FORENSIC ANALYSIS ON IMAGE TEMPERRING

Dissertation submitted in partial fulfilment of the requirements for the degree of

MASTER OF TECHNOLOGY

In

COMPUTER SCIENCE AND ENGINEERING

By

SONIA SHARMA

11506189

Supervisor

Kanwar Preet Singh

Assistant Professor

School of Computer Science and Engineering

Lovely Professional University

Phagwara, Punjab (India)

May 2017

LOVELY PROFESSIONAL UNIVERSITY
Transforming Education, Transforming India

TOPIC APPROVAL PERFORMA

School of Computer Science and Engineering

Program : P172::M.Tech. (Computer Science and Engineering) [Full Time]

COURSE CODE : CSE546 **REGULAR/BACKLOG :** Regular **GROUP NUMBER :** CSERGD0258

Supervisor Name : Kanwar Preet Singh **UID :** 15367 **Designation :** Assistant Professor

Qualification : _____ **Research Experience :** _____

SR.NO.	NAME OF STUDENT	REGISTRATION NO	BATCH	SECTION	CONTACT NUMBER
1	Sonia Sharma	11506189	2015	K1518	9780504462

SPECIALIZATION AREA : Programming-II **Supervisor Signature:** _____

PROPOSED TOPIC : Forensic Analysis on Image Tampering using Adaptive over-segmentation Technique.

Qualitative Assessment of Proposed Topic by PAC		
Sr.No.	**Parameter**	**Rating (out of 10)**
1	Project Novelty: Potential of the project to create new knowledge	7.75
2	Project Feasibility: Project can be timely carried out in-house with low-cost and available resources in the University by the students.	7.50
3	Project Academic Inputs: Project topic is relevant and makes extensive use of academic inputs in UG program and serves as a culminating effort for core study area of the degree program.	7.75
4	Project Supervision: Project supervisor's is technically competent to guide students, resolve any issues, and impart necessary skills.	7.75
5	Social Applicability: Project work intends to solve a practical problem.	7.50
6	Future Scope: Project has potential to become basis of future research work, publication or patent.	8.00

PAC Committee Members		
PAC Member 1 Name: Janpreet Singh	UID: 11266	Recommended (Y/N): Yes
PAC Member 2 Name: Harjeet Kaur	UID: 12427	Recommended (Y/N): Yes
PAC Member 3 Name: Sawal Tandon	UID: 14770	Recommended (Y/N): Yes
PAC Member 4 Name: Raj Karan Singh	UID: 14307	Recommended (Y/N): NA
DAA Nominee Name: Kanwar Preet Singh	UID: 15367	Recommended (Y/N): Yes

Final Topic Approved by PAC: Forensic Analysis on Data Tampering(Remarks: Narrow down Topic)

Overall Remarks: Approved (with minor changes)

PAC CHAIRPERSON Name: 11011::Dr. Rajeev Sobti **Approval Date:** 26 Oct 2016

ABSTRACT

Today images are utilized nearly as a part of the considerable number of utilizations, for example, climate determining, remote detecting, news coverage, internet business and so forth. Image can be effectively tempered or produced by utilizing software, for example, Photoshop, Pi-casa, photograph supervisor and so on. This present any software are utilized to alter the color, contrast, brightness of an Image. hence images are not quite the same as the unique image. Image forgeries is essentially stowing away or expelling some significant or valuable data about images. We can't identify the manufactured image by simply taking a glance at the Image. Acknowledgment of controlled image from genuine image is hard. Scientific image examination is the way toward identifying manufactured image by utilizing a few strategies. the genuineness and uprightness of images must be existing. In this work, we will discuss about the process of image tempering, image tempering techniques, forensic image analysis, tools and techniques used in forensic analysis, algorithm used for detecting forged or manipulated image and comparison among the various techniques.

DECLARATION

I hereby declare that the research work reported in the dissertation entitled **"FORENSIC ANALYSIS ON IMAGE TEMPERING"** in partial fulfilment of the requirement for the award of Degree for Master of Technology in Computer Science and Engineering at Lovely Professional University, Phagwara, Punjab is an authentic work carried out under supervision of my research supervisor **Assistant Professor Kanwar Preet Singh**. I have not submitted this work elsewhere for any degree or diploma.

I understand that the work presented herewith is in direct compliance with Lovely Professional University's Policy on plagiarism, intellectual property rights, and highest standards of moral and ethical conduct. Therefore, to the best of my knowledge, the content of this dissertation represents authentic and honest research effort conducted, in its entirety, by me. I am fully responsible for the contents of my dissertation work.

Signature of candidate

Sonia Sharma

11506189

CERTIFICATE

This is to certify that the work reported in the MTech Dissertation entitled **"FORENSIC ANALYSIS ON IMAGE TEMPERING"**, submitted by **Sonia Sharma** at Lovely Professional University, Phagwara, India is a bonafide record of her original work carried out under my supervision. This work has not been submitted elsewhere for any other degree.

Signature of Supervisor

KANWAR PREET SINGH

Date:

Counter Signed by:

1) Concerned HOD:

HoD's Signature: _____

HoD Name: _____

Date: _____

2) Neutral Examiners:

External Examiner

Signature: _____

Name: _____

Affiliation: _____

Date: _____

Internal Examiner

Signature: _____

Name: _____

Date: _____

ACKNOWLEDGEMENT

The satisfaction that accompanies the successful completion of any task would be incomplete without the mention of people who made it possible and whose constant guidance crowned our efforts with success.

I sincerely express our deep gratitude to the management of our college for giving us liberty to choose and to work on the most relevant project i.e. "**Forensic Analysis on Image Tempering**". I am thankful to Dalwinder Singh (HOD, CSE DEPT.) for ensuring that we have a smooth environment in the university by providing us with the best suitable mentors according to our field. I would also like to thank the research and development department (R&D department).

I would like to thank my guide Assistant Professor Kanwar Preet Singh, Assistant Professor, CSE Department, who encouraged and insisted in the formulation of problem definition and without his valuable guidance and constant inspiration it would have been difficult us to prepare this report.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

TABLES **PAGE NO**

CHECKLIST FOR DISSERTATION-III SUPERVISOR

Name: _____ UID: _____ Domain: _____
Registration No: _____Name of student: _____

Title of Dissertation:

_____

☐ Front pages are as per the format.

☐ Topic on the PAC form and title page are same.

☐ Front page numbers are in roman and for report, it is like 1, 2, 3…….

☐ TOC, List of Figures, etc. are matching with the actual page numbers in the report.

☐ Font, Font Size, Margins, line Spacing, Alignment, etc. are as per the guidelines.

☐ Color prints are used for images and implementation snapshots.

☐ Captions and citations are provided for all the figures, tables etc. and are numbered and center aligned.

