Detection of Geometric Transformations in Copy-Move Forgery of Digital Images

Thesis submitted in partial fulfillment
of the requirements for the degree of

Master of Technology

in

Computer Science and Engineering

by

Meenal Shandilya

(Roll No: 213CS2171)

under the guidance of

Prof. Ruchira Naskar

Department of Computer Science and Engineering
National Institute of Technology, Rourkela
Rourkela-769 008, Odisha, India
June, 2015.

Department of Computer Science and Engineering
National Institute of Technology Rourkela
Rourkela-769 008, Odisha, India.

Certificate

This is to certify that the work in the thesis entitled " ***Detection of Geometric Transformations in Copy-Move Forgery of Digital Images***" submitted by ***Meenal Shandilya*** as the record of an original research work carried out by her under my supervision and guidance in partial fulfillment of the requirements for the award of the degree of Master of Technology in Computer Science and Engineering, National Institute of Technology, Rourkela. Neither this thesis nor any part of it has been submitted for any degree or academic award elsewhere.

Prof. Ruchira Naskar
Assistant Professor
Department of CSE
National Institute of Technology
Rourkela-769008

Place: NIT,Rourkela-769008
Date: 29 - 05 - 2015

Acknowledgment

The success of a project requires help and contribution from numerous individuals and the organization. First of all, I would like to express my heart felt gratitude to my project supervisor Prof. Ruchira Naskar . Her constant support and encouragement has made me realize that it is the process of learning which weighs more than the end result. Without her invaluable advice and assistance it would not have been possible for me to complete this thesis. Writing the report of this project work gives me an opportunity to express my gratitude to everyone who has helped in shaping up the final outcome of my project work. I would like to take this opportunity to express my thanks towards the teaching and non- teaching staff in the Department of Information technology. I am also grateful to all my parents and my friends for their concerns, help, encouragement, and suggestions.

Meenal Shandilya

Abstract

Digital Forensics is a branch of forensic science which is related to cyber crime. It basically involves the detection, recovery and investigation of material found in digital devices. Digital images and videos plays most important role in digital forensics. They are the prime evidences of any crime scene. So the fidelity of the image is important. Digital images can be easily manipulated and edited with the help of image processing tools. Copy-move Forgery is the most primitive form of cyber attack on digital images. In Copy-move forgery a part of image (region) itself is copied and pasted into another part of the same image. The intension behind this type of attack is to "add" or "disappear" some objects from the image. Hence to break the fidelity of the image and fool the viewer. Copy-move attack is more prevalent in images having uniform texture or patterns, for e.g. sand, grass, water etc. In this thesis exact block matching is used as a detection technique. This technique is based on block matching, for these the whole image is divided into number of block and then the matching process is applied.

Sometimes the copied region is processed before pasted i.e. some geometric transformations is applied on the pasted region. The transformations like scaling, rotation etc. It is not possible for human eyes to detect such kind of forgeries. Whenever forgery is done in this manner the common techniques like block matching, exhaustive search, auto-correlation and robust match etc. are not able to detect the forgery having geometric transformations. So that for identification of forged region we need some technique which are based on local features and also invariant to transformations. In this thesis SIFT is used for forgery detection. SIFT stands for Scale Invariant Feature Transform, this gives local feature points which are invariant to scales. The key points helps to find the duplicated region with different matching algorithms.

Contents

List of Figures

Chapter 1

Introduction

Digital Forensics is a branch of forensic science which is related to cyber-crime. It basically involves the detection, recovery and investigation of material found in digital devices. The digital forensic is commonly known as Computer forensic. In nowadays it is not just related with the computer device because the forensic has expended to cover investigation of all the devices which are able to store the digital data. Digital forensics is the process of uncovering and interpreting electronic data for use in a court of law. The goal of the process is to preserve any evidence in its most original form while performing a structured investigation by collecting, identifying and validating the digital information for the purpose of reconstructing past events.

forensic investigation of digital media devices, intellectual property theft detection and investigation, fraud detection, e-discovery of potential digital evidences and testifying those in courtroom, confirm alibis or statements, determine intent identify sources (e.g. in copyright cases) and authenticate documents.

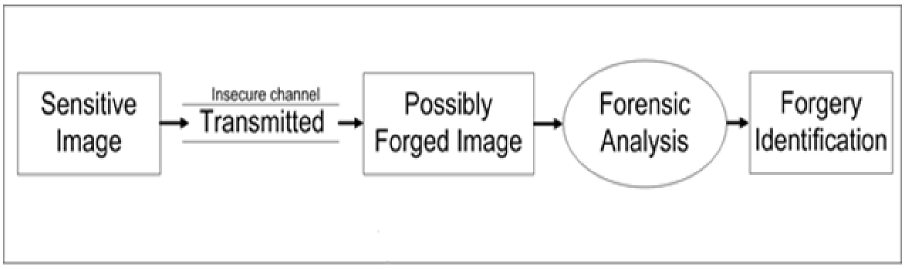

Figure 1.1: Example of a digital forgery.

Digital data like image and video plays most significant role in digital forensics. The authenticity of an image is the major issue in digital image forensic They are the most powerful form of evidences in media-broadcast industry as well as in the courtroom. The improvement and advancement of technology arises questions about the reliability of the digital images or videos, because of the cheap availability of the software and powerful image processing tools.

1.1 Digital Image Forgery

Image forgery is basically divided into broad approaches: Active approach and Passive Approach. The active approach involves digital watermarking and digital signature while passive approach involves tempering in images. The area of work is focused on Passive part of the forgery. In nowadays many digital forgeries are developed like Image splicing, retouching And copy-move Forgery. Image splicing makes composite image by joining two or more images. Image retouching is a process of enhancing image features such as sharpness, color adjustment, white balance etc.

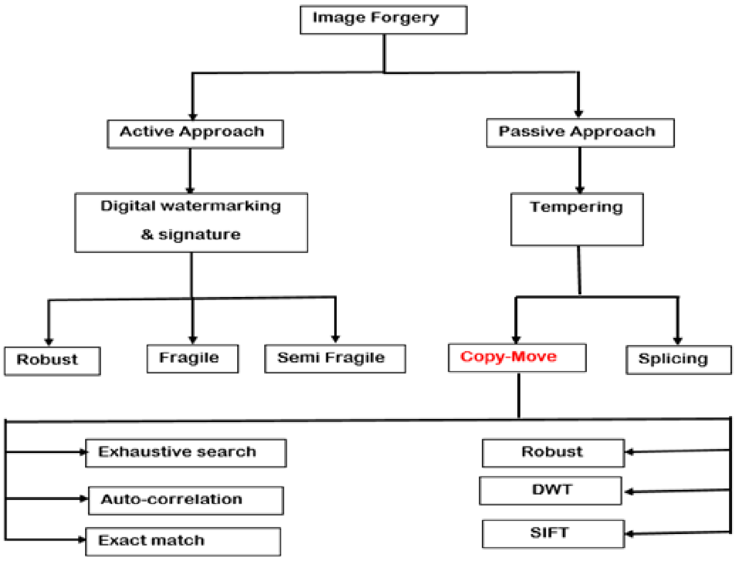

Figure 1.2: DIgital Image Forgery Approaches.

