guidance and review of my project work. I take this opportunity to express gratitude to all of the Department faculty members and seniors for their help and support. I also thank my parents for their financial and mental support. Finally I would like to thank all of my friends who helped me directly or indirectly.

Abstract

Copy-move is a common practice of digital image tempering. Due to the availability of low cost software, the forging rate of image is increasing. That is why, image security authentication is playing a critical role in our society. So copy move forgery detection (CMFD) is enabled to detect the forged portion of an image. This detection is done by Scaled ORB and k-means++ algorithm. The pyramid scale space is identified first which is essential in the next step. Feature is an important property for detecting a region. So the ORB descriptor plays an important role in this method. From each scale space, extracting FAST key points and the ORB features. With respect to the original image, the coordinates of the orientated FAST key points are reverted. Now k-means++ algorithm is applied on ORB descriptors. The clustered features are matched every two different key points using hamming distance. Then the forged key points are detected. Based on those key points, two circles are drawn on the forged region and original region. If the forged region becomes rotational invariant, moment is needed to be calculated. In this method, geometric transformation (scaling and rotation) is feasible. This paper shows a method to detect the forged region efficiently for images which are modified by rotation and smoothing condition. The proposed method reduces the running time compared to the previous work.

Table of Contents

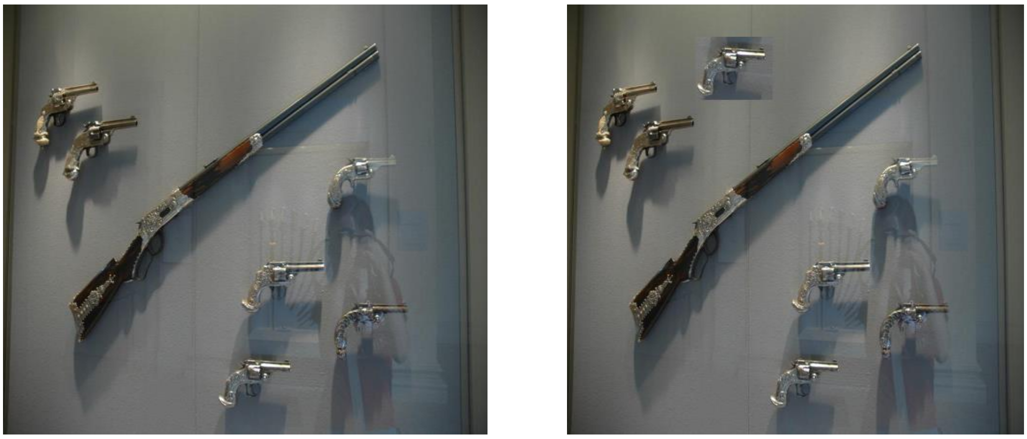
List of Figures

List of Tables

Chapter 1

Introduction

The world has become technologically advanced. So it is easy to forge images with the help of many low cost softwares. So authentication of an image is not ensured. Images can be forged in many ways. Copy move forgery is one of them. In this method an image is forged by copy and paste of one or multiple parts of the image. One can add an extra part to the image hiding its real part. So authentication of that image becomes vulnerable. Nobody can recognize those forged images by visual look. Sometimes criminals get passed freely with the help of forged images and victims do not get their justice. Moreover, judges can not identify the incident properly because of forged images. Many newspapers publish fake news. So many times normal people fail to identify whether the images are right or not. So it can be said that public security becomes at stake due to forged images. To restrict forgery, many methods have been proposed. With the help of those methods an forgery can be identified easily. Thus image authenticity increases and people get justice. With the advent of forgery detection, criminals think twice before committing a crime. Copying a part of an image and pasting it on the same image is termed as forged image. Detecting the forged region is a passive forgery detection. For detecting and localizing the image many method have been introduced. The methods are divided into two categories-Block-based methods[1] and key points-based methods[2]. In block-based methods, overleaping or non-overleaping blocks of equal size are required for extracting the features from each of the block. Then comparing those blocks, the forged region is easily detected. If specific block pair is matched, it is named as ‘copy-move’ because of having similar features. But in key-points based methods, key point detectors and features are used to identified the key points. And extracted those key points from a region are used to feature matchng. But dis-advantages of these key point is false matching. RANSAC[3] is an eliminating algorithm to remove the false matching. Key point based technique takes less execution time over block-based method. In key-points based method, for feature extraction and matching the region around the key points are to be considered. But the entire image blocks are considerd for matching in block-based technique.



(a) (b)

Figure 1.1: (a) Original image. (b) Forged image

1.1 Copy Move Forgery Detection

Image security authentication are playing a critical role in our society. If an image being forged then we never get real data. To get real data image never be forged. But many times these images are being duplicated. Copy move forgery is most used forgery method. The component of the region copied from the same image will be compatible with the whole image and hard to be detected by Human Visual System (HVS). In copy move forgery detection copied blocks are from same image so they sustain the same properties as the other blocks of the image and it makes the difficulty to detect forgery. So, several number of methods are being used to detect copy move forgery. The first one has been proposed by Fridrich. They divided an image into overlapping blocks of equal size. Coefficient of each block extracted by discrete cosine transformation (DCT). Digital image forensic has two principal approaches to detect forgery. First one is active approach which includes digital signatures. Second one is passive approach which includes two methods. First one is image source identification which only tells the image is computer generated or digital camera image. This method can not detect forged images. Second one is tempering detection and it can detect forged images.

1.2 Background and Present State of the Problem

Copy move image forgery technique is the widely used to edit the digital image. Copy move forgery involves the pasting of image blocks in the same image and hide important information or object from the image. For this approach the originality of the image is lost and puts at stake the authenticity of that digital image. In copy move forgery detection copied blocks are from same image so they sustain the same properties as the other blocks of the image and it makes the difficulty to detect forgery. Few years ago, copy move forgery detection was so much difficult. But with the help of technology and methods it is now very easy task to detect copy move forgery. There are many methods to detect copy move forgery detection. Detection of copy move image forgery algorithm using block matching approach and Principal Component Analysis (PCA). In order to detect images through post-processing operations quickly, efficiently and accurately. forged image detection based on radon and Fourier-Mellin transform is presented [5]. Another possibility for forgery detection is to classify textures that occur in natural images using statistical measures and find discrepancies in those statistics between different portions of the image [6]. At this point, however, it appears that such approaches will produce a large number of missed detections as well as false positives. Since the key characteristics of Copy-Move forgery is that, copied part and the pasted part belongs to the same image, one technique to detect forgery is exhaustive search, but it is computationally complex because, blocks are directly extracted from original image and thus resulting in a large number of blocks. Author proposed copy-move forgery detection method based on speeded up robust features (SURF), which detects duplication region with different size [7] There are many other methods which was proposed to detect copy move forgery. But we know that most of these methods accuracy are not too good. So many of us try to propose a better method to detect copy move forgery. I hope accuracy rate of detecting copy move forgery will be better than other methods.

1.3 Motivation of the Research

At present, in the world forged images is a regular topic. People forged images in order to get benefits. Generally forged images are used for illegal activities. Forged images are responsible for following activities:

- Increased number of crimes.
- Publication of fake news.
- Decreased security.

Those reasons motivated me to done this project. I hope this methods will help us to remove those bad activities from our society. So people will get real news. Criminals will being punished for crime. Victims will get justice.

1.4 Objectives

The objectives are here below:

- To implement copy move forgery detection.
- To identify forged images.
- To detect forged portions.

1.5 Contribution of the Work

The main objective of this work is to develop a copy move forgery system which can identify copy move forged by comparing the features of the images. According to my work this method will take an image. Dividing the images into multiple small blocks. Extract each block features and after that match each block features to identify forged images.

Our key objectives and possible outcomes of this work may mention in the following:

- To design a system that can detect copy move forged in images.
- To develop an approach to calculate copy move forged more accurately.
- To evaluate the performance of the proposed innovative technology in real environment.

1.6 Challenges

The algorithm processing of copy move forgery detection is quite complex. Matching the ORB descriptor one by one is much time consuming. That's why first needs to clustering the descriptor. So number of count in matching is reduced. To reduce time complexity the algorithm has become complex. On the other hand, to increase accuracy rate we have used the false matching algorithm called RANSAC. we had to face problems when we used low quality images. So if we would increase image quality by using another method then it would be much better, the difficulty of the project would be increased number of times. Copy move forgery detection method can detect only those forged images which is forged by the same image property. If an image is being forged by the property of other image through copy pasting, then this method will not able to detect that forged image

1.7 Organization of the Report

The remainder of the report is structured as follows. In the next chapter, an overview of our project related terminologies, the relation among copy move forgery detection algorithm and with their parameters and also contains brief discussion on previous works that is already implemented with their limitations. Chapter 3 describes the working procedure of our proposed system. In Chapter 4, we have illustrated our implementation of the project in details. Chapter 5 centers on the experimental result of the proposed system. In order to evaluate the system, we have used subjective as well as quantitative measures. The project concludes with a summary of research contributions and future plan of our work in Chapter 6. This thesis contains two appendices intended for persons who wish to explore certain topics in greater depth. Appendix A represents indexing. we tried every way to make this research to carry forward to the more advanced system as well.

Chapter 2

Literature Review

In this chapter, we have tried to represent the terminologies related to the project which are important to understand. This chapter also contains brief discussion on related previous works.

2.1 Copy Move Forgery Detection

Copy move forgery detection is a technological system that uses features of an image to identify forged region. This detection method depends on image features. If one can able to extract features from each block exactly then this method will work more accurately. So copy move forgery detection method works based on features extraction.