☐ All the equations used in the report are numbered.

☐ Citations are provided for all the references.

☐ Objectives are clearly defined.

☐ Minimum total number of pages of report is 50.

☐ Minimum references in report are 30.

Here by, I declare that I had verified the above-mentioned points in the final dissertation report.

Signature of Supervisor with UI

CHAPTER 1
INTRODUCTION

Today images are used almost in all the applications such as medicine, weather forecasting, remote sensing, journalism, e- commerce etc. Image can be easily tempered or forged by using software such as Photoshop, Pi-casa, photo editor etc. This software's can be used to change the color, brightness, and contrast of an image. This makes image different from original image. Image forgery is basically hiding or removing some meaningful or useful information about images. We cannot detect the forged image by just looking at the image. Recognition of manipulated image from real image is very hard. Forensic image analysis is the process of detecting forged image by using some tools and techniques. We need to find the authenticity and integrity of images. Our main focus is to discuss about the process of image tempering, image tempering techniques, forensic image analysis, tools and techniques used in forensic analysis, and algorithm used for detecting forged or manipulated Image. Image and videos are the main information carrier in today's world. There are numerous effective devices which can be utilized for altering and controlling images. Images can be controlled in faultlessness that fraud can't be recognized seemingly. Image giving is considered as including or expelling a few components from image without leaving evident follows. So, it is considered as intentional manipulation. Image can be tempered by many ways such as cloning process, image splicing, image retouching, resampling etc. Researchers have classified these image forensic tools into five categories: -

i. Pixel-based approach that works at pixel level.
ii. Format-based approach that are based on image formats and used primarily for JPEG format.
iii. Camera-based image forgery approach is used through capturing image using any kind of digital camera.
iv. Physically-based approach helps to detect differences in 3-D communication among physical substances, light and the camera.

v. Geometric based approach takes extent of objects present in the world and the object of position related to the camera [3].

Forensic image analysis is the utilization of science and domain mastery to translate the element of image in legitimate way. The principal objective of forensic image analysis is to appearance at the progressions performed over the images. Forensic image analysis performs its work in three ways: Image Interpretation, Image Examination, and Technical Preparation. Image interpretation is the application of examining the subject matter of the images and to draw some conclusion about the subject matter. Example: attainment inference about the state of nose. Image examination is the utilization of image knowledge for removing data from images. Example: image alteration evaluation. Technical preparation deals with finding out the performance of tasks such as interpretation or output. Forgery detection is to detect the image is tempered or not. In forensic science, we have many Techniques and algorithm to detect the forgeries created on the images.

1.1 PROCESS OF FORENSIC IMAGE ANALYSIS

We have few steps used which are performed in forensic image analysis to detect that image is tempered or not.

i. Input an image
ii. Preprocessing on the tempered image
iii. Selection and extraction of various features
iv. Perform forensic image analysis
v. Output will define image is tempered or not

First step of forensic image analysis is to input an image to verify the authenticity of image. Then next step is to process the image known as preprocessing. it enhances the quality of an image and find the inferring data. The next step is feature selection and extraction. It consists with extracting the meaningful or useful information from the image. After that forensic image analysis process is performed. It finds the authenticity and validity of image by

using various tools and techniques. The last step is the output. It consists with image and data.

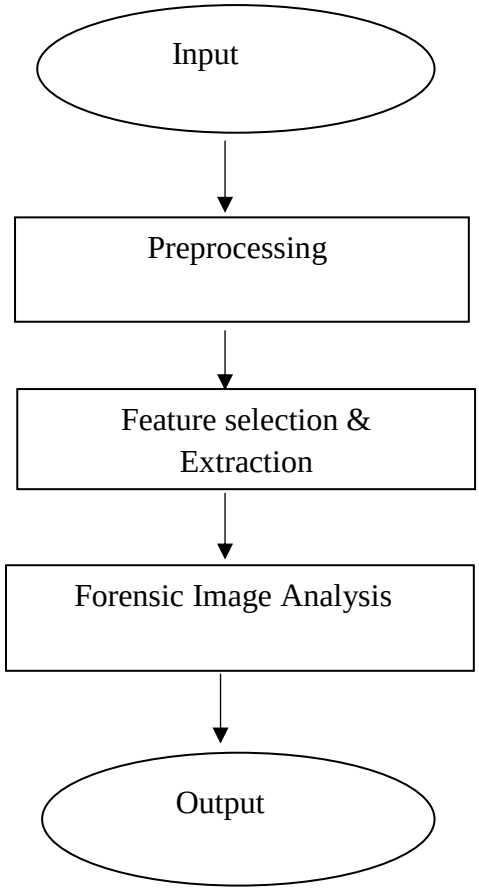

Figure 1.1: Steps of Forensic Analysis

1.1.1PRE-PROCESSING

After the development of Image detecting, preprocessing is done on the image for conveying the image in appropriate form for additional investigation. Preprocessing is typically performed at the pixel level, may equally be reached out to semantic level to copy the human vision or to find the information which uncommonly individual will most likely be unable to dispersed as a result of visual disablements. Such sort of preprocessing incorporates following things: threshhold to decline grayscale or shading image to binary noise is decreased to

diminish unnecessary information, segmentation is prearranged to unmistakable different segments exhibit in the image, and, in conclusion, limit discovery is utilized to permit less demanding resulting recognition of relevant components and things of interest to the editor.

1.1.1 FEATURE EXTRACTION

Feature extraction is the way toward separating the significant data or valuable data from the images. The components removed from the entire image is called global features and the elements. These elements are separated from the part of the image is called local features. These components are utilized to strengthen to the procedure used to measure for the process of image investigation in the events of interpretation, examination and technical preparation. The procedure of dimensionality reducing diminishes the capacity and handling time. There can be a few classes of elements: textural, geometric, fragment, structural and content based. The extractions of global and local components are given as contribution to image examination process or technique. The benefit of feature extraction is that it lowers the data when compared with original image to represent the image for grasping the element of the images.

1.1.2 FORENSIC IMAGE ANALYSIS

Forensic image analysis is the way toward recognizing the tempered image by utilizing different strategies or devices. It is a massive rule that any confirmation that should be introduced in court must be interested in investigation and be testable. It decides the legitimacy of unique image. The processing is performed on the image for the improvement of image or for any other reason. The portion of image where images can be altered by utilizing any kind of software, for example, some algorithm calculations are moderately confusing and the outcomes might be quick-tempered to alterations in the application. Images that has been generally processed by utilizing programming could be all around tested in court. forensic Image Analysis tries to give inductive and deductive rationale however Mathematical information, Pattern investigation, Physical properties, Chemical properties, Morphological (basic) properties, Biological properties.