1.2 Copy-Move Forgery

Copy-move forgery is the most primitive form of cyber attack on digital images. In copy-move forgery a part of image (region) itself is copied and pasted into another part of the same image. The intention of the attacker behind this, is to “add” or “disappear” some objects from the image. Hence to break the fidelity of the image and fool the viewer. Copy-move attack is more prevalent in images having uniform texture or patterns, for e.g. sand, grass, water etc.

In Figure 1.3 image a) is the original image and image b) is the forged one. The original image have some clues which are hidden by other regions of the same image. So that the identification of such forgeries are important in digital forensic.

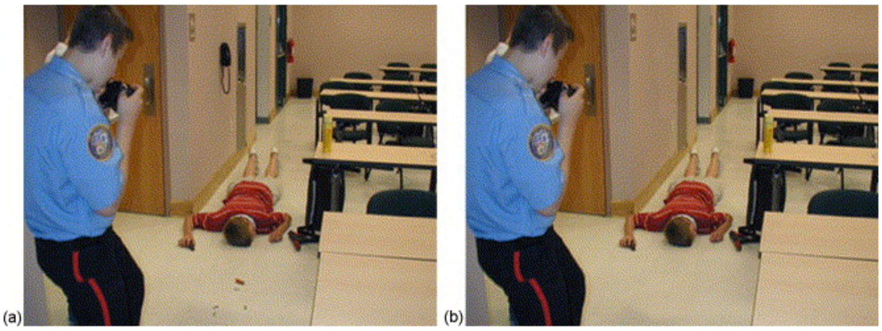

Figure 1.3: a) Original Image b) Forged Image.
[7]

1.3 Motivation

Digital images and videos plays most important role in digital forensics. They are the prime evidences of any crime scene. So the fidelity of the image is important. Digital images can be easily manipulated and edited with the help of image processing tools. This is due to the cheap availability of powerful image processing and editing software. It is difficult to perceptually distinguish the edited image from the original image. It is not possible to identify the forged image or the forgery with necked eyes. The forgery can be done with only one image, two images or more than two images. In copy-move type of forgery the attacker needs only one image i.e. the original image and performs forgery with that particular image only. The purpose behind this thesis is to detect copy-move in digital images while the duplicated region is geometrically transformed.

1.4 Problem Statement

In the copy-move forgery detection the exact block matching gives appropriate results only when the copied region is directly pasted i.e. duplication is performed without any transformations. If in case the copied region being transformed geometrically then block matching and correlation methods are fail to detect the forgery. So that we need some technique which gives correct matching in these situations.

Some useful methods are available for identification purpose of such kind of copy-move forgery detection, they are SIFT,Speed-Up Robust Features (SURF), Harris Detector. The SIFT is more invariant than the other methods. So that in this thesis the key points extraction is performed by using SIFT.

1.5 Objective

1. Detection of copy-move forgery in digital images.

   In this we are using exact block matching technique, divides the image into over-lapping blocks and perform matching of the extracted blocks.

2. Detection of geometric transformations like rotation, re-scale of duplicated image regions.

   This technique identifies geometric transformations applied on the copied region. The geometric transformations are like rotation, rescaling and both rotation and re-scaling. The exact block matching technique is not able to detect those forgeries.

1.6 Organisation of Thesis

In Chapter 2 we present a survey of existing literatures related to digital image forgery detection. In Chapter 3 represents detection technique of copy-move forgery. We are using exact block matching technique for identification purpose. The working of exact block matching is mentioned there. Chapter 4 covers detection of geometric transformations in copy-move forgery technique. To identify such forgeries we uses SIFT as detection technique. The details about SIFT is given in Chapter 4. In Chapter 5 we describe all the simulation results of copy-move and region duplication with geometric transformations. Finally Chapter 6 is conclusion and future work.

Chapter 2

Literature Review

One of the pioneer works in the direction of detection of copy-move forgery was done by Fridrich et.al. [5]. The authors [5] discussed different techniques to identify the forgery. The techniques are Exhaustive search, Auto-correlation , Exact block match and Robust match. In all the techniques Exact block matching is described in details in further chapters. The main idea of exact block matching is divide the whole image into non overlapping block and perform matching between those blocks and find out the copied – pasted blocks. Any Copy-Move forgery introduces a correlation between the original image segment and the pasted one. This correlation can be used as a basis for a successful detection of this type of forgery. Because the forgery will likely be saved in the lossy Joint Photographic Experts Group (JPEG) format and because of a possible use of the retouch tool or other localized image processing tools, the segments may not match exactly but only approximately [5].
A robust detection algorithm for copy-move forgery in digital images is proposed by Cao et.al. [3]. They also uses block matching method with Discrete Cosine Transform (DTC) transformation. The framework of the method is as follow:

1. Diving the suspicious image into fixed size blocks.

2. Apply DCT to generate quantized coefficients.

3. Extract features from quantized coefficient with the help of circle block.

4. Searching similar block pairs.

5. Finding correct blocks.

According to Pan and Lyu most existing methods to detect region duplication are based on searching exact copies of pixel blocks, which cannot handle cases when a region is scaled or rotated before pasted to a new location [13]. They uses SIFT method to identify the duplication region because SIFT is not a global vector but it is a local feature. The key points extracted by this method are invariant to different scales. Each key point is associated with 128 dimension feature vector, which makes the key points distinctive. After that matching and pruning of the SIFT key points has done and then the process of estimating duplicated region is performed.

Memon et.al. [2] proposed An efficient and robust method for detecting copy move forgery. The method is robust to lossy compression, scaling and rotation type of forgeries. They uses Fourier-Mellin Transform (FMT), Counting Bloom Filters. [2]. David lowe et.al. [11] gives a very useful method for extracting key points i.e. SIFT. This method is very popular on key point based approaches. The SIFT feature vectors are invariant. The two main part of his paper are SIFT key points detection and SIFT descriptor. Due to the Descriptor the key points are represented in a more described form. David Lowe proposed few steps for getting the invariant key points which are 1) Scale space extrema detection, 2) Key point localization, 3) Orientation assignment, and 4) Key point descriptor.

Jing and Shao also proposed image region duplication detection using local invariant features SIFT. And for matching purpose they use kd-tree and Best Bin First(BBF) algorithm. The detection method detects the tempered region with some post operations like JPEG compression, Gaussian blurring, rotation, scaling. The SIFT method fail to identify the forgery for smoothed areas. It can not extract features from these areas. [8]

Hashmia et.al. [6] uses a combined approach of Un-decimated Wavelet Transform and Scale Invariant Feature Transform. Dyadic Wavelet Transform (DyWT) performs better than Discrete Wavelet Transform (DWT), but it is not appropriate for down sampling in the image. Their algorithm has higher matching rate and most robust to the pre-processing [6].

Kang and Cheng proposed the detection method based on singular value decomposition and passive blind detection technique. The method obtains singular value block matrix, and correlation coefficients which helps to improve matching capabilities [9].