2.2 Classification of Copy Move Forgery Detection

There are two principal approaches in the digital image forensics which is shown in Figure 2.2.1. Watermarking and stenography are very popular which are known as active approach. These are executed at the time of image acquisition. For the digital image security, a special implementation of hardware is needed which includes the digital image encryption. A specific information in an image is hidden when the image is taken as input and the embedded information is extracted from the image and proved that it was original watermarks is called water marking. Hence, this method depends on the source information beforehand. Second approach is known as passive approach which relies on traces left on the image by different processing steps during image manipulation. Passive approach consists of two methods. Source identification of an image is the first one which identifies the device used for digital image acquisition. It proves that this kind of image is digital camera or computer generated image. So this method can’t identify the forgery image location. Second one is intentional manipulation of images is called tempering detection. Image tempering is done when the content of visual image is changed. Tempering detection can be divided into three. When an image is being small or large to its original size after tempering is known as image sampling. When a region of an image replicates twice or more on that image is called ‘copy-move’ or image cloning. And image retouching is very common in film making. When an image is being scored from its original image is called image retouching.

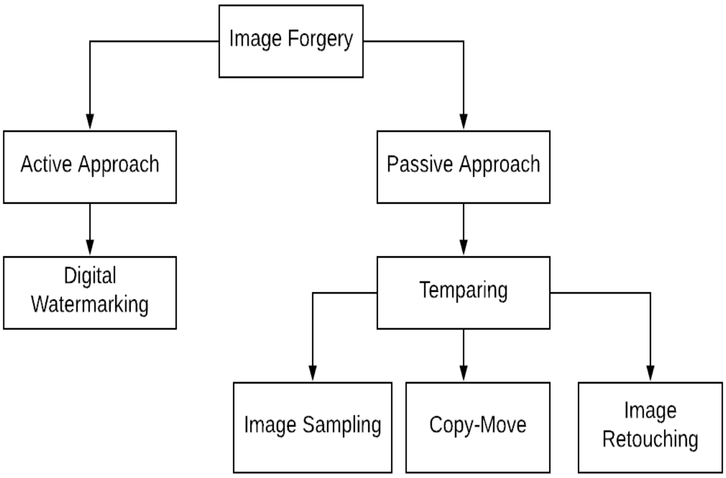


Figure 2.2.1: Classification of copy move Forgery Detection

2.3 Fundamental Properties of Copy Move Forgery Detection

- **Universality**: Every individual image accessing the application should possess the trait.
- **Complexity**: Reducing time complexity.
- **Uniqueness**: The given trait should be sufficiently different across others images.
- **Permanence**: This will work every time. When this method identify a forged image then it has capability to identify that forged image again and again. On the other hand, if an image be clear then it will not show forged portion if it has to check next time.
- **Measurability**: This method will identify exact forged portion rather than only identify the image is forged or not forged.
- **Performance**: The accuracy rate depends on features extraction. When features extraction done successfully then the accuracy rate increased. Hopefully my project accuracy rate is acceptable.
- **Acceptability**: This method works only when the copying portion is same image property. Otherwise it will not work.
- **Key Points**: The key points are very special because no matter how the image is changed.
- **Scaled Invariant**: It is the characteristic of key points that no matter how you scaled.
- **Clustering**: The scattered points needs to clustering that's way we choose K-means++ algorithm. It's the optimal clustering algorithm for choosing the seeds point.

2.4 Typical Copy Move Forgery Detection

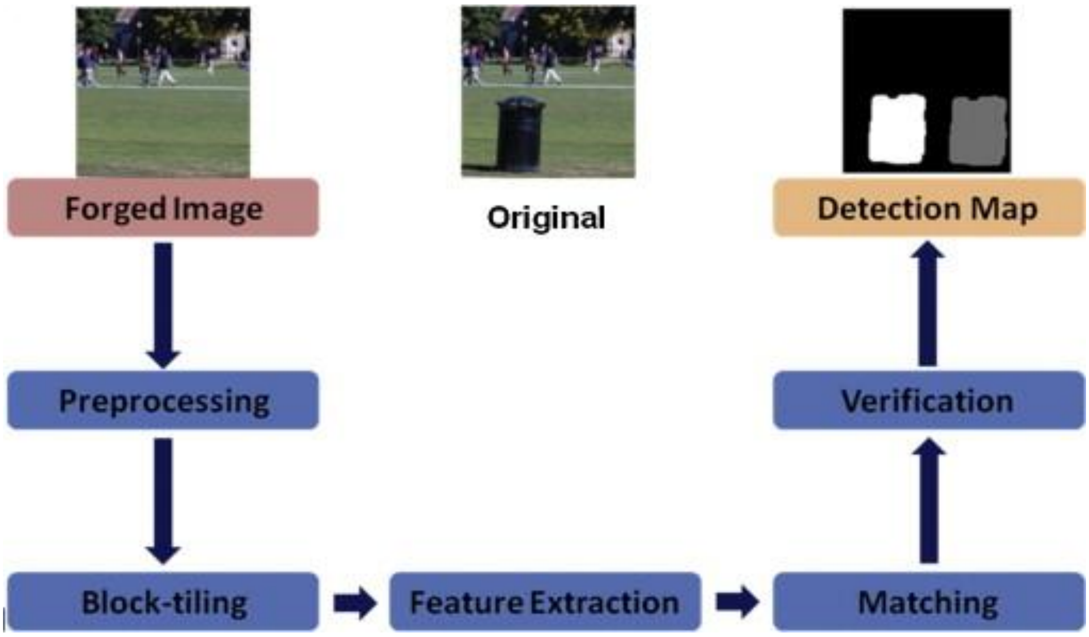


Figure 2.4.1: Typical Recognition System

2.5 Application of Copy Move Forgery Detection

- Detect copy move forgery.
- To reduce forgery rate
- To increase trustworthy of general people on digital images
- Identity forged portion of the image.
- Provide true news to the public and clear the confusion of the public.
- Reduce number of crimes.

2.6 ORB: an efficient alternative to SIFT or SURF

The ORB stands for Orientation and Rotated BRIEF, where BRIEF can be derived as Binary Robust Independent Elementary Feature. The main purpose of ORB algorithm is to create ORB descriptor. The ORB matching show the following figure.

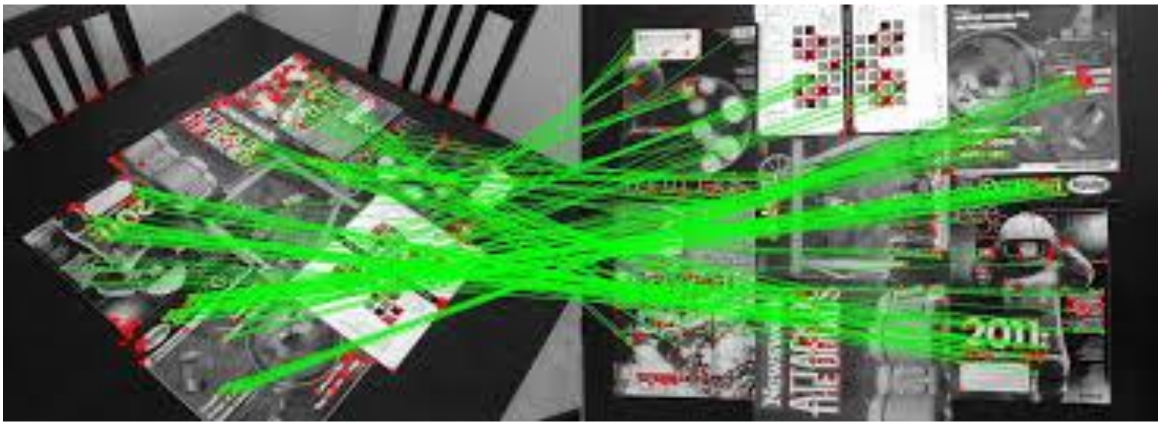


Figure 2.6.1: ORB feature matching.

The Computation of ORB algorithm takes several steps:

2.6.1 Extract Scaled ORB feature:

Actually ORB feature is not a scaling-invariant descriptor but in the field of image processing scale-invariant descriptor is important. For making the feature descriptor scaling-invariant, the pyramid scale information is assingned to each key point.

2.6.2 Extract the FAST key points:

For extracting key points we use a rapid algorithm known as FAST (Features from Accelerated Segment Test) [18,19]. It focus on every pixel and the Bresenham cyclo-region. Getting the accurate value we take the radius 3. Firstly, the number of pixels in Bresenham cyclo-region that are less or greater than the centric point(x,y) is checked. Then if the number is higher than the threshold, the centric point(x,y) is FAST-9 points. So it can be denoted as fast(i)=[x,y,oc,in].

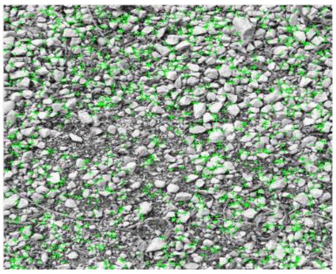


Figure 2.6.2.1: FAST key points.