1.2 IMAGE TEMPERING

Image tempering is the process of changing the original images. The image can be any kind of digital images. Images are stored in the computer system in the form of grid of picture elements also called pixels. The pixels of image contain all the information about the color of image or brightness information. Image editor can change the pixels to enhance or to alter the image. The pixels can be changed individually or in the form of group by using some kind of algorithm by image editor. Traditional analog image editing is also known as photo retouching using tools such as airbrush to modify photos.

Figure 1.2: Image Blurness

In this picture, it is shown that image is tempered by the process of Gaussian bluer. The are several other methods to temper the images. the methods are increasing decreasing size of image called scaling, changing the contrast or brightness of image, changing color or shape of image. There are also several other methods which will be discussed.

1.3 METHOD TO TEMPER IMAGE

1.3.1 AUTOMATIC IMAGE ENHANCEMENT

There can be different tools such as camera or any kind of computer editing tools that provide automatic image enhancement that changes color or brightness as well as other image editing features such as removing red eye, sharpness adjustment, zooming features and automatic cropping. They all can

perform changes without human interaction, with just one clicks of button or mouse button or by selecting option from the menu list hence called automatic.

1.3.2 DIGITAL DATA COMPRESSION

Compression is performed on different kinds of file formats to reduce the size of file and hence save storage space. Compression can take place in camera or in computer system by the image editor. If images are stored in JPEG format, it means compression has already taken place. The compression can be performed in different levels. Compression can be lossy or lossless compression. In Lossless compression, no information is lost. E.g.- PNG File format. In lossy compression, information is lost, hence reduce quality or content that can be restored. E.g.- JPEG file format.

1.3.3 IMAGE SIZE ALTERATION

The images can be resized by the image editor, called scaling. The resizing consists with increasing or decreasing the size of image. The result is images becomes larger or smaller than the original image. High resolution cameras can produce large images that can be reduced for internet use. Image editor use mathematical process called resampling to calculate the new pixel value whose space is larger or smaller than the original image.

1.3.4 CROPPING AN IMAGE

The images are cropped using digital editors. The process of cropping can be performed by selecting any rectangular portion from the image being cropped. Likewise, we can remove the unwanted part of image. It doesn't affect the resolution of part of image being cropped. If original image has high resolution then good result can be obtained while cropping the image. We can also remove unwanted part of image by using clone tool. Removing distraction elements from the image allow us to focus on the subject of image.

Figure 1.3: (a) Uncropped Image, (b) Lily cropped image from the original image

1.3.5 CUTTING OUT PART OF IMAGE FROM BACKGROUND:

The outline of picture can be selected and background is removed by using selection tool. Based on the edge, it may be more or less difficult to do it properly.

HISTOGRAM:

The histogram can be created of image being edited. Histogram plots the number of pixels called vertical axis with brightness value called horizontal axis. Algorithm are used by digital editor to adjust brightness value of pixels and display the result of image. Thereby improve the quality in terms of brightness and contrast.

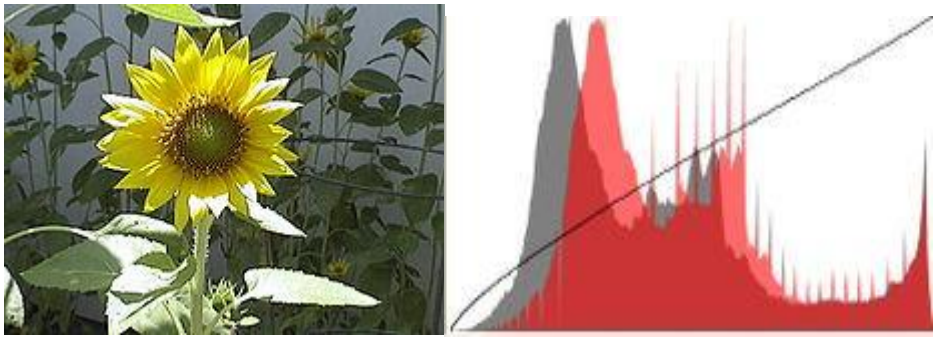

Figure 1.4 (a) Sunflower image, (b) Histogram of sunflower image

1.3.6 NOISE REDUCTION

There are number of algorithms used by image editor to add or remove noise in an image e.g. JPEG artifacts can be removed, dust and scratches can be removed etc. the more noise reduction can lead to loss of detail. Noise tends to invade images when the images are taken in low light setting.

1.3.6 COLOR CHANGE

The color of images can be changed to alter the images. the editor can also change the color of selective part of image. The images can be converted into grey scale images that consist with two color images that are grey and black.

1.3.7 IMAGE ORIENTATION

Image editors can change the orientation of image in which editor can the rotate the image in any angle and to any degree. Mirror images can be generated of the original image. Mirror images are reflected duplicate of image that look identical to original image. Images can be flipped horizontally or vertically. After rotating image, we need to perform cropping to remove

Figure 1.5: Image positioning: left to right, real image, -30-degree rotations, reversed

1.3.9 CONTRAST CHANGE AND BRIGHTENING

Image editor can change the contrast and brightness of image, hence can dark or brighten the image. The recent advancement allows us to change the brightness of pixels below a particular threshhold. Therefore, we can brightness of one part of image without effecting rest of the image. The transformation that are applied to color of image depends on editor to editor.

figure 1.6: Contrast Transformation, left side of Image is untouched

1.4 TEMPER DETECTION TECHNIQUES

There are different strategies for matching images and these can be arranged into three general classes. Copy-move attack, also called Cloning, is a strategy in which as opposed to having an outer image as the source, it utilizes segment of the Original base image as its source. In this way, the source and the goal of the transformed originate from a start Image.

The second category of image tempering systems is known as Image-Splicing, which is a procedure that includes a composite of at least two images which are joined to make a false image and the third classification of image tempering strategy is known as Image Retouching in which certain elements of image are being upgraded or diminished keeping in mind the end goal to make the image more fascinating. This kind of forgery is viewed as less harmful and is utilized for the most part by the editorial manager

The authenticity of image security is an intense issue and it is developing day by day. There are many techniques used to validate the authenticity of images. These techniques are generally divided into two categories. Intrusive (active) and non-intrusive (passive) technique:

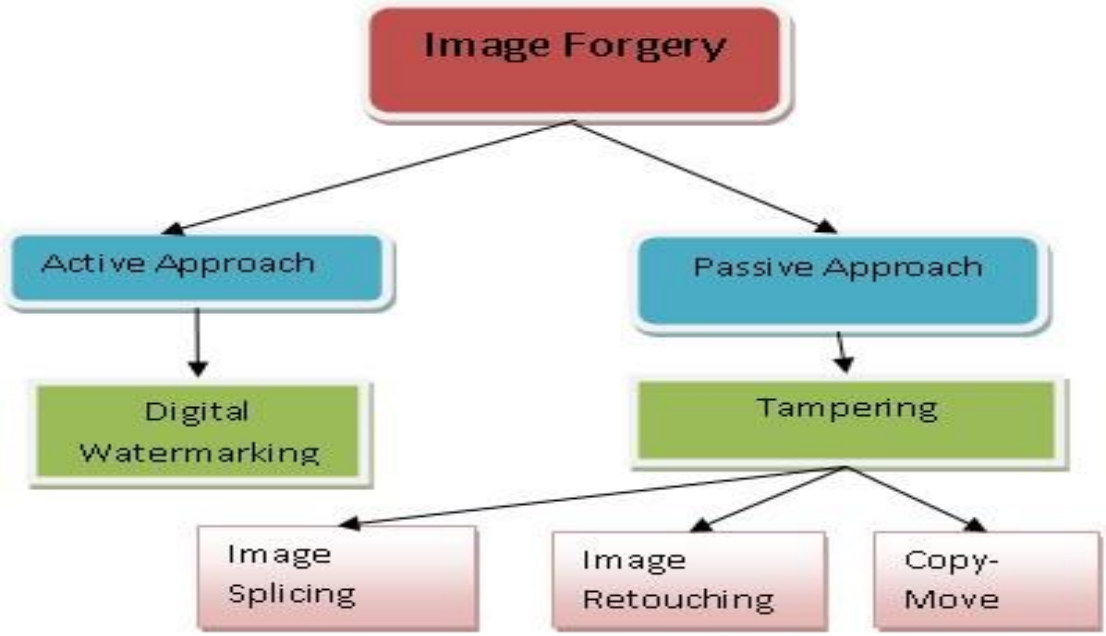

figure 1.7: Classification of Image Forgery

1.4.1 ACTIVE APPROACH

In this approach image require some kind of preprocessing such as watermark embedded or signature are generating while crating image. It provides security to the image. It consists with the two techniques of providing security to the image.

a) WATERMARK

It is a method of active temper detection. In this method, security structure is embedded into image. Watermark technique is of two types. Watermark can be visible or invisible watermark. Visible watermark is addition of concept of logos. Invisible watermark is conceited in the content. The limitation of watermarking technique is most of the devices do not contain this feature. Watermarking was the default method to provide protection which legally provides integrity and authentication.

b) SIGNATURE

It is another method of active temper detection in which signature are used for the security purpose of images. Today with the advancement of technology biometric is used to verify the signature placed on the image.

1.4.2 PASSIVE APPROACH

This procedure is otherwise called blind approach. This strategy is a tremendous challenge in image processing systems. It manages investigating the tempered image in view of different insights and semantics of image substance to restrict treating of image. Thus, this technique likewise called raw image investigation. Detached image crime scene investigation is typically an extraordinary test in image processing procedures. The stream of image altering identification manages breaking down the tempered image in light of different measurements and semantics of image element to restrict altering of image. Neither build is implanted in the image and nor connected with it for security, as like active methodologies. Aloof procedures depend on the suspicion that despite the fact that altering may not leave any visual follow but rather they are probably going to change the hidden insights. Passive strategies are further named dependent and independent forgery detect method and forgery free strategies. Forgery ward recognition strategies are considered to identify just certain kind of forgeries, for example, copy-move and splicing. The principle target of passive detection strategy is to distinguish a given image as unique or altered image.

a) COPY MOVE FORGERY

This is a method of treating image by duplicating the portion of image and pasting onto a similar image or different image. By duplicating and sticking image onto the produced image it hides the essential data of the image. This imitation is exceptionally hard to identify. Copy move is a one of the widespread amongst the broad cast image altering method, likewise it is extremely hard to recognize this type of forgery as the replicated image is taken from a similar image. copy move forgery is typically done to either covering some part of the image to validate some part of the image in different conditions. The objective of Copy-move forgery identification is recognizing the comparative zones. Numerous techniques have been proposed to take care of this issue. These recognition strategies are comprehensively categorized into two classes: block matching and point matching based. While making a Copy-move forgery, it is frequently

important to include or expel essential elements from a image. To complete such forensic analysis, different technology instruments have been introduced.

b) **IMAGE SPLICING**

Image splicing forgery includes joining of at least two images and change the original image. Splicing detection is worrying issue where composite regions are investigated by variety of strategy. Fast changes in various areas that are combined and their experience give profitable traces to identify splicing in the image. If there is different occurrence of images with contrasting foundation are joined and it turns out to be exceptionally hard to make the borders and boundaries invisible.

c) **RETOUCHING**

This procedure does less alteration on the image. It just upgrades a few components. Modifying may require scaling, turn and so on. retouching is organized into two classifications. Technical retouching and creative retouching. The detection is difficult as there is no radical change in various portion of image [11]. "In Image Retouching, the images are less adjusted. It just improves a few elements of the image. One traditional sight on retouching is that it is dependably a changing the truth, and that a retouched image is not a "photo" in the genuine sense of the word.

d) LIGHTNING CONDITION

This kind of forgery can be effortlessly done by joining two different images together. E.g. it is extraordinarily basic when two stars are demonstrated impractically included. Both performing artists are from various scene and distinctive lightning condition and it is difficult for forger to organize correct lightning state of each other. Such variety in lighting conditions can be utilized to recognize the treating in the image. As the merged tempered images are from various lighting conditions, the lightning state of joined photo won't not manage. This lighting irregularity in the combined image can be utilized for the recognizable of image altering.

Table 1.1: Comparison of various techniques

Image tamper technique	**Image operations/tools used**	**Tamper detection techniques**
copy-move	copy, move,	paste, selection
Exhaustive search, Block matching	(using DCT or PCA),	Autocorrelation
image-splicing	copy, resize, move,	paste, selection
Bi spectral analysis, Bi coherence	analysis, Noise variation estimation,	Alpha variance estimation,
Higher order statistics	Re-sampling resize, crop, rotate,	scale, skew, stretch

1.5 EFFECT OF TAMPERING IN DIFFERENT AREAS OF SOCIETY

Altering is regularly done to cover questions in an image with a specific end goal to either deliver false confirmation or to make the image more attractive for appearance.

In the field of medicine, reports of patients are greatly classified and are constantly expected to be reliable. Medicinal images are created in the majority of the cases as confirmation for unhealthiness and claim of sickness. Since medicinal images are managing large measures of cash, individuals can get cheated to alter images for declaring beneficial protection. Likewise, medicinal outcomes are for the most part set as evidences or choices for staying away from disciplines in courts.

In the field of education, distinctive altering methods give us incorrect data which in blows stimuli to the transport of off base information to the association. Understudies completed huge measure of fake with their records for their own particular advantage. This bothers the security of the administration which is an insistent issue to be understood.