B. Mahadian et.al. [12] proposed a new method to identify copy–move including noise, contrast and blur forgeries and it also identify lossy JPEG format data.
V. Christlein et.al. gives an extension to copy-move forgery detection which deals with affine transformations. They proposed Same Affine Transformation Selection (SATS) wchich are invariant to outliers. [4]

Weihai Li. et.al. describe an efficient algorithm that uses Fourier-Mellin Transform for identification of copy-move forgery in digital images. They proposed vector erosion filter, the algorithm is robust to arbitrary rotating, slightly scaling, and JPEG compression. [10]

Hao-Chiang Hsu et.al. uses Gabor filter with rotation angle, frequency and scaling. [7] Seung-Jin Ryu et.al. proposed a technique which find rotation forgery using Zernike moments. [14] Irene Amerini et.al. presents SIFT based copy-move forgery detection technique. [1]. Another method is available for identifying copy-move forgery proposed by Resmi Sekhar et.al. [15]

Chapter 3

Copy-Move Forgery Detection in Digital Images

An image forgery is called as Copy-Move forgery when some content (region) of an image is copied and pasted within that same image. This is usually done in order to conceal some information of the image. There must be a possibility that one or more region is copied and moved into the image. Just because the duplicated portion or portions comes from the same image so that properties of the repeated region must be same as the original region so that the detection methods must be compatible with the statistical measures presents in each part of the images.

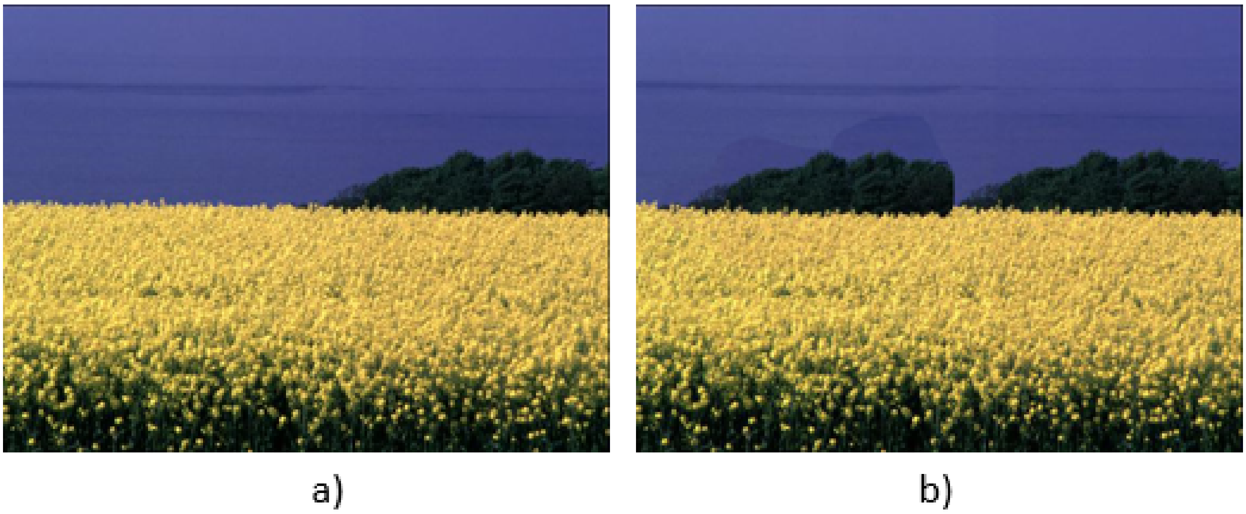

Figure 3.1: Copy-Move Forgery a) Original Image, b) Forged image

The image which is at the right side is forged image. presents an example of copy-move forgery in digital images. The image at the top is the original image and the bottom image is the forged image. In the bottom image the background foliage is copy-pasted on to another location of the same image, to generate its forged version.

3.1 Detection Based on Exact Block Matching

In exact block matching algorithm first we have to divide the image into non-overlapping blocks. After that we have to find the repeated blocks. There may be more than two blocks are copied as well as pasted into the image we have to display them. The approach is as follows :

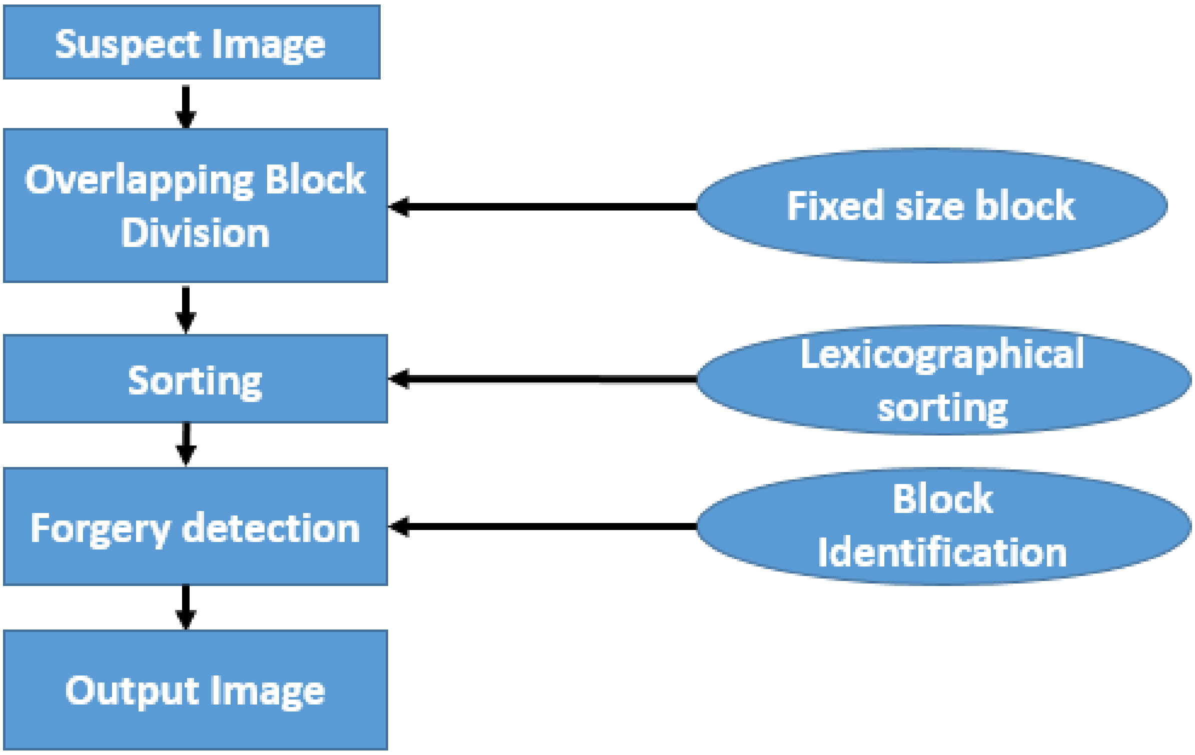

Figure 3.2: Detection Algorithm : Flow Chart

Method

According to the above architecture the whole detection framework is as follows :

1. Let the segment or the block size is $K \times K$ pixels.

2. The square block is moved pixel by pixel to cover the image from the upper left corner to right corner and top upper corner to down the lower right corner.