2.6.3 Orientation compute:

For computing orientation of that key points needs to deal with the moment. The (p+q)th order invariant moment $m_{p,q}$of key point'O' is defined. To conveniently compute, the neighborhood N(x,y) is at the first quadrant of Cartesian coordinates, and 'O' is origin.

$$m_{p,q} = \sum_{x,y} x^p y^q \, I(x,y)$$

Then, the centroid 'C' of N(x, y)is determined as

$$C=\left(\frac{m_{10}}{m_{00}},\frac{m_{01}}{m_{00}}\right)$$

The orientation θ of the key point 'O' is determined by

$$\theta = \text{atan}\left(\frac{m_{01}}{m_{10}}\right)$$

Where, m_{10} is called row moment .

m_{01} is called column moment.

We get a new parameter is called Ө(Theta). So the equation becomes fast(i)=[x,y, Ө,oc,in]

2.7 Build the rBRIEF feature:

The binary feature of BRIEF is automatically translation invariance but no invariant rotation characteristic [13]. Therefore an efficient method to steer BRIEF is according to the orientation of key point θ, which can obtain the rBRIEF (Rotation-Aware BRIEF) feature with rotational invariance. A binary test τ is defined by

$$\tau(P\colon x,y) = \begin{cases} 1, & p(x) < p(y) \\ 0, & p(x) \geq p(y) \end{cases}$$

Where p(x) is the gray of point x. In addition, y satisfies the Gaussian distribution in the neighborhood of point x. The feature BRIEF is defined as a vector of n(n=256) binary tests:

$$f_n(p) = \sum_{1\leq i\leq n} 2^{i-1} \;\tau(P\colon x,y)$$

A feature set of n binary tests at x and y define matrix P=$\begin{bmatrix} x1 & \ldots.. & xn \\ y1 & \ldots.. & yn \end{bmatrix}$. using the operation Theta(Ѳi) and the corresponding rotation matrix $R_\Theta = \begin{bmatrix} cos\Theta_i & -sin\Theta_i \\ sin\Theta_i & cos\Theta_i \end{bmatrix}$, steered matrix P_{Θ_i} =R$\Theta_i. P$ will be constructed. Now ORB descriptor of oFAST point becomes

$$\text{ORB(i)} = f_n(p)|(x_i, y_i) \in P_\theta$$

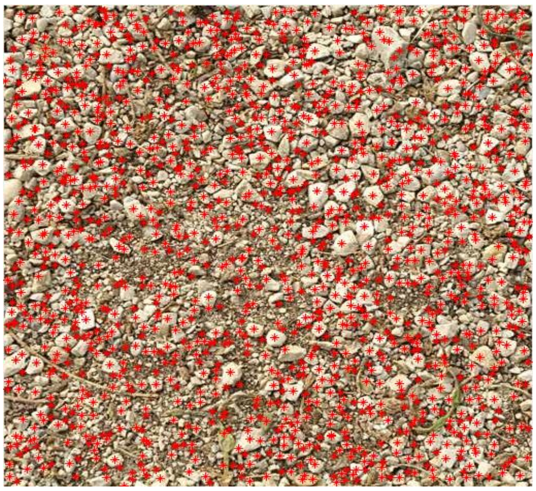


Figure 2.7.1: ORB Descriptor.

2.8 K-means++

D. Arthur and S. Vassilvitski proposed a clustering algorithm [17] known as k-means++. This is the extended version of k-means. Here the cluster center is chosen wisely. So the required number of iterations is less than k-means. In k-means++, the initial center is chosen randomly like k-means. K-means++ algorithm is then applied on the ORB descriptors.The distance between dataset X and its closest cluster center is represented as D(x). Now the algorithm follows these steps.

1. A cluster center c_1 is chosen randomly from the dataset X like k-means.
2. Then all the possible distances are calculated from the chosen center and denoted as D(x).

3. New cluster center c_i is chosen based on the distance D(x). The long distance cluster center is selected compared to all D(x) and this is known as weighted probability $D(x)^2 / \sum_{x \in X} D(x)^2$.
4. The steps 2 and 3 are repeated until the k centers are found.
5. All the processes are computed like the standard k-means algorithm.

Though the steps 2 and 3 take more time to select a perfect center, the step 5 converges very quickly which is the advantage of k-means++ over k-means clustering algorithm.

2.8.1 Why K-means++?

1. K-means has worst case running time while K-means++ has O(logk). Where k is the number of cluster.

2. K-means++ is an optimal clustering.

3. It requires fewer iterations and higher chance of finding the global optimal.

2.8.2 K-means++ pros/cons

1.Computationally cost relative to random initialization, but the subsequent K-means often converges more rapidly.

2. Tends to improve quality of local optimal and lower runtime.

2.8.3 Drawback of K-means++

1. It can find a suboptimal solution (it’s still an approximation)

2. Not consistency faster than Lloyd’s algorithm(K-means).

3.More complicated than Lloyd’s algorithm(K-means).

4. Better algorithm may exists for specific metric spaces.

5. NP-hard problem

2.9 Previous Work

To identify accurate features, a lot of researches have been published for detecting copy-moved regions. Many block-based and key-point based methods have been introduced to detect forged regions by identifying appropriate features which are scale invariant, translation and rotation. Numerous methods such as SIFT, ORB and BRISK are relatively new and very efficient to extract the feature. On the contrary, these methods require low computational cost compared to block-based method.

Fridrich et al. [5] proposed a method where DCT has been used to extract the features on the overleaping blocks. And it is known as block-based method. Here few datasets were used on their experiment. It was the first work on forgery image. In block-based method, if the forged region is scalable, it will not capable of detecting the tempered region.

Popescu et al. [6] proposed a method based on PCA for feature extraction. Approximately 100 images of size 512x512 have been used as their dataset. This method can’t be responsive in the geometric transformation i.e. after rotation and scaling of a sample, it can not be detected as forged.

Li et al. [7] mentioned a method based on DWT and SVD also known as block-based method. This method works only when the sample is being highly compressed or edge processed.

Huang et al. [9] and I. Amerini et al. [21] used SIFT feature extraction method and it was a key point based extraction method. Noisy and blurred sample can not be detected as a forged image.

Zhu et al. [16] proposed a method based on Scaled ORB where ORB features help to detect the forged region of a digital image. The dataset was collected from the Columbia University natural images library. But time complexity is not good as it compares all extracted descriptor. Descriptors being sent to clustering, our proposed method performs better. So it is needed to compare only clustered center to detect the forged region.

Jian Li et al. [20] used SIFT based approach where the running time for detecting the forged region is high and also its false positive rate is high. Kakar et al. [21] can not detect the multiple duplicate regions as forged image.

Chapter 3

Methodology

3.1 Overview of the Overall copy move forgery detection

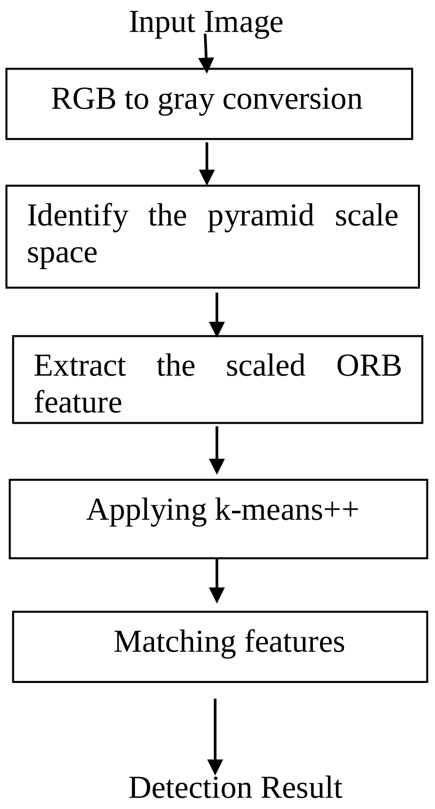


Figure 3.1: Flowchart of copy move forgery detection

3.2 Copy Move Forgery Detection Procedure

In order to have a clear understanding of the proposed system we have subdivided the whole system into seven parts-

- Image acquisition
- Image resize
- Image convert from RGB to grayscale
- Identify the pyramid scale space.
- Extract scaled ORB feature

1.Extract the FAST key points

2.Orientation Compute.

3.Build the rBRIEF feature.

- Clustering On ORB descriptor.
- Matching the feature.
- Remove the false matching
- Display image

Each of the sub-parts are discussed in details below.

3.2.1 Image Acquisition

For copy move forgery detection first of all we have to take an image. Then it should be checked and declared that image as forged or real. Image quality depends on two main aspects: lighting system and positioning system of image capturing device. Some other factors should be considered while taking image for copy move forgery detection :

i Capture image having sufficient resolution and sharpness.

ii Artifacts should be removed from the images for better recognition.

3.2.2 Image convert from RGB to grayscale

We have to convert image from RGB to grayscale. So that unnecessary data will be remove and our project task will be easier. Actually ORB descriptor can be gained from the grayscale image.

3.2.3 Identify the pyramid scaled space

To identify pyramid scaled space, Gaussian pyramid is used which was proposed by David Lowe [17]. With octaves and intervals, the pyramid scale space is constructed. Octaves mean an image which gained after resizing by the specific interval. With the help of Gaussian smoothing, same octaves are built in intervals. Where $L_{oc,\,in}(x, y, \sigma_{oc,\,in})$ is the pyramid scale space at ‘oc’ octave and ‘in’ interval, $G(x, y, \sigma)$ is Gaussian function, σ is the smoothing factor of Gaussian function.