In the field of agriculture, altering is likewise finished with the varied images utilized among the preparation of the farmers which results to the misguidance to the agricultural understudies. This sort of falsification irregularity the security administration which is to be explain soon.

In the field of e-commerce, the majority of the exchanges are helped out through web whether it is cash exchange, Shopping reason, charge installment and so forth. In this, Security of the client's points of interest is the prime concentration of the administration. However, numerous unapproved clients control the information which carries about genuine crime. This polluted or bothered security administration prompts to genuine wrongdoing. Thus, in the period of computerized innovation, altering is an important danger to the innovation which requires quick consideration.

1.6 ADAPTIVE SEGMENTATION AND FEATURE MATCHING

Adaptive segmentation and feature matching is the technique used to detect forgeries in the images. the most common type of forgery is copy-move forgery. This technique is very useful for the forgeries like scaling, rotation, and cute paste forgery.

The technique adaptive segmentation divides the main image into non-overlapping and asymmetrical blocks adaptively. Then features are mined from each block of image that are called block features. After extracting those features from each block of image, these features are matched with one another to locate the feature point. This way it detects the forgery contained within image.

To detect the more precise forgery region of image, the forgery area removal algorithm is proposed that substitutes the feature point through small super pixel called block feature, then combine the neighboring blocks with comparable local

color feature to feature block to produce merged region and then apply morphological operation into merged region to detect forgery region.

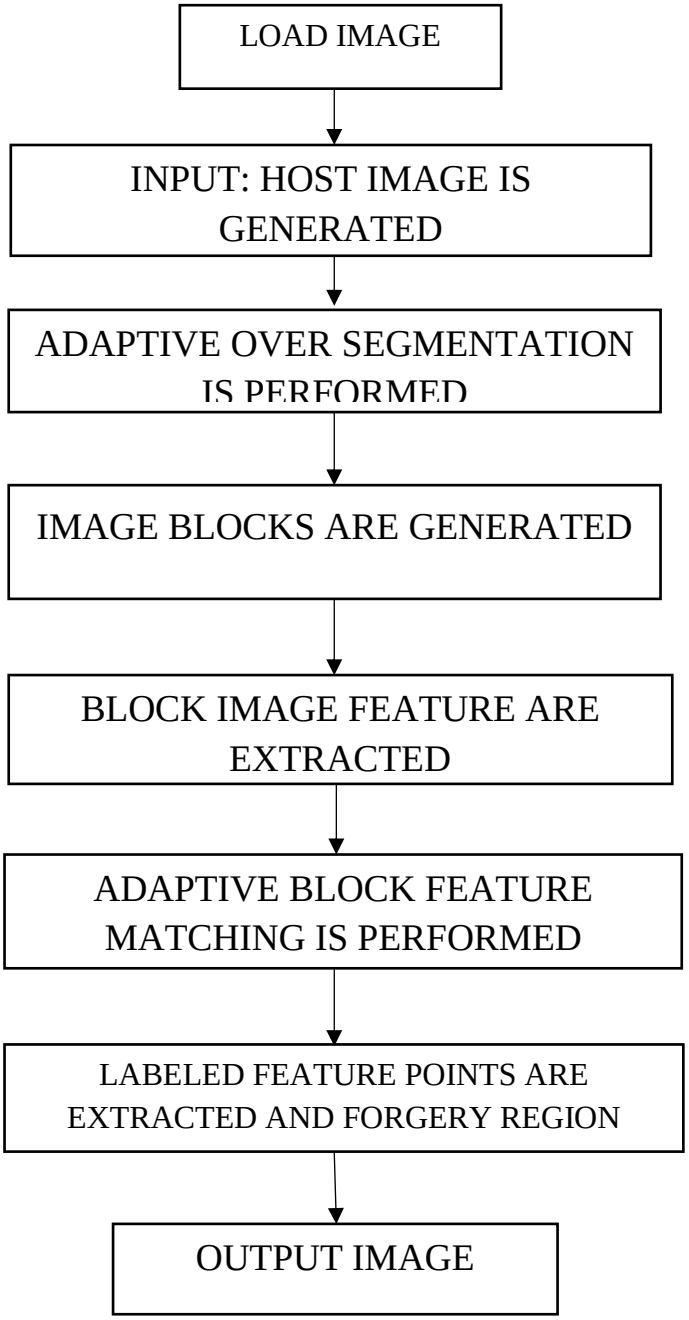

Figure 1.8: Adaptive Image Segmentation Framework of Adaptive Segmentation and Feature Matching Technique

The process of this technique is divided mainly into three steps:

1. Image segmentation
2. Feature detection and extraction
3. Feature matching

1. ADAPTIVE SEGMENTATION

Image segmentation is the process of dividing the image into multi segments which contain set of pixels contain called super pixels. Using this technique, the image is divide into various non-overlapping and irregular blocks adaptively. The goal of dividing large image into multiple blocks is to make the representation of image more meaningful so that it can be more useful and becomes easier to analyze. When the size of image increases, the matching process becomes more expensive hence adaptive segmentation is used which decreases the computational expenses. for most of cases unequal and expressive region represents forgery area much improved than consistent blocks. The existing algorithm use various techniques for forgery detection such as DCT, PCA, DWT, SVD. The most common technique used for image segmentation is SLIC known as simple linear iterative clustering algorithm. It adjusts k means clustering method to generate super pixels efficiently.

2. FEATURE DETECTION AND EXTRACTION

After dividing image into various non-overlapping blocks, then the features mined from each and every block hence called block features. The feature mined from image must be robust to the various distortions like scaling, rotation etc. Feature points are the points that invariant under some changes like zooming the image, lightning condition etc. features are the interesting part of image and it act as starting point for the various algorithm to detect forgery. The types of feature include edges, corners or interest point etc. Feature detection process consist with examining the feature in each pixel of the image. If the algorithm used for feature

extraction is good then it takes less time to extract feature by examine certain region. Feature detector is used to detect the features. The technique which are used to extract features are SURF and SIFT. SIFT is applied to extract feature point which are then matched with each other. After the value of shift vector increased more than the threshhold then multiple corresponding SIFT features describes forgery region. SURF is applied to extract image feature instead of SIFT. Though this method cannot detect forgery region very well hence do not produce satisfactory result.

3. BLOCK FEATURE MATCHING

Blocks are matched according to matching threshhold. Matched feature points indicate the forgery region. The block feature is first loaded, then we can find correlation coefficient of image block. Then threshhold is calculated and matched.