3. The pixel values of a block is stored into a 2D array.D

4. Each row of array D represents one block which is sliding over the image.

5. Lexicographical sorting is applied to sort the rows of maytrix D.

6. The sorting takes MNlog2(MN) time to computed.

7. The identical blocks are now shown into the image.

3.2 Implementation Details of Exact Block Matching

We are using MATLAB for our implementation purpose. In this algorithm the whole image (forged) is divided into overlapping fixed size blocks. Let us assume we have M*N grayscale image I, where M is number of rows and N is number of columns. If the image is color then convert it into grayscale by using I= rgb2gray(I). Now we first divide the image into B*B non-overlapping fixed size blocks, where B is the size of the block. If the size of the segment or block is minimum then it will give more accurate results. The square block is slid by one pixel from left to right, when one row is completed then the block moves to the next row. Now for each block position, all the pixel values of the block are extracted in row-wise manner into a 2-D matrix A. Each row of matrix A is dedicated for all pixel values of a block. So that the first row of A stores pixel values of first block, second row stores second block pixels values and so on. So that matrix A contains B2 columns and (M-B+1)*(N-B+1) rows.

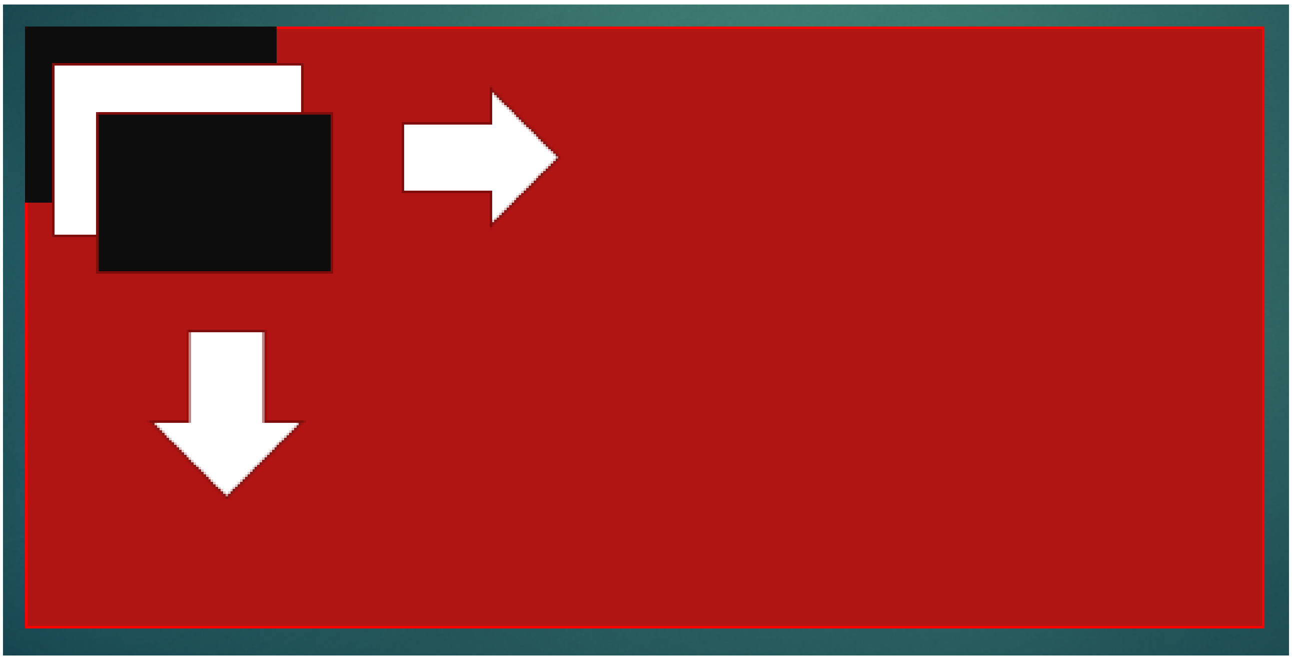

Figure 3.3: Exact Block Matching: Depicting how the image is divided into blocks

Once all the block are extracted then we have applied lexicographical sorting on matrix A, which sorts A in row-wise manner. We can also use radix sort in place of lexicographical sorting but the time complexity of lexicographical sorting is less than radix sort that is why we are using lexicographical sorting. After applying lexicographical sorting the similar rows of matrix A comes at consecutive locations. Similar rows depicts copied and moved blocks. At last we have to find the location of the original and forged blocks in the given image and output them.

We have taken one standard 512*512 image and performed forgery on that image and block size is 8*8. Because of that the total number of non over lapping blocks extracted are (512-8+1)*(512-8+1) = 255025. The size of matrix A is 255025 x 64. The result of the exact block matching is shown in Chapter 5.

3.3 Summary

The Exact block matching technique gives correct matching result but only when a copied region is simply pasted onto other location. If any type of transformation is applied by the attacker then this technique are not able to give desired results. So that we require other methods to identify such forgeries in Copy-Move attacks.

Chapter 4

Detection of Geometric Transformations in Copy-Move Forgery

Copy-move forgery or region duplication is the simplest and most common form of image forgery. When a region is copied from an image, then it might be goes through the geometric distortions. The existing region duplication detection methods are based on blocking matching technique, if any kind of transformation is applied into the moved region then the block matching techniques are unable to identify those type of forgeries. In this work we describe a new technique for region duplication detection. This starts by key-point based features like SIFT.

4.1 Detection of Image Region Duplication Using SIFT

Here we present a new detection approach which is based on SIFT. SIFT is local feature aspect of image, and it stands for Scale Invariant Feature Transform. The key-points extracted using SIFT are insensitive to any geometric transformations, so that it makes the matching procedure easier. We first extract the SIFT key-points of the suspect image. Once the key-points are extracted we divide the whole image into non- overlapping inspect blocks or segments. For each inspect block we are finding nearest match of that block into the image. For all the SIFT key-points present in the inspect block, we are finding nearest neighbor. With the help of matched key-points we can find the moved region, which is geometrically transformed by applying scaling and rotation.

The overall detection method is as follows :

- SIFT Features Extraction
- Key-points Matching and Pruning
- Region Transformation Detection
- Display the Original and Forged Region