$L_{1,1}(x,\mathrm{y},\sigma_{1,1})$ denote the gray image of the main image I(x, y).Last pyramid scale space $L_{oc,in}$ is achieved by down sampling of the last octave by a factor 2.

$$L_{oc,in}(x,y,\sigma_{oc,in}) = G(x,y,\sigma_{oc,in}) * L_{oc,in-1}(x,y,\sigma_{oc,in-1})$$

$$G(\mathrm{x},\mathrm{y},\sigma) = 1/2\pi\sigma^2 e^{-(x^2+y^2)/2\sigma^2}$$

3.2.4 Extract Scaled ORB feature

Actually ORB feature is not a scaling-invariant descriptor but in the field of image processing scale-invariant descriptor is important. For making the feature descriptor scaling-invariant, key points assign the pyramid scale information.

3.2.4.1 Extract the FAST key points

For extracting key points, we use a rapid algorithm known as FAST [18,19]. It concentrates on the Bresenham cyclo-region and each pixel. Getting the accurate value we take the radius equal to 3. Firstly, check the pixel's number in the Bresenham cyclo-region than the centric point(x, y). If the number of pixels is larger than the threshold value, the centric point(x, y) is known as FAST-9 points. So it can be denoted as fast(i)=[x, y,oc$_i$,in$_i$].

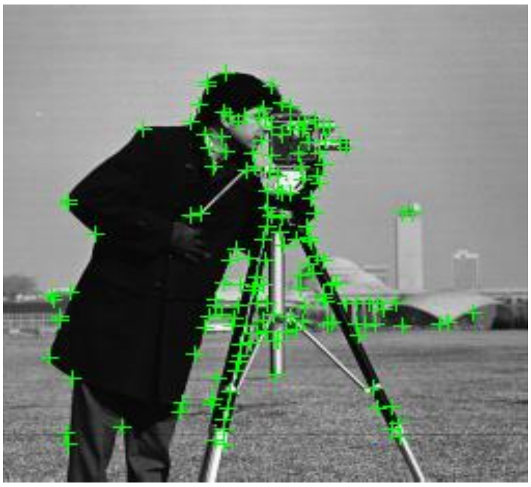


Figure 3.2.4.1: FAST key points.

3.2.4.2 Orientation Compute

For computing orientation of that key points needs to deal with the moment. The (p+q)th order invariant moment $m_{p,q}$of key point‘O’ is defined. To conveniently compute, the neighborhood N(x,y) is at the first quadrant of Cartesian coordinates, and ‘O’ is origin.

$$m_{p,q} = \sum_{x,y} x^p y^q \; I(x,y)$$

Then, the centroid ‘C’ of N(x, y)is determined as

$$\text{C=}\left(\frac{m_{10}}{m_{00}},\frac{m_{01}}{m_{00}}\right)$$

The orientation θ of the key point ‘O’ is determined by

$$\theta \; = \text{atan}\left(\frac{m_{01}}{m_{10}}\right)$$

Where, m_{10} is called row moment .

m_{01} is called column moment.

```
[row,col]=size(c);
 moment01=0;
 moment10=0;
 for i=1:row
   x=c(i,1);
   y=c(i,2);
 moment01=moment01+im(x,y)*y;
 moment10=moment10+im(x,y)*x;
 end
 theta=atan(moment01/moment10);
 %figure, imshow(im/4);
 image(im/4);
```

Moment calculation

We get a new parameter is called Ө(Theta). So the equation becomes fast(i)=[x,y, Ө,oc,in]

3.2.4.3 Build the rBRIEF feature

The binary feature of BRIEF is automatically translation invariance but no invariant rotation characteristic [13]. Therefore an efficient method to steer BRIEF is according to the orientation of key point θ, which can obtain the rBRIEF (Rotation-Aware BRIEF) feature with rotational invariance. A binary test τ is defined by

$$\tau(P\colon x, y) = \begin{cases} 1, & p(x) < p(y) \\ 0, & p(x) \geq p(y) \end{cases}$$

Where p(x) is the gray of point x. In addition, y satisfies the Gaussian distribution in the neighborhood of point x. The feature BRIEF is defined as a vector ofn(n=256) binary tests:

$$f_n(p) = \sum_{1 \leq i \leq n} 2^{i-1} \ \tau(P\colon x, y)$$

A feature set of n binary tests at x and y define matrix P=$\begin{bmatrix} x1 & \ldots\ldots & xn \\ y1 & \ldots\ldots & yn \end{bmatrix}$. using the operation Theta(ϴi) and the corresponding rotation matrix R_Θ =$\begin{bmatrix} cos\Theta_i & -sin\Theta_i \\ sin\Theta_i & cos\Theta_i \end{bmatrix}$, steered matrix P_{Θ_i} =R$\Theta_i . P$ will be constructed. Now ORB descriptor of oFAST point becomes

$$\text{ORB(i)} = f_n(p) | (x_i, y_i) \in P_\theta$$

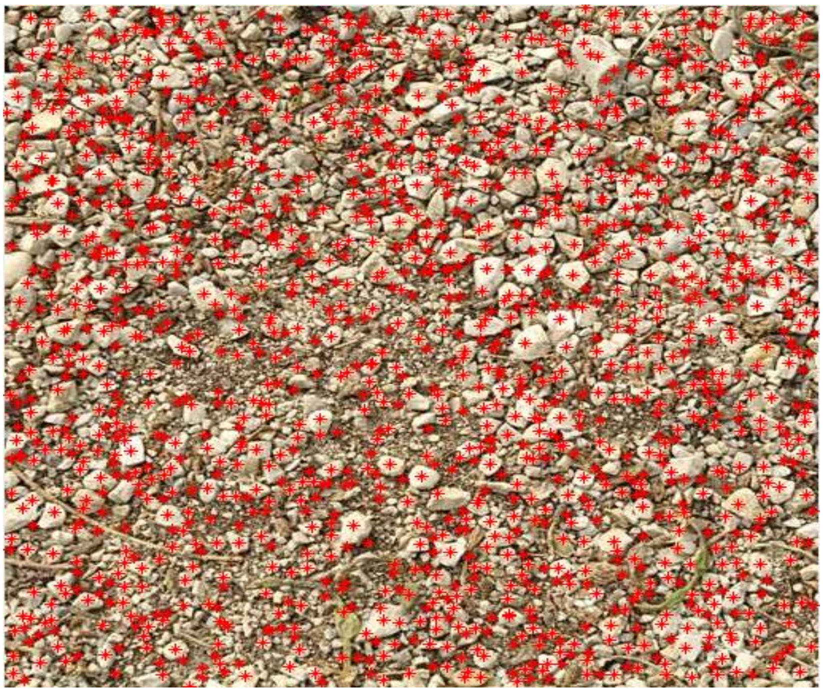


Figure 3.2.4.3.1: ORB Descriptor.

3.2.5 K-means++

A clustering algorithm proposed by David Arthur and Sergei Vassilvitski [10]. Where it initialize the center of the cluster for the K-means clustering algorithm.

Let D(x) represents the distance which is calculated between a data point x and its closest center. The algorithm consists of the following steps.

1. Select one center c_1 at random from the data points X.

2. Compute D(x) for each data point.

3. Select one new center c_i from the, using a weighted probability $D(x)^2 / \sum_{x \in X} D(x)^2$

4. Repeat 2-3 until k centers have been selected.

5. Continue the algorithm with the standard k-means.

In spite of the fact that steps (2-3) takes extra time, the k-means step (5) converges very fastly after this contribution and thus the algorithm reduces the computation time significantly.

3.2.6 Match the feature

The feature matching process compute using double loop i.e complexity N*N. Using double loop from 1-k the matching be checked. where K is the number of cluster of the ORB descriptor.

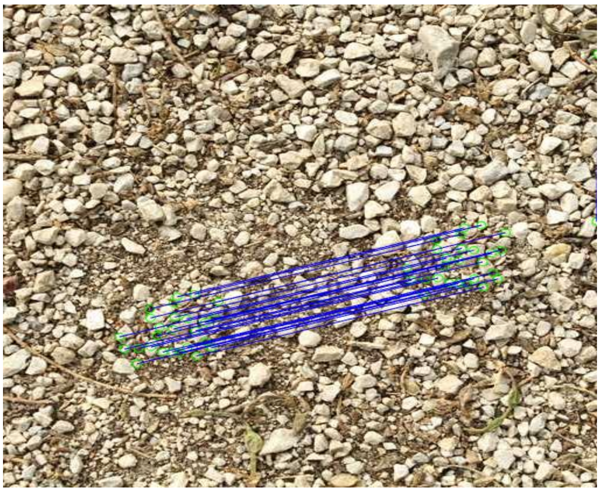


Figure 3.2.7.1: Showing feature match

Chapter 4

Implementation

The implementation view of this system requires designing a Graphical User Interface and development of a system which can be used to represent the estimated level of copy move forgery detection. The overall system in the User Interface first match the features then identify the forged region and finally provides output. In our Interface it also shows the graphical representation of calculated data in real time.

4.1 Implementation Tools

The necessary tools to implement this system can be divided into Categories-Hardware & Software as illustrated below:

- **Hardware Requirements**
  - Personal Computer
- **System Configuration**
  - Windows Operating System.
  - Dual core 2.66 GHz or faster processor
  - USB 2.0 bus
  - 2 GB RAM

- **Software Tools and Libraries**
  - MATLAB R2018a

4.1.1 Detailed Hardware Requirements

First of all we need a laptop or desktop which has sufficient properties to complete our task. But some hardware is recommended for fast calculations in our system architecture for image processing. Following table shows the minimum and recommended hardware requirements.