Table 1.2: Comparison of Various Techniques

FEATURE DETECTION TECHNIQUE	ADVANTAGES	DISADVANTAGES
DCT, PCA, SWD, DWT (block matching)	• Existing techniques used to detect forgeries • These techniques are used to detect copy move forgery	• These techniques do not provide geometric transformation such as scaling, rotation etc. • It uses less feature to represent each block.
SIFT (key point matching)	• It detects duplicated region with continuous rotation region • It is used for key point matching • It is also used for duplicated and distorted region. • It provides guarantee about geometric invariance.	• SIFT may fail to detect forgery in smooth background
SURF (key point matching)	• 1.SURF is an alternative technique to detect forgery. • SURF is more robust and can be variant to rotation. • SURF is faster than SIFT. • SURF +FMT can be used for flat or non-flat region.	• Recall rate is low • Most of this technique cannot detect some forgery region hence do not provide satisfactory result. •SURF is not faster as SIFT.

CHAPTER 2

LITERATURE REVIEW

E. V. J. A. Karthick, "Forensic Technique for Detecting Tamper in Digital Image Compression," vol. 2, no. 3, 2013, In this paper, primary concentration is performed on image altering at time of compression images. Since the vast majority of the adjustments in images are done at the compression of images. Images are tempered by altering DCT and DWT coefficient. Forensic practices are created to separate these coefficients. The Wavelet transformation of the images comprise to breaking down the image into various segments. After that review, every part with purpose corresponding to its scale. SPHIT is a compression strategy which depends on the wavelet transform and identifies the treating amid image compression in view based on the type of histogram. For the validation of image verification, and altering location, number of scientific procedures have been created. The purpose of digital image forensic investigation is to discover the validness of images by recovering data about their history. Digital Image Forensics is the branch of multimedia security and sound security, combined with Digital Watermarking, gives at contrasting and effective image manipulation. In this paper, they have proposed a set of forensic operations used to find compression fingerprints from digital images.

.

D. P. Patil, "Forensic Technique for Detecting Image Tampering using Statistical Intrinsic Fingerprints- A Survey," vol. 920, no. 3, pp. 919–920, 2014, This paper analyses the approaches for distinctive contrast improvement and copy & move forgery by identifying elements for every operation of intrinsic fingerprint. The paper determines numerous strategies to distinguish contrast enhancement globally or locally, detect histogram, resizing and editing of images and noise. The computerized images are becoming to be particularly important part in the field of data crime scene investigation and security, on account of the forgery of image altering instruments, advanced images can be effectively modified. Consequently, it is important to make legal strategies which ought to be fit for distinguishing altering in image. There are

number of strategies to distinguish distortion in image, each of which accompanies a few satisfactory circumstances and weaknesses. We concentrated few of them in this paper. The methods talked about above are helpful for identifying cut and glue sort forgeries. This paper does a wide study on the procedure to identify copy move forgery that is replicating in image.

C. S. Gupta, M. T. Scholar, F. Detection, and C. Forgery, "' A Review on Splicing Image Forgery Detection Techniques ,'" vol. 6, no. 2, pp. 262–271, 2016. In this paper, they have characterized forgeries in two classes. It can either be intrusive (dynamic) or non-intrusive (visually impaired or inactive). In active method, the image needs some type of pre-prerocessing, for example, watermark installed and marks are produced on time of producing image. Passive image forensic investigation is typically an extraordinary test in image handling methods. It incorporates the idea of Copy-Move Forgery, Retouching and Image Splicing. In this paper, a greater amount of the exploration work is done on Image Splicing Techniques and Copy-Move Forgery. In Active approach, Watermarking is a technique for active forgery, as a security structure inserted into the image. Signature is second strategy for active tempering detection, in which signature is inserted into the image as a security implies. If there should arise an occurrence of Passive approach, the first is copy and move, which is exclusive kind of image control method which consist with part of the image itself replicated and glued into another part of a similar image. The second one is Re touching that is characterized as hanging the image on an entirety

G. B. Chittapur and B. S. Anami, "comparison and analysis of photo image forgery detection techniques," no. 6, pp. 45–56, 2012, Digital images are used everywhere like, on the fronts of magazines, daily newspapers, courts, and everywhere all over the Internet. We should know that seeing does not generally accepting. In this paper, they have proposed procedures to recognize such incredible photograph images and main to distinguish formed area by given just the forged image. They have represented file system formats, for example, JPEG, Other image groups like png, bmp and so on. They have outlined calculation running behind with the idea of anomalies and distinguish the fraud areas. This paper focusses on the strategies for identifying

forgeries from various images called as copy and create type of image forgeries. Some forgeries images that are created from various replicated parts and shifted inside alike image to "hide" something is called as copy and move forgery. Along these outlines, the test plan and examination thus concentrates on copy and create and copy and move image frauds. Craftiness person, who needs to finish image forgery, with time not component, for the most part give any discovery technique inconvenience. In the event that image altering happens in a compacted then JPEG Block approach's is to strengthen and do in advance fraud area together with various image strategy in the period in-between uncompressed image after that image gets changed over to the JPEG image formed, the JPEG Block Technique will disregard to catch confirmation of altering. The transformation procedure extinguishes all validation regarding altering subsequently the first altering do not influence any JPEG squares, the JPEG Block Technique validates guarantee when used for testing an image for altering. A multi-layered method is the best training to take after to choose an image is manufactured or true when direction filter is utilized as a proof of tempering.

g. k. s. gaharwar, p. v. v nath, and r. d. gaharwar, "comprehensive study of different types image forgeries," pp. 146–15, Image forgery implies controlling digital image to covering some essential and key data from the image. Usually, the forgery is done as such carefully that it is tremendously hard to distinguish the altered image from the real image. This papers reviews diverse types of active forgery detection techniques through digital signature and digital watermarking furthermore different passive image techniques through copy move forgery, image splicing, image modifying, and lighting condition. Image forgery is a regard huge risk as new and new instruments are accessible with less expensive cost for altering digital images. As there are many kinds of image forgeries, viz, copy move forgry, image retouching, image splicing, and lighting condition, it is extremely hard to have a image forgery identifiable unaffected strategies which applies to all. kinds of frauds. There are combination of forgeriess like copy-move forgery, image retouching and image splicing, which are purposefully ended with no goals.

D. Sharma and P. Abrol, "Digital Image Tampering – A Threat to Security Management," vol. 2, no. 10, pp. 4120–4123, 2013, Modern advanced development accessibility of progressively capable image processing devices undoubtedly control the digital images without leaving clear visual hints been altered, consequently there is a critical need for recognizing the authenticity of images. In fields like forensic science, medical imaging process, internet business, and advanced photography, and authenticity integrity of image is fundamental. In this survey work, extensive review had included for reading and examining the risk of Digital Image altering for security purpose. Different techniques and research issues including the tempering detection and image verification have been talked about and appropriate suggestions for security situation have been introduced. This paper surveys how tempering of images can impact in different application area, for example, medicinal field, internet business, enterprises, photography and so on it likewise divides the danger of the digital image tempering. This paper represents the different categories of tempering, for example, copy-move, image splicing, resize, crop, noise and so on it additionally depicts the image tempering detection control, for example, DCT, DWT, and PCA and impact of tempering in various sections of society. Hence, the issue of constructing up image authenticity has turned out to be more confusing with simple accessibility of digital images and free downloadable image altering software's motivating to decrease the trust in digital photos.