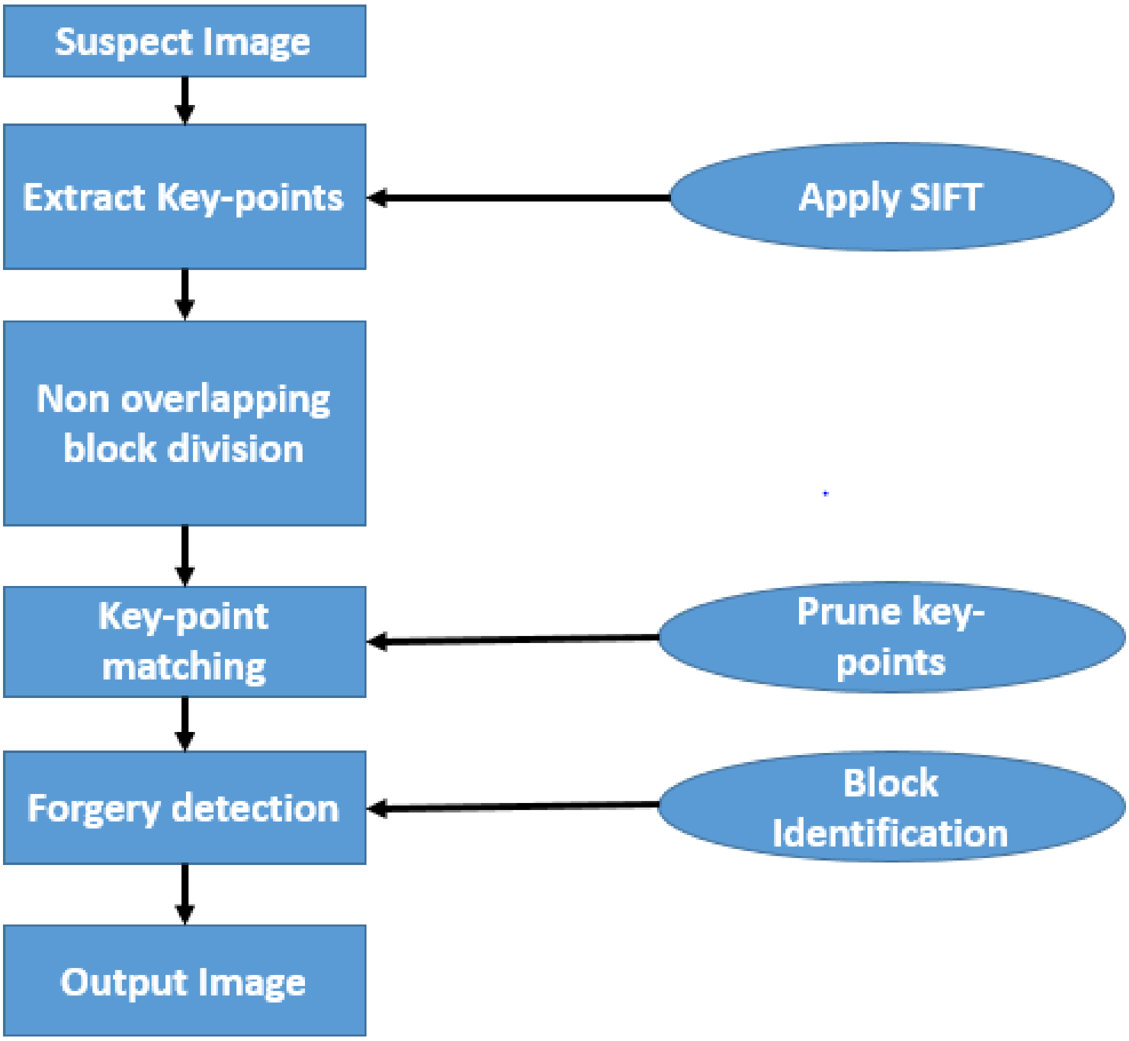

Figure 4.1: cloud architecture

4.1.1 SIFT Features Extraction

SIFT was proposed by Lowe [5]. The key-points extraction using SIFT technique itself consist few steps which are as follows :

a. Scale Space Extrema Detection :

In this stage we are identifying the position and scale of the points. The points which are same at different scales or in different views of the image are selected. Those points are invariant or more stable than the other points on different scales. For an image scale space is defined as $S(a, b, \sigma)$

$$S(a, b, \sigma) = F(a, b, \sigma) * A(a, b) \tag{4.1}$$

The scale space function is generated by convolution of Gaussian function and input image A. Where $F(a,b,\sigma)$ is Gaussian function defined as

$$F(a,b,\sigma) = \frac{1}{2\Pi\sigma^2} * \exp^{\frac{-(a^2+b^2)}{2\sigma^2}} \tag{4.2}$$

To make scale space more stable Lowe [11] apply difference of Gaussian in the scale space function.

$$D(a,b,\sigma) = (F(a,b,k\sigma) - F(a,b,\sigma)) * I(a,b)$$

$$D(a,b,\sigma) = S(a,b,k\sigma) - S(a,b,\sigma)$$

b. Local Extrema Detection :

From the Difference of Gaussian the points are selected if they are either maximum or minimum in their own 3*3 block and also from the 3*3 blocks of predecessor and successor DOG. In this process some noisy point are also extracted as a selective point. The elimination of noisy point and edges are done after that.

c. Orientation Assignment :

In this step local orientation are assign to each key-point. This provide local features to key-points. The orientation assignment provides rotation invariance to SIFT. For each scale space function gradient orientation m(a,b) and magnitude $\theta(a,b)$ are calculated.

$$m(a,b) = \sqrt{F_1^2 + F_2^2}$$

$$\theta(a,b) = \tan^{-1}(F_2/F_1)$$

where F_1=F(a+1,b,σ)-F(a-1,b,σ) and

F_2=F(a,b+1,σ)-F(a,b-1,σ)

The purpose behind key-point descriptor is to add more local information to the key-points. It adds 128 dimensional vector to each key-points. This 128 dimensional vector is created from all the orientation histogram and magnitude of the key-points.

4.1.2 Key-points Matching and Pruning

We are having two images original image and forged image. Let us take K1 and K2 such that
K1 = the key-points present in the inspect block in the original region
K2 = the key-points present in the moved block.
In this step for each SIFT feature points present in the original image, we are calculating the D distance between the 128 dimensional vectors of the key-points, with all the key points present into the forged image. The matching concept is that the key-points extracted in the original image must be extracted into the forged image. Only the duplicated region gives the difference in number of key-point which are extracted. The key-points of copied region and the moved region have some correlation between key-points, which helps to identify the forged portion. The key-points comes with SIFT are much noisy so we have to prune them. The pruning removes all the false matches so that only correct matched will remains.

4.1.3 Region Transformation Detection

Now we are finding the potential transformation between the original and forged block. In this work we are considering only copy-move forgery, scaling, rotation, both rotation and scaling forgery.

a. Copy-move region:

If the copied region is directly moved to any other location within the same image then key-points extracted in the original region and the key-points extracted in the moved region are must be same. The SIFT 128 feature vectors of each key-points are also same in both of the regions. And the distance D which we were calculated are also same for both original region as well as moved region. So that the forged region is easily be detected if there is no distortion has done.

b. Re-scaling:

If attacker scaled the duplicated region then D-distance plays most important role. The number of key-points available on original portion are differ from number of the key-points available on the forged region. All the SIFT key-points which are present at original region are not extracted into the forged portion. Although all the key points are not available so that the D-distance between pair of few key-points in the forged region must be multiple of their replicates presents in the original region.

$$D(\vec{a}, \vec{b}) = d1$$

$$D(\vec{a'}, \vec{b'}) = d1'$$

where($\vec{a}, \vec{b} \in K1$) and ($\vec{a'}, \vec{b'} \in K2$)

Where D is the Euclidean distance between 128 feature vector of the key-points and $(\vec{a}, \vec{b})$ are the key-point pair present in the original block and $(\vec{a'}, \vec{b'})$ are the key-point pair present in forged region.

$$\frac{||d1||}{||d1'||} = constant \tag{4.3}$$

We are plotting histogram of the ratios of D-distances comes from pair of SIFT key-points in K1 and K2. The maximum frequency of the histogram gives the scaling factor or the forged region.

c. Rotation

If the attacker rotates the copied region before it is being pasted then it is very difficult to identify the forgery. Although the SIFT key-points in K1 and K2 are nearly exact, but the position of the correspondences replicated key-points are changed. They are shifted to some angle. We can use mathematical rotation function to identify the forgery.