Table 4.1.1.: Hardware Requirements

	Minimum	Recommended
Processor Type	Dual-core	Core-i5
Clock Speed	2.3 GHz	3.1 GHz
RAM	2GB	4 GB
Hard Drive Space	2 GB	4 GB
OS	32 Bit Windows 7	64 Bit Windows10
USB Port	2.0	3.0

4.2 Implementation Details

The first phase of the implementation for this system is to establish a set up environment. Then we have to maintain the following procedure-

- Image acquisition
- Identify the pyramid scale space.
- Image convert from RGB to grayscale
- Extract scaled ORB feature.
  - i) Extract the FAST key points
  - ii) Orientation Compute.
  - iii) Build the rBRIEF feature.
- K-means++ Clustering.
- Matching feature.
- Display the forged image

4.2.1 Image Acquisition

We can take an image through image read.

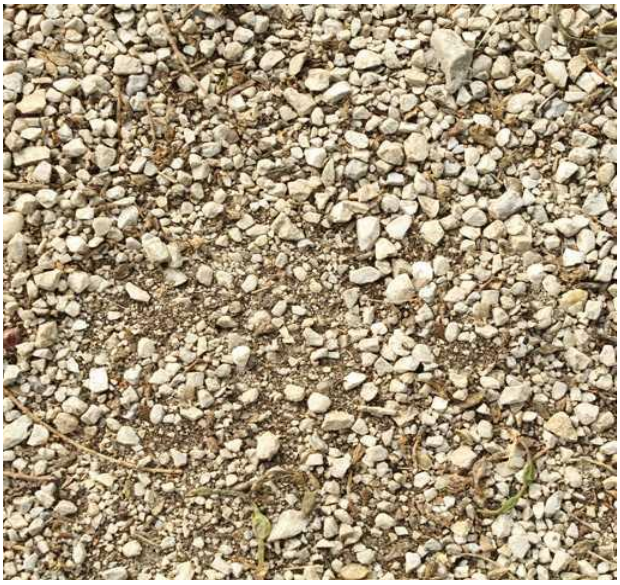


Figure 4.2.1.1: Image acquisition

4.2.2 Image Convert from RGB to grayscale

We have to convert image from RGB to grayscale. So that unnecessary data will be remove and our task will be easier.. By using rgb2gray an image can easily convert to grayscale. Figure 4.2.3.1 shows that-

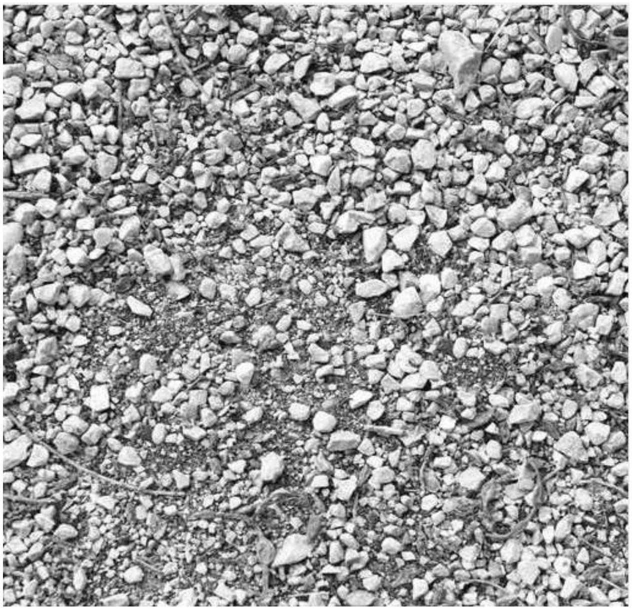


Figure 4.2.2.1: RGB to grayscale

4.2.3 Identify pyramid scale space

Actually this is a resizing step of an image. For our convenient purpose, image needs to subsampling at the interval 2. If an image is being 512x512 then next octave will be 256x256.

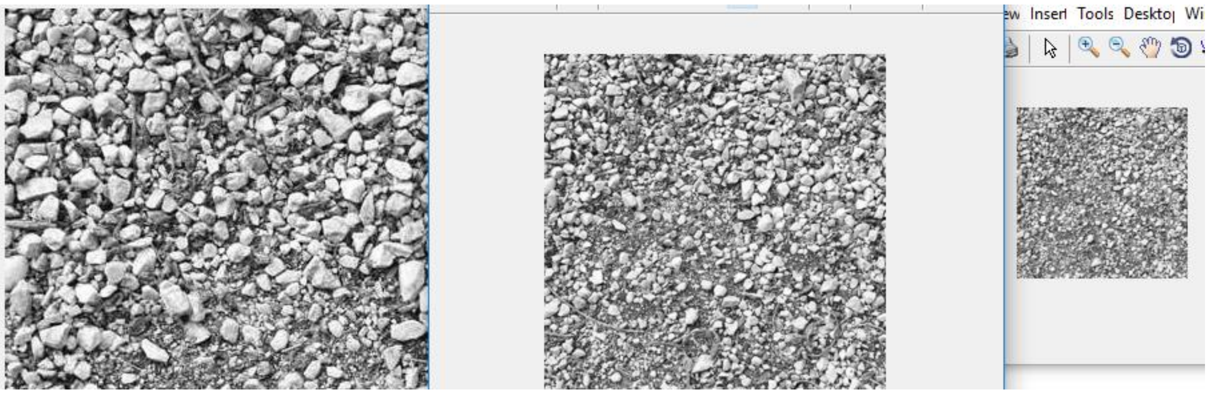


Figure 4.2.3.1: Identify Pyramid scale space.

4.2.4 Extract scaled ORB feature

Using the DetectFASTFeatures() build in function detects the corners points and their location. Then applying the central moment and rotation matrix on that points the ORB descriptors are being extracted. The following two figure illustrates that, First one is FAST features and the second one is ORB descriptors after applying moment and rotation.

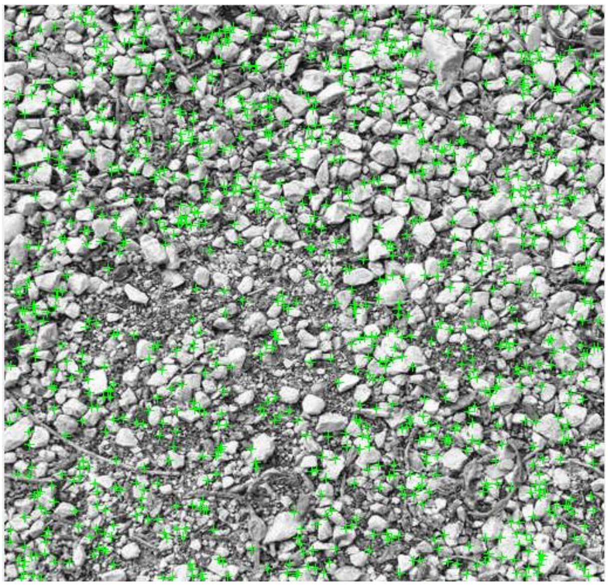


Figure 4.2.4.1: Extract Fast key points.

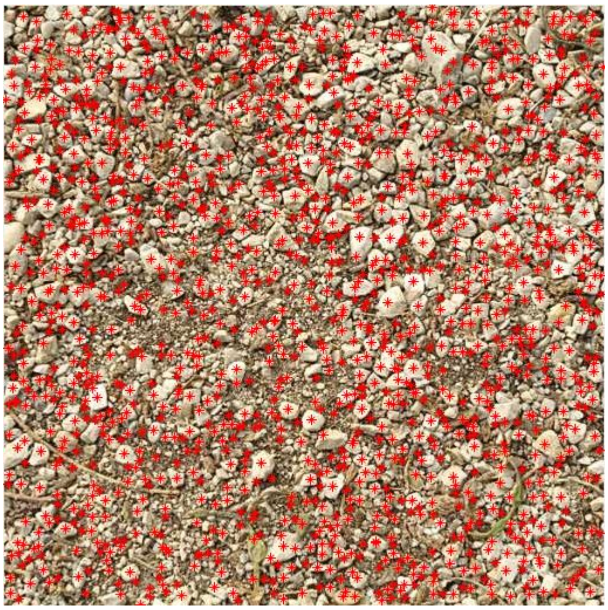


Figure 4.2.4.2: ORB descriptors.

4.2.5 K-means++

Now applying K-means++ clustering algorithm on the ORB descriptors getting the less clustered key points which are used in matching process and decrease the time complexity.