G. Sahu and U. Kiran, "Survey of Different Techniques for Image Tamper Detection on Digital Images," ***Int. J. Adv. Res. Comput. Eng. Technol. (*****, vol. 2, no. 12, pp. 3215–3218, 2013**. In this paper reviews distinguishing the types of image forgeries and various forgery detection technique. It demonstrates techniques that determines original image is recognized from the forged image to provide integrity and authenticity. Image forgery suggests control of the digital image to cover up and to expel important or valuable data of image. Acknowledgment of forged image from the actual image is hard. we can't recognize image without applying much effort to recognize the altered image from original Image. Henceforth, it's necessary to grow such a technique that can distinguish the real image from the altered image. The recognition of an altering image is controlled to provide authenticity and to preserve

integrity of image. This paper reviews distinctive sorts of image forgeries and forgery detection techniques. The review has been done on existing measures for tempered image this paper for the most part concentrates how to distinguish image forgeries. There are miscellaneous techniques for image forgery recognition and limitation identified with them. More useful strategy can be produced to defeat these kinds of limitations caused by the various techniques.

M. Singh and E. H. Singh, "Detection of Cloning Forgery Images using SURF + DWT and PCA," pp. 1–10, 2016.This paper describes the surf technique which act as detector that works with two techniques PCA and DWT to detect the forgery part of image from the tempered image. The image can be tempered by any kind of process such as copy move forgery, cut paste forgery, cloning, splicing etc. this paper reviews the various reasons to perform tempering and the consequences of changing the image. The main focus is done to detect the forgery by using SURF technique. The comparison is performed in DWT and PCA. PCA SURF improves the performance and takes less time usually half time than SURF DWT. hence SURF is used. This methodology used in this paper consist with the basically following parts. Discreate wavelet transform(DWT), lexicographic sorting, shift vector calculation, neighbor block matching. The flowchart that represent the methodology is shown as:
The process goes in four steps: First part is the original image, second is forged image, third image is the image where the actually detection part of image from black and white image that means 2D color. In the last part, copied part of image is displayed. The experiments performed by the author of the paper shows DWT SURF detecting copy move forgery result and PCA SURF perform detection by performing on parameters.

A. Dada, R. V Dharaskar, and V. M. Thakare, "A Survey on Keypoint Based Copy-Paste Forgery Detection Techniques," Procedia - Procedia Comput. Sci., vol. 78, no. December 2015, pp. 61–67, 2016. This paper consists with the survey on key point based copy paste forgery detection technique. This paper work on detecting the copy and move forgery. the copy and move forgery is generally divided into two

main categories. Block based forgery and key point based copy and move forgery. Both use comparable kind of framework but different in feature extraction procedure. Block based copy and move forgery detection is good for detecting forgery and provides high accuracy but also contains high computational complexity. This paper reviews key point approach to detect forgery. key point copy and move forgery detection consist with detecting local features using algorithm SIFT and SURF. local feature detector and descriptor is used. Key point is better to use for large size images than block based approach.

In this paper, the author has proposed a hybrid approach. The author has used two different method for key point detection and to describe those key points. The key points of image are extracted using SURF and then BRISK (binary robust invariant scalable key points) are extracted at these points. The features extracted from BRISK are matched using KNN search to detect the similarity. To find the nearest neighbor, hamming distance is used. The distance of neighbor at a point is compared according to threshhold range lie between 0.3 to 0.5, to remove the outliers in image. This process is robust to affine transformation and post processing operation like JPEG compression or Gaussian noise.

S. Baboo, C. Applications, C. Applications, and C. Forgery, "Detection of Region Duplication Forgery in Digital Images Using SURF," vol. 8, no. 4, pp. 199–205, 2011. This paper detects the duplicate region using SURF for digital images. the common type of forgery is copy and move forgery where most of the approaches are used to detect forgeries. This paper use SURF and KD-Tree for multidimensional data matching for finding copy and move forgery. The key points are extracted in forgery region are matched with the original image. This paper consists with detecting the forgeries in two different steps. The first is using SURF for feature extraction and second is second is key point matching then the next step is verification step filter matching pair which tracks common type of pattern. KD is used for key point matching which provides reliable and lower false rates. The proposed detection method of this paper detects the duplication region when SURF method extracts key points from images and their descriptors are matched according to threshhold. The overview of the

proposed algorithm of this paper is shown with the help of diagram as:

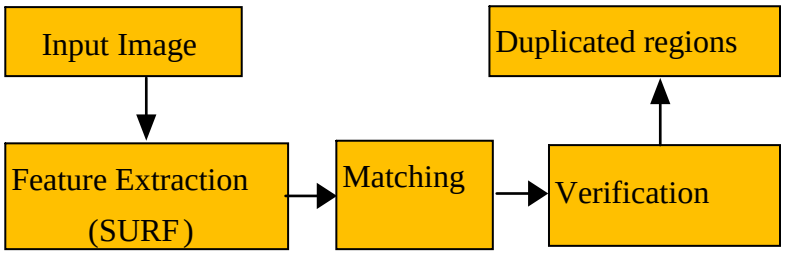

figure 1.1 steps of forgery detection

In this paper, the proposed approach is implemented using the software MATLAB. The SURF is used to detect the key points of image and describe descriptors. The experiments performed in this paper use descriptor mode to get 128-d SURF descriptor and KD- tree is used for key point matching. To test the techniques large image data set of resolutions 3000*2400 pixel is used. The duplicated region in forged image varies with the size and texture.

M. M. Fegade, "Image Forensics for Forgery Detection using Contrast Enhancement and 3D Lighting," pp. 257–260. This paper consists with image forensic for forgery detection using contrast enhancement and 3D lightning based on general reflection model. The contrast and brightness of image can be adjusted by contrast enhancement technique. Then source image is used to match the contrast of two images. In this paper, the author had discussed forgery detection mechanism's in two tiers. The first is contrast of original and forged image is checked and based on contrast matching then image is checked for forgery by 3D lightning effect. This provides more accuracy. This paper had used SLIC for segmentation and two algorithms named as affine transformation and global contrast detection is used to check. if contrast found then image is forged. Face detection algorithm is used to detect face, if face is detected then lightning condition is used with high accuracy. The methodology used in this consist with the steps, initially affine transformation is used on the image. Affine transformation is the function between affine spaces which preserve points straight lines and planes of image. It preserves the ratio of distance between points in a straight line. After that matching process is used to locate the pixels

of forged image to represent in more exact way. The interested points are extracted to reduce the checking time. then EM (expectation maximization) algorithm is used, it computes interpolated coefficient in images to detect the forgery.