We estimate the transform between two or more local coordinate systems of the original and the duplicated region We pick three non-collinear keypoints from K1 and their correspondences in K2 that have the strongest matches. As rotation does not change these coordinates, we compute coordinates of each pixel location in K1. Their transformed correspondences are obtained by using the same set of coordinates in the coordinate system. Such that d1=d1'

d. Rotation and Re-scaling

Till now identification of the forged block is not so difficult because we are having only one type of forgery applied on the copied region. But in this case both rotation and scaling are performed in the forged blocks. The order of the forgery does not make any difference. The number of SIFT key-points extracted in the forged region only varies according to the scaling factor, rotation does not change the number of SIFT key-points extracted. Now in both type of geometric distortion the scaling is the dominating one. Rotation just give angle to the region. So the SIFT key-points of the forged region are having a constant ratio of D-distances same as scaling forgery.

$$D(\vec{a}, \vec{b}) = d1$$

$$D(\vec{a'}, \vec{b'}) = d1'$$

where($\vec{a}, \vec{b} \in K1$) and ($\vec{a'}, \vec{b'} \in K2$), such that

$$\frac{||d1||}{||d1'||} = constant$$

Due to rotation the relative distances of the key-points and the relative position are constant. d1=d1'

Again the maximum frequency of the histogram gives the scaling factor which is drawn from the D-distance ratios.

4.1.4 Display the Original and Forged Region

In this step the matching results are displayed. All the SIFT key-points present in the original image are also present in the forged image except for the moved block, so that we are getting lots of matched SIFT key-points. But to display only the copied-moved block we have to remove some inliers for that purpose we are using RANSAC method. The RANSAC removes the inliers of the image.

4.2 Summary

The SIFT key-points are invariant to geometric transformations ,which helps to detect geometric transformation in copy-move forgery. Due to this technique we can identify the transformations like copy-move, rotation, re-scaling, and both rotation and re-scaling in copy-move forgery.

Chapter 5

Simulation Results

All simulation was done in MATLAB R2014a. In this section we describe the results of our experiments. The implementation work is performed on MATLAB. Our test image is standard 512×512 Lena image. We have applied different types of forgeries on our test image. For example copy-move forgery, re-scaling, rotation, both re-scaling and rotation forgery.

5.1 Simulation Results of Copy-Move Forgery Detection Using Exact Block Matching

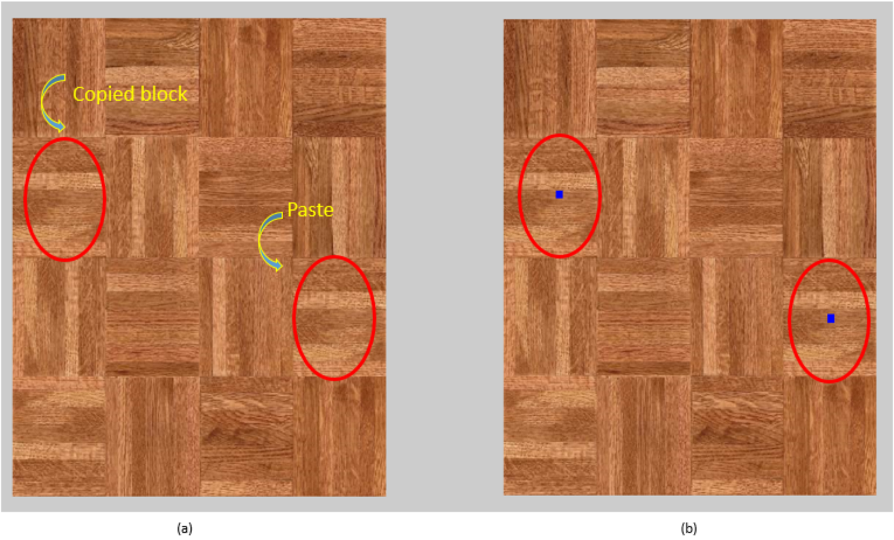

Figure 5.1: Exact Block Matching: (a) Tampered Image, (b) Output Image

In our experiment, we tampered images by copying and pasting one image block over another, in the same image. In our first method i.e exact block match, we took a 512×512 pixel image and 8×8 to be the smallest block size. We circularly shifted the image by one pixel each time and matched for the common region of minimal block size.

Figure 5.1 (a) is the forged image and Figure 5.1 (b) is output image. In this result we are identifying the block duplication for smallest 8×8 block.

In the second image the original image is shown in figure 5.2(a), the tampered image is shown in figure 5.2 (b) and the final output image of this method is shown in figure 5.2 (c). The image was then subdivided into$(512 - 8 + 1) \times (512 - 8 + 1)$ sub blocks off size 8×8 and stored in column order in an array. The array was then lexicographically sorted to find the adjacent matching blocks and the matching block was then mapped to the forged image to find the copy-moved segment. Figure 3.4.3(a) shows the original 512×512 image. Figure 3.4.3(b) shows the corrupted image and figure 3.4.3(c) is the output for this method.

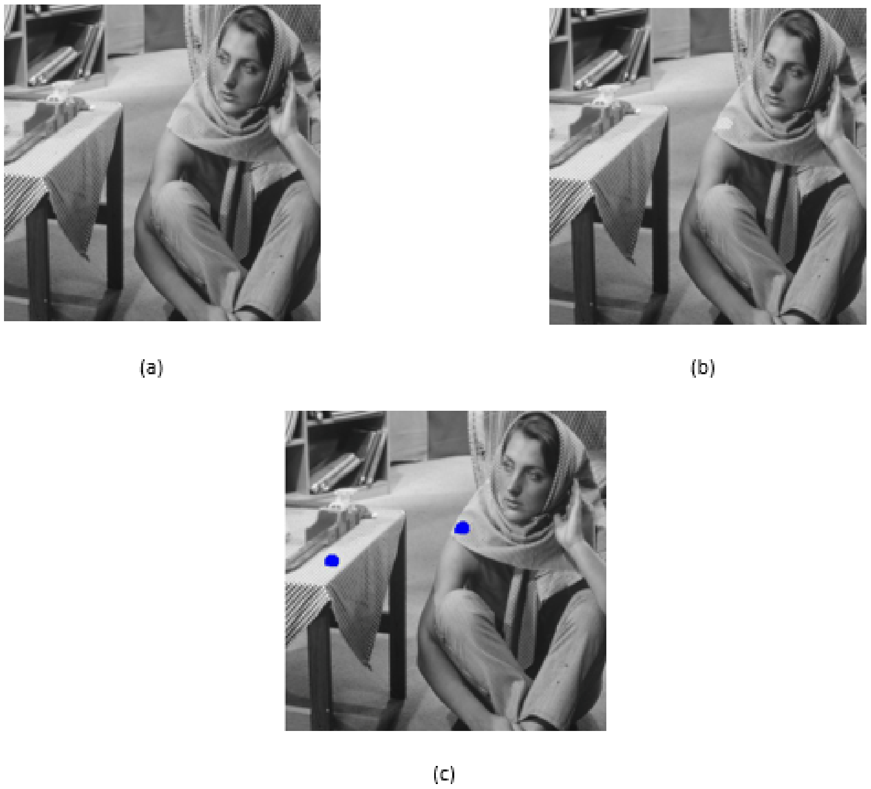

Figure 5.2: Exact Block Matching: (a) Original Image, (b) Tampered Image, (c) Output Image