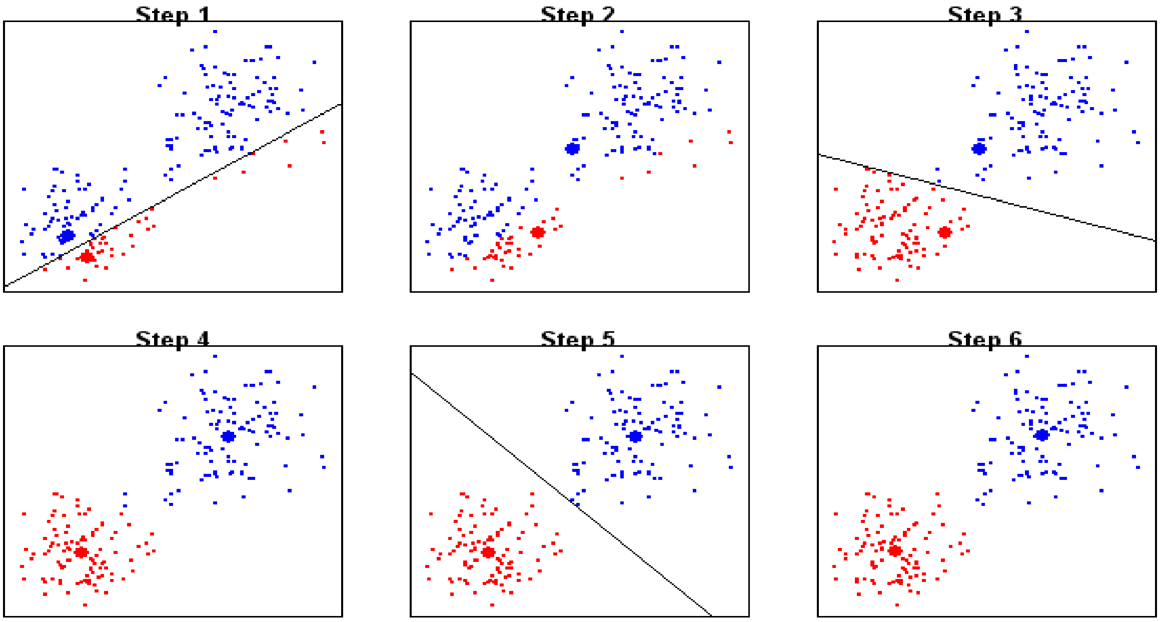


Figure 4.2.6.1: Clustering steps

4.2.6 Feature Match

Feature matching be performed using clustered by clustered. A double loop is used to performed this. And here complexity of the matching process is N*N.

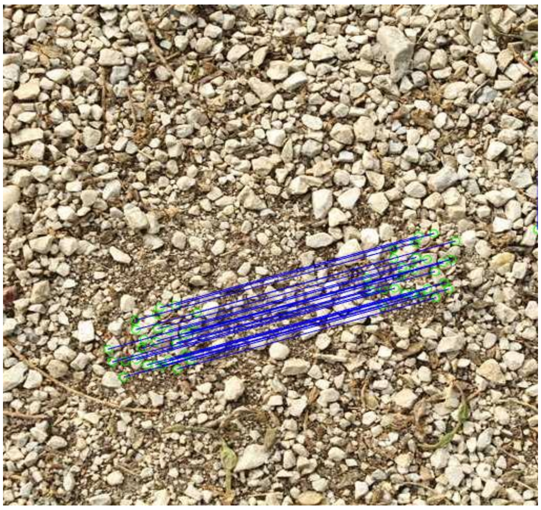


Figure 4.2.7.1: Matching result.

4.2.7 Display Image

Now recall the main image and displaying the result with drawing the circle.

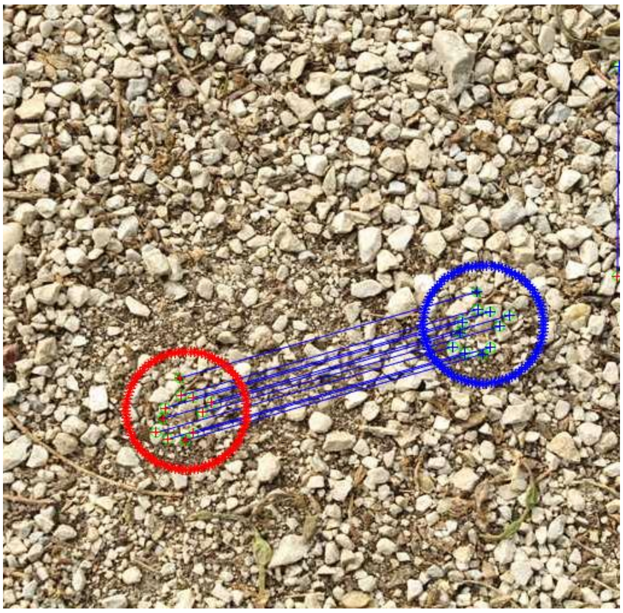


Figure 4.2.8.1: Display forged image

Chapter 5

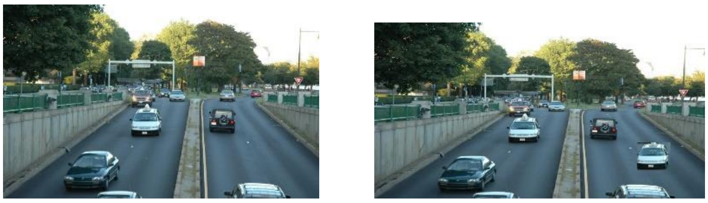
Experimental Results and Discussion

5.1 Experiment Setup

ORB algorithm was firstly implemented by Zhu et al. [16] to find out the ORB descriptors. The experimental environment follows the windows 10 operating system and the Matlab R2018b. Dataset is collected from MICC-F220 and CoMoFoD (small)[22] for this project. We also created 30 dataset for checking our proposed method.

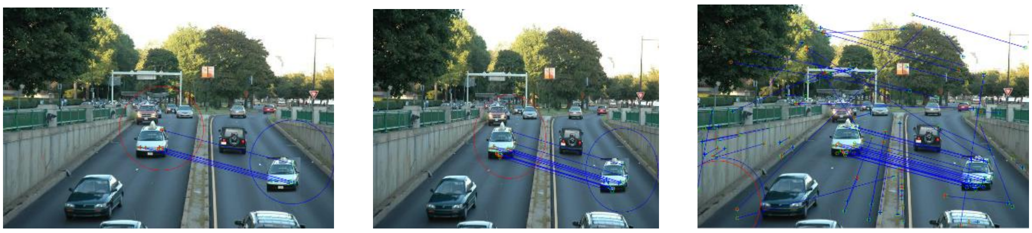
5.2 Experiment results and analysis

The proposed method is evaluated using the dataset of MICC-220 and CoMoFoD (small) [22]. Dataset in different size like 1000*700 or 700*1000 which are divided into three groups. Some non-compressed dataset with only translation of copied region, some are only non-compressed and some are simple scenes. In 2013, the CoMoFod (small) [22] database was publicized where the size of the dataset was 512*512 in PNG format. Different categories of images are stored in this dataset like translation (40 images), rotation and scaling (40 images). The original image is shown in figure 4(a) from the dataset of MICC-F220. The tempered form of the original image is shown in figure 4(b). The temper detection of the images is shown in figure 5 on the basis of different threshold value. When the low threshold value is applied, less number of key points is extracted. If the forged region is small, the possibility of extracting the key points decreases. As a result, it becomes difficult to detect the forged region. When the threshold value is high, it extracts large number of key points and the possibility to detect the false match increases.



(a) Original image (b) Tempered image

Figure 5.2.1: Tempered image with its original image.



(a) T=0.4 (b) T=0.5 (c) T=0.8

Figure 5.2.2: Detection result of tampered image in different threshold

Table 5.2.1: Matching result with different threshold value

Threshold value	0.1	0.3	0.4	0.5	0.6	0.8
Number of matches	12	24	26	30	36	146
Number of false matches	0	0	0	2	9	too many

We performed some common post processing methods on MICC-F220 dataset of temper images for making our method robust and sensitive. Most of the images are from different papers and internet. The optimal threshold value is taken T=0.5. When the threshold value is low, less number of key points is extracted. But when the threshold value is high, large number of key points is extracted where the probability of false matching increases figure 10(c). So the threshold value is kept at optimal level to detect the forged region efficiently. To measure the performance of the proposed method a confusion matrices is used. We used the dataset of MICC-F220 which consists of 50 images. The dataset has both forged and original images. We performed our test and result as follows: 40 forged images are detected as forged, 5 forged images are detected as original image, 2 original images are detected as forged image, and 3 original images are detected as original images.