G. Sahu and U. Kiran, "Survey of Different Techniques for Image Tamper Detection on Digital Images," *Int. J. Adv. Res. Comput. Eng. Technol. (*, vol. 2, no. 12, pp. 3215–3218, 2013.This paper had worked on adaptive forgery detection and feature point matching to detect the forgeries. Adaptive over segmentation procedure is like to traditional block based forgery, that divides the host image into block with defined and fixed block size. The forgery is detected by matching blocks. but the detected region is composed of regular blocks which accurately detect forgery and also recall rate is low. If size increases computations also increase. So, this paper has proposed SLICO algorithm used to segment the image. By using this user not need to set parameters and hence can try different values. This generate regular shape pixel in both textured region and non-textured region alike. SLICO is as fast as SLIC but provide high computation efficiency. And SURF is used for feature extraction.

I. Amerini, L. Ballan, S. Member, R. Caldelli, A. Del Bimbo, and G. Serra, "A SIFT-based forensic method for copy-move attack detection and transformation recovery," pp. 1–12, 2011. In this paper SIFT base forensic method is used for copy move forgery and transformation recovery. Sift is proposed to detect forgery for various geometric transformation and to detect copy move forgery. This paper present result very precisely and also estimates geometric transformation with high reliability and also deal with multiple types of cloning. After extracting features using SIFT, geometric transformation is applied and matching is performed. This works in three steps: SIFT for feature extraction, key point clustering is performed using agglomerative hierarchical clustering, and geometric transformation. This paper uses two databases for testing that are MICC-F220 and MICC-F2000 which is a large image dataset. In this paper, the proposed approach is able to detect copy move forgery with different kind of geometrical transformation. A robust feature matching mechanism is used to match the features and clustering on key point are used to manage multiple types of copy move forgery. Hierarchical clustering is applied after feature extraction.

it produces hierarchy of clusters which is represented by tree structure and then spatial distance among the various clusters is computed. And find the closest pair of cluster. this way final merging is performed.

J. Zheng, Y. Liu, J. Ren, T. Zhu, Y. Yan, and H. Yang, "Fusion of block and keypoints based approaches for effective copy-move image forgery detection," *Multidimens. Syst. Signal Process.*, 2016.This paper consists with fusion of block and key point based approach to detect copy move forgery. In this paper two approaches are used to detect copy move forgery that are block based approach and key point based approach. Block based approach has two limitation that is high computational complexity and cannot used for geometric transformation. key point overcome this limitation in this paper but difficult for smooth region detection. SIFT is used for feature point extraction. Ratio between number of key points and total number of pixels used to classify region into smooth and non-smooth block based using Zernike moment key point using SIFT along with filtering and preprocessing key provide reliability point. Block based technique is efficient., hierarchical clustering is used and RANSAC filter is used to filter outliers. SLIC is used for segment the image into small regions. In this paper, the image s firstly divided into non-overlapping region using SLIC algorithm. After that SIFT is applied to detect the key points from the image. Then region is classified as smooth or key point region based on the ratio of key points to the number of pixels is less than threshhold. in this paper, multiple key points matching is also performed in key point to detect candidate forgery region. Zernike moments are used as block features, if there are more than two smooth regions. To obtain the initial size of super pixels. four level DWT is used to analyze frequency distribution of image.

Key point extraction follows two principles, if ratio between number of key points and number of pixel is less than threshhold T, it is smooth region, otherwise it is key point region. Where N_f, is the number of key point and N_p is the number of pixels and R=0 indicates the key point region and R=1 indicates smooth region.

V. Agarwal, "Reflective SIFT for Improving the Detection of Copy- Move Image Forgery," pp. 84–88, 2016. This based is based on reflective SIFT for improving detection of copy move forgery. The images can be scaled, rotated, or flipped. SIFT is

used to match image but fail for flipped images. in this paper, it is shown how MIFT improvise SIFT and dataset MICC-F2000 and CASIA V2.0 is used. This paper has combined the Lowe's SIFT with Irene's contribution and improvise it with X.GUO's MIFT. MIFT work even for image splicing and retouching kind of forgeries. The FPR for detection is 0. Accuracy has also been improved in this paper. Computation time is less but this paper is failed to detect the forgeries in flat region. The technique used in this paper have advantages like it can deal with the various transformation like blurring, deformation. Time and space required for computation is also very less as compared to block based methods. But it consists with some problems that it does not work for the flat images areas and high false positive rate is a major issue to be resolved. Computational efficiency can be improved by using proposed technique.

P. Kovesi, "Image Segmentation using SLIC SuperPixels and DBSCAN Clustering," vol. 34, no. 11, pp. 1–6, 2017. In this paper, image segmentation is performed using SLIC super pixel and DB SCAN clustering is performed. This paper had proposed SLIC super pixel and algorithm for over segmentation of image. These pixels are processed using DB SCAN clustering algorithm to form cluster of super pixel to compute final segmentation. It is easy to perform and simple. In this paper, the analysis is performed on image segmentation and MATLAB is used to detect the forgery using adaptive over segmentation approach. This paper describes that for edge based detection canny algorithm is used for good segmentation. For Forgery threshhold based algorithm, adaptive thresholding produces good result. For region based algorithm, split method provides good result. For clustering based algorithm, mean shift fuzzy is better than K-means algorithm. For graph based algorithm, normalized cut is used to cut an image into number of cuts.

M. Singh and E. H. Singh, "Detection of Cloning Forgery Images using SURF + DWT and PCA," pp. 1–10, 2016.This paper works on two techniques DWT and PCA that are used with SURF which act as detector that is used to detect the forged part of the image. Both SURF with DWT and SURF with PCA technique is used for validation but PCA when used with SURF provide better result in all the respective. PCA detect the forged part with SURF and takes less time in detection process than DWT SURF.

The images can be tempered in many ways like adding new things in the image, removing some part of image, or misrepresenting the information of image. The methodology used in this paper used for detecting forgery consist with the following parts: discreate wavelet transform, lexicographic sorting, shift vector calculation, neighbor block matching. To detect the forged part of image from the original image, the image is acquired first, then image is read, correlation measures are applied on image. the difference is measured to identify the original and forged image. the author has performed different experiments on SURF, PCA, and DWT which provides different result for copy-paste forgery detection. PCA SURF technique is used to detect copy and paste part of the image, same way DWT SURF shows which