5.2 Simulation Results of Geometric Transformations Detection in Copy-Move Forgery

This section contain outputs of detection of geometric distortions in copy-move forgery. The forgeries are rotation, re-scaling , direct copy-move and both rotation and re-scaling. Figure 5.3 is our test image. We have taken standard 512×512 Gray scale Lena image. All the geometric transformations are performed on this image. If the image is color image then first we have to convert it into gray image by using rgb2gray(image).

Figure 5.3: Test Image of size 512×512

Figure 5.4 depicts all the SIFT key-points extracted from different scales. All the key-points are invariant. Similarly we are extracting the SIFT key-points for the forged image also. Each SIFT key-points have 128 dimension feature vectors. These 128 dimensional vectors are comes from orientations an magnitudes of the key-points.

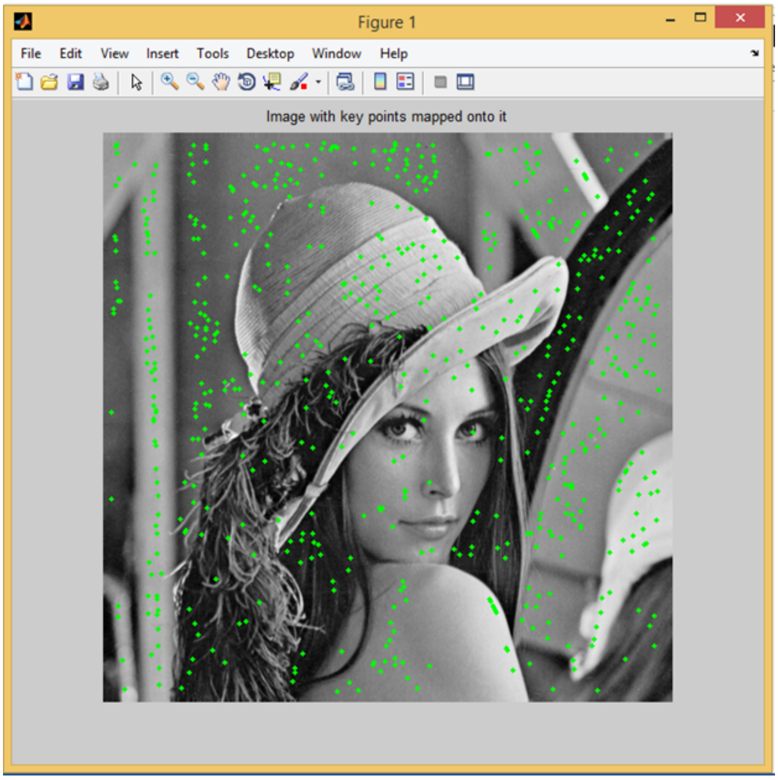
Figure 1
File Edit View Insert Tools Desktop Window Help
Image with key points mapped onto it

Figure 5.4: SIFT key-points mapped into the test image

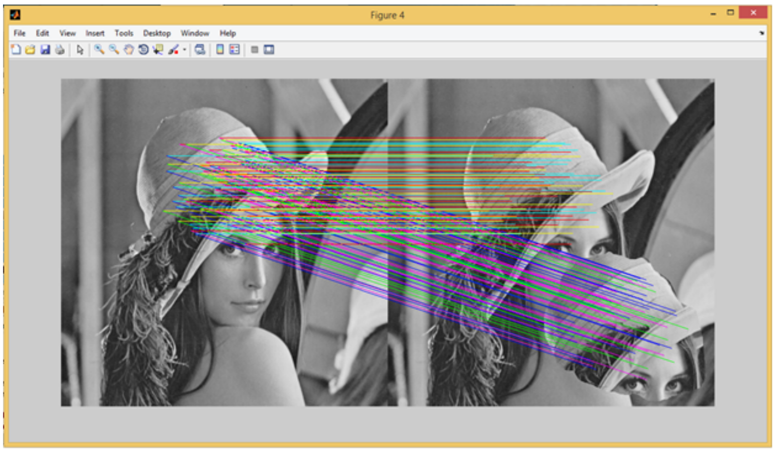

Figure 5.5: Detection of simple copy-move forgery

The direct copy-move forgery is depicted in Figure 5.5 . In this image we have copied a region and pasted into another location. The colorful line shows the matched original region and forged region in the image. The 128 feature vectors of the SIFT key-points in both regions must be same. In direct copy-move attack the duplicated region is directly pasted into another location without any distortions. When we are comparing the key-points according to their 128 dimensional feature vector, all key-points at both the regions having same 128 dimensional feature values.

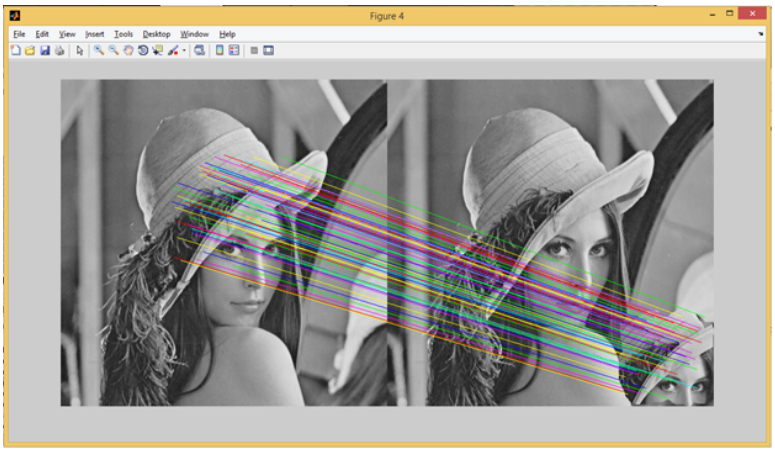

Figure 5.6: Detection of re-scaled duplicated image region

In Figure 5.6 we have applied re-scaling forgery. The copied portion is scaled and pasted to the bottom right corner. In this the matched lines shows the forged region. The SIFT key-points are selected from different scale spaces so that there are lots of key-points extracted,which makes the matching process easier. The number of key-points are differ in both original and forged region. Due to scaling copied block is reduced in size so that the number of key-points , magnitude are changed. That is the main reason why we are getting less number of key-points in the forged region.