Table 5.2.2: Confusion matrics

Number of images	TP	FP	TN	FP	Accuracy
50	40	5	2	3	86%

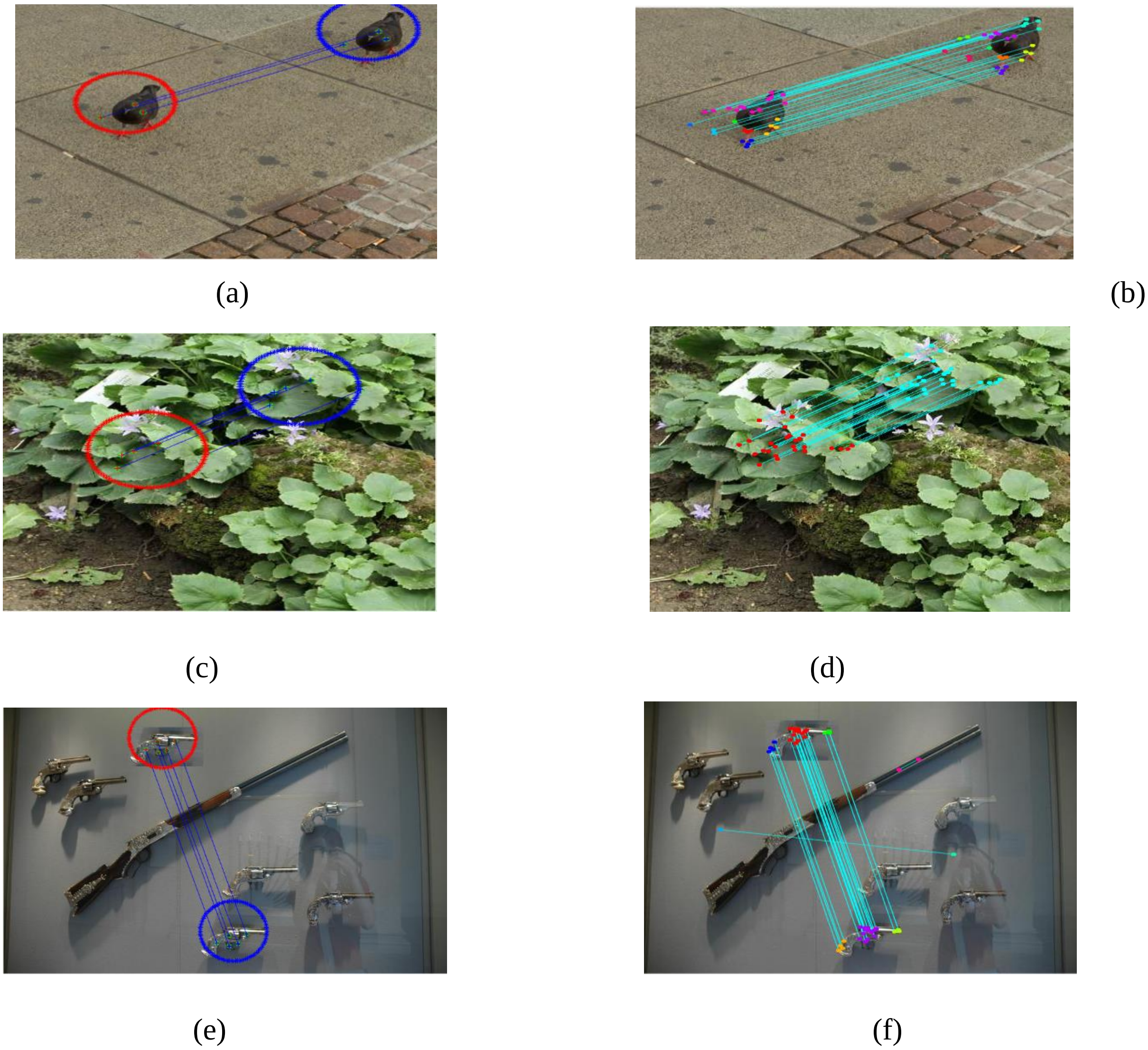
5.3 Comparison with a SIFT[19]method

Images	Method	Elapsed time(second)	No matches of	True match	False match
1.Baboon	ORB and K-means++	0.7457	84	84	0
	SIFT	3.8326	162	162	0
2.Stones	ORB and K-means++	1.0929	70	68	2
	SIFT	15.020270	193	193	0
3.Road and cars	ORB and K-means++	1.034195	30	30	0
	SIFT	2.5560	53	53	0
4.Pegion	ORB and K-means++	0.549761	46	46	0
	SIFT	2.600425	54	52	2
5. Grass and Number plate.	ORB and K-means++	0.771040	210	208	2
	SIFT	11.2812	850	812	38
6.Large coin	ORB and K-means++	0.621096	264	234	30
	SIFT	2.284661	366	292	74
7.Rifles	ORB and K-means++	0.931181	38	32	6
	SIFT	1.630468	43	41	2
8.Books	ORB and K-means++	0.600027	86	84	2
	SIFT	2.416834	166	166	0
9.Window	ORB and K-means++	0.513452	104	84	20
	SIFT	2.397863	267	241	26

Table 5.3.1: The matched key points and running time

Methods	The number of key matched points(Total)	Running time Sec (Total)	False match (Total)
SIFT[19]	3589	73.3386	246
Proposed Method	1553	13.2594	104

Above table shows the calculation of 15 forged images from the dataset of MICC-F220.



(a) (b)

(c) (d)

(e) (f)

Figure 5.3.1: Result of Scaled ORB and k-means++ and SIFT[19] respectively

Table 5.3.2: Threshold value setting based on forged region detection

Threshold	Detection of forged region	Non forged region detected as forged
0.1	Fair	No
0.3	Fair	No
0.5	Good	No
0.8	Bad	Yes

Table 5.3.3: The Performance rate for different methods

Modifications	Different methods		
	G.Lynch[23]	*Y.Huang[8]*	Proposed method
Without modification	97%	99.9%	99.9%
Rotation	0%	Only less than 5 deg.	99.5%
JPEG compression	30%	80%	68%

5.4 Input Image & Output Image

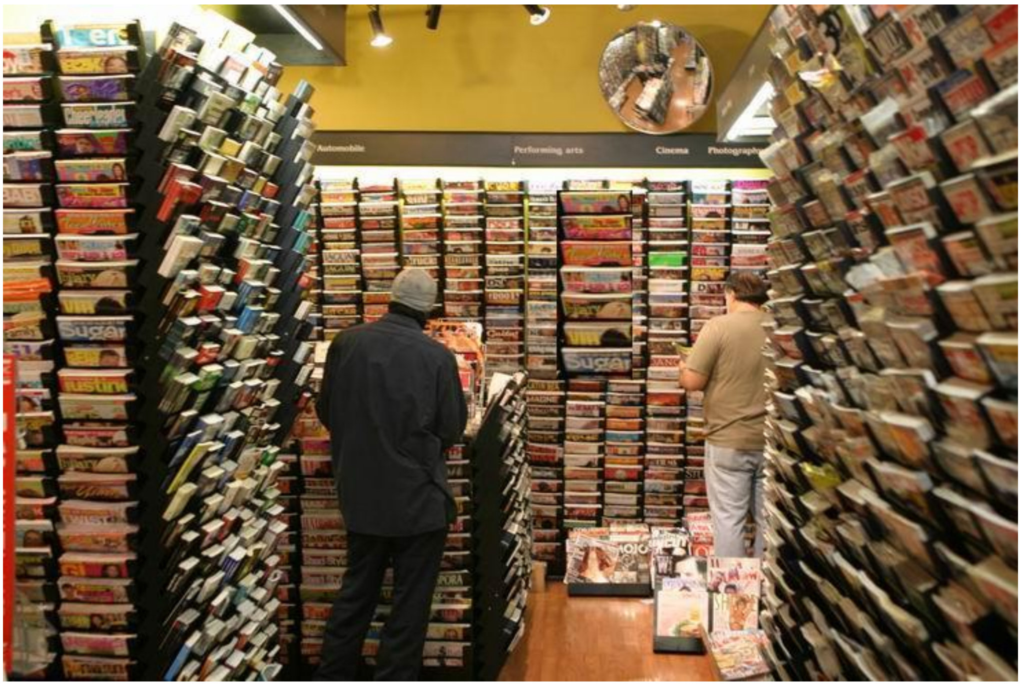


Figure 5.4.1: Input image

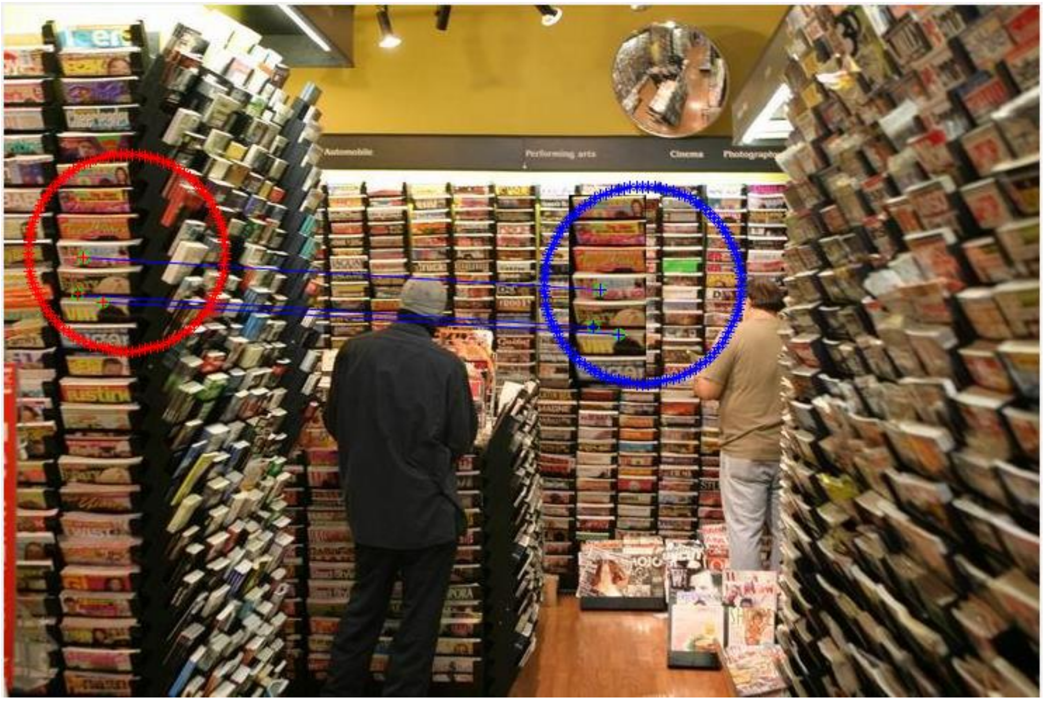


Figure 5.4.1: Output image

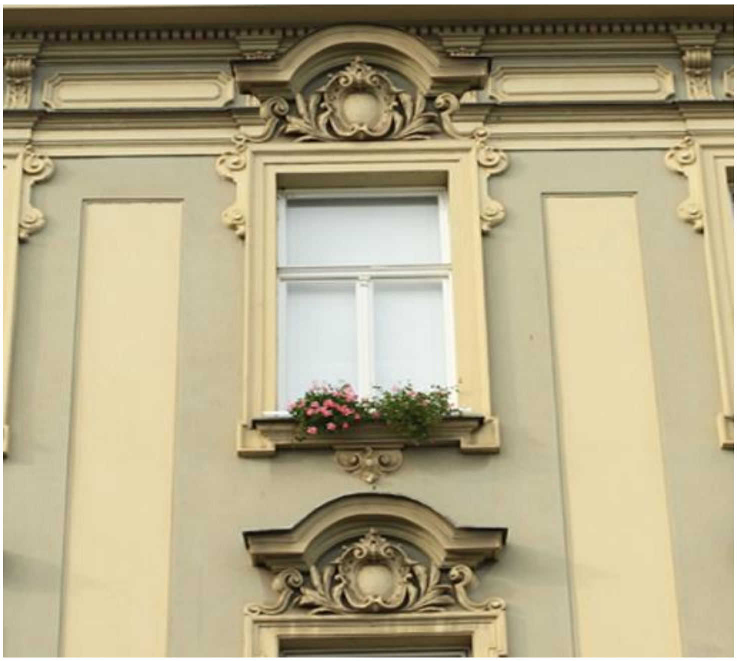


Figure 5.4.2: Input image

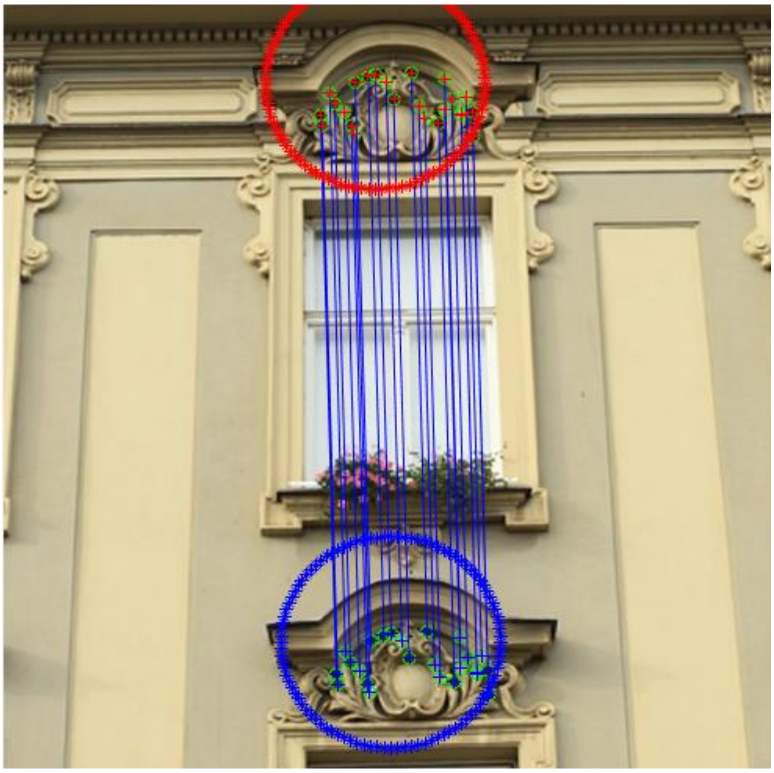


Figure 5.4.2: Output image

5.5 Discussion

The Primary focus of this work is to develop a framework that can estimate the level of accuracy by implementing the proposed algorithm in simulated environment. This research results can be implemented for further improvement of copy move forgery detection. Though level of detection is a relative matter based on image features, we tried to establish an aesthetic framework for this project. The experimental results especially the quantitative evaluation revealed that the propose system is functioning well. Although the results degreed in some cases due to some environmental factors and some complexity in manual measurements, the overall performance can be said satisfactory. Moreover, it can be said that the project is successful to estimate the proper level of copy move forgery detection rate of performance in simulated environment.

Chapter 6

Conclusion and Future Recommendation

We have worked with Accuracy Level of copy move forgery detection. It is a very important factor to create a standard method to detect copy move forgery. In this paper we focused on developing the copy move forgery detection, based on features matching. This chapter contains an overview of the system and its limitations with future recommendations.

6.1 Conclusion

In this paper, an efficient forensic method based on the scaled ORB for detecting the copy-move forgery in digital image was proposed. The method not only detects duplicated regions but also determines the geometric transformations and post-processing applied to the forged regions. In addition, when duplicate regions of which SIFT[19] and SURF[16] cannot detected in locating, that algorithm also perform good. However, the method is still time consuming for forgery detection of high resolution images.

6.2 Future Recommendations

Though we have done our project successfully but there are some opportunities to improve the system. First of all we can say that if we could enhancement image then image quality would increase and our accuracy rate would also increase. The future recommendations are

- Copy move forgery from different image should have detected.
- Using noise reducing system and make the system more accurate.
- Some false descriptor also be marked, so try to remove those false match.
- Applying different post processing method on tempered image, detect the forged region.

When our system will get those facilities then our system will more accurate and faster. Since there was not enough time to add all of those facilities, we hope next we can add those facilities if we get an opportunity. Moreover, our system was better than previous systems. Hoping one this system will be best system for copy move forgery detection.

Bibliography

[1] Mahdian, Babak, and S. Saic. “Detection of copy-move forgery using a method based on blur moment invariants”, *Forensic science international* 171.2 (2007): 180-189.

[2] Huang, Hailing, W.Guo, and Y. Zhang. “Detection of Copy-Move Forgery in Digital Images Using SIFT Algorithm”, *Computational Intelligence and Industrial Application,* 2008. PACIIA’08. Pacifc-Asia Workshop on. Vol. 2. IEEE,2008.

[3] M. Fischler, Bolles, “Random sample consensus: a paradigm for model fitting with applications to image analysis and automated cartography ”, *Communications of the ACM 24, 6(1981),381-395*

[4] Qureshi, M. Ali, and M. Deriche “A bibliography of pixel-based blind image forgery detection techniques”, *Signal Processing: Image Communication 39* (2015): 46-74.

[5] Fridrich., Soukal, and Lukas, A.J., “Detection of Copy-Move Forgery in Digital Images”, *In Proceedings of Digital Forensic Research Workshop, Citeseer(2003).*

[6] Popescu, Farid, “Exposing digital forgeries by detecting duplicated image regions*”, Dept. Comput.Sci., Darmouth College, Tech. Rep.* TR2004-515,(2004).

[7] Li, Guohui, et al. “A sorted neighbourhood approach for detecting duplicate regions in image forgeries based on DWT and SVD”, *Multimedia and Expo, 2007 IEEE International Conference on. IEEE,2007*

[8] Huang, Yanping, et al. “Improved DCT-based detection of copy-move forgery in images”, *Forensic science international* 206.1 (2011):178-184.

[9] Huang, Hailing, W.Guo, and Y. Zhang. “Detection of copy-move forgery in digital images using SIFT algorithm”, *Computational Intelligence and Industrial Application, 2008. PACIIA’08. Pacific-Asia Workshop on. Vol.2.IEEE,2008.*

[10] B.Yang, X. Sun, H. Guo, Z. Xia, X. Chen. “A copy move forgery detection method based of CMFD-SIFT”.

[11] Pan, Xunyu, and S. Lyu. “Region duplication detection using image feature matching*”, Information Forensic and Security,* IEEE Transactions on 5.4(2010): 857-867.

[12] Jaberi, Maryam et al. “Accurate and roboust localization of duplicated region in copy-move image forgery”, *Machine vision and applications* 25.2.(2014):451-475

[13] Shivakumar, and L. D. S. S. Baboo. "Detection of Region Duplication Forgery in Digital Images Using SURF", *IJCSI International Journal of Computer Science Issue* 8.4(2011).

[14] Bo, Xu, et al. "Image Copy-Move Forgery Detection Based on SURF", *Multimedia Information Networking and Security (MINES),2010 International Conference on IEEE,* 2010.

[15] Isaac, M. Mary, and M. Wilscy. "Copy-Move forgery detection based on Harris Corner points and BRISK", *Proceedings of the Third Internation Symposium on Women in Computing and Informatics.* ACM,2015.

[16] Zhu, Ye, X. Shen, and H. Chen. "Copy-move forgery detection based on scaled ORB*", Multimedia Tools and Applications(2015*): 1-13.

[17] D Arthur, S. vassilvitskii, "K-means++ : the advantages of careful seeding*", in Proceedings of the 18th SODA,2007,*pp,1027-1035.

[18] M. Fischler, Bolles "Random sample consensus: a paradigm for model fitting with applications to image analysis and automated cartography", Commun ACM 24:381-395.

[19] Amerini, Irene, et al. "A sift-based forensic method for copy-move attack detection and transformation recovery", *Information Forensics and Security, IEEE Transactions on 6.3 (*2011): 1099-1110.

[20] J. Li, X. Li, B. Yang, and X. Sun, "Segmentation-Based Image Copy-Move Forgery Detection Scheme", *IEEE Trans. Inform. Forensics and Security,* vol. 10, no. 3, pp.507-518, March 2015.

[21] P. Kakar and N. Sudha, "Exposing postprocessed copypaste forgeries through transform-invariant features", *IEEE Trans. Inf. Forensics Security, vol. 7, no. 3,* pp. 10181028, jun.2012.

[22] Tralic, Dijana, et al. "CoMoFoD—New database for copy –move forgery detection." ELMAR, 2013 55th *International Symposium. IEEE,* 2013

[23] G. Lynch, F.Y.Shin and H.Y.M.Liao, "An efficient expanding block algorithm for image copy-move forgery detection", *Elsevier Science* Inc. 2013,pp. 253-265