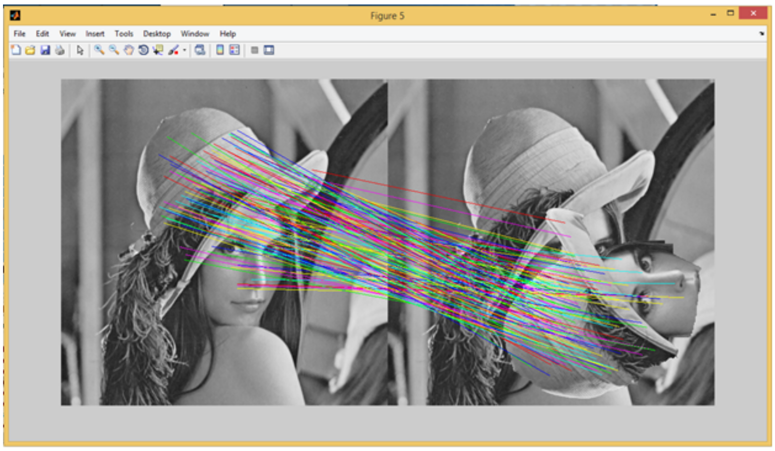

Figure 5.7: Detection of rotated, duplicated image region

Figure 5.7 identifies the rotation forgery applied in the copied region. The copied portion i.e. the small face part of the image is rotated and pasted to the bottom right of the image. In this type of forgery the number of SIFT key-points are same in both the regions, i.e. original region and forged region. The 128 feature vectors of the SIFT key-points are also get changed due to the rotation, because the orientations are changed.

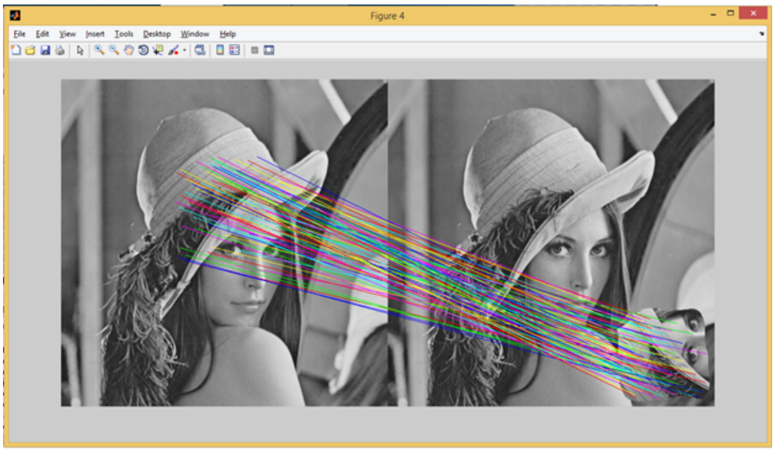

Figure 5.8: Detection of copy-move forgery with both rotation and re-scaling operations

In figure 5.8 we have taken a region and perform rotation and re-scaling on that region and that we have pasted it. The matching lines shows the mapping between original region and forged region. The re-scaling is the dominating factor in this forgery. Because rotation does not affect the number of SIFT key-points but re-scaling changes the number of key-points extracted.

All of the output shows that geometric transformations are correctly detected using the proposed method. In such type of forgeries for searching matched key-points is totally depends on SIFT key-points.

5.3 Summary

All the experimental results are shown in this Chapter depicts that the method proposed for detecting Geometric Transformations in copy-move forgery works efficiently with rotation, re-scaling and both rotation- scaling.

Chapter 6

Conclusion and Future Work

In this paper we have proposes an efficient method to detect copy-move forgery in digital images. The proposed method is also capable of detecting geometric transformations applied on the forged region, with the help of SIFT key-points. Our experimental results prove that the proposed method can detect a region duplication forgery, in which rescaling and rotation attacks are applied together or individually on the duplicated region. The proposed method is more effective and gives better performance than the exact block matching techniques, in terms of geometric attacks detection in region duplication. The future research direction includes identification of other forms of geometric attacks, relevant to copy-move forgery, such as reflection, as well as other image region transforms, such as gray level interpolation.

Bibliography

[1] Irene Amerini, Lamberto Ballan, Roberto Caldelli, Alberto Del Bimbo, and Giuseppe Serra. A sift-based forensic method for copy–move attack detection and transformation recovery. *Information Forensics and Security, IEEE Transactions on*, 6(3):1099–1110, 2011.

[2] Sevinc Bayram, Husrev T Sencar, and Nasir Memon. An efficient and robust method for detecting copy-move forgery. In *Acoustics, Speech and Signal Processing, 2009. ICASSP 2009. IEEE International Conference on*, pages 1053–1056. IEEE, 2009.

[3] Yanjun Cao, Tiegang Gao, Li Fan, and Qunting Yang. A robust detection algorithm for copy-move forgery in digital images. *Forensic science international*, 214(1):33–43, 2012.

[4] Vincent Christlein, Christian Riess, and Elli Angelopoulou. On rotation invariance in copy-move forgery detection. In *Information Forensics and Security (WIFS), 2010 IEEE International Workshop on*, pages 1–6. IEEE, 2010.

[5] A Jessica Fridrich, B David Soukal, and A Jan Lukáš. Detection of copy-move forgery in digital images. In *in Proceedings of Digital Forensic Research Workshop*. Citeseer, 2003.

[6] Mohammad Farukh Hashmi, Vijay Anand, and Avinas G Keskar. Copy-move image forgery detection using an efficient and robust method combining un-decimated wavelet transform and scale invariant feature transform. *AASRI Procedia*, 9:84–91, 2014.

[7] Hao-Chiang Hsu and Min-Shi Wang. Detection of copy-move forgery image using gabor descriptor. In *Anti-Counterfeiting, Security and Identification (ASID), 2012 International Conference on*, pages 1–4. IEEE, 2012.

[8] Li Jing and Chao Shao. Image copy-move forgery detecting based on local invariant feature. *Journal of Multimedia*, 7(1):90–97, 2012.

[9] Li Kang, Xiao-pin Cheng, K Li, and C Xiao-ping. Copy-move forgery detection in digital image. In *Proc of the 3rd International Congress on Image and Signal Processing.[S. l.]: IEEE Computer Society*, pages 2419–2421, 2010.

[10] Weihai Li and Nenghai Yu. Rotation robust detection of copy-move forgery. In *Image Processing (ICIP), 2010 17th IEEE International Conference on*, pages 2113–2116. IEEE, 2010.

[11] David G Lowe. Distinctive image features from scale-invariant keypoints. *International journal of computer vision*, 60(2):91–110, 2004.

[12] Babak Mahdian and Stanislav Saic. Detection of copy–move forgery using a method based on blur moment invariants. *Forensic science international*, 171(2):180–189, 2007.

[13] Xunyu Pan and Siwei Lyu. Detecting image region duplication using sift features. In *Acoustics Speech and Signal Processing (ICASSP), 2010 IEEE International Conference on*, pages 1706–1709. IEEE, 2010.

[14] Seung-Jin Ryu, Min-Jeong Lee, and Heung-Kyu Lee. Detection of copy-rotate-move forgery using zernike moments. In *Information Hiding*, pages 51–65. Springer, 2010.

[15] Resmi Sekhar et al. Recent block-based methods of copy-move forgery detection in digital images. *International Journal of Computer Applications*, 89(8):28–33, 2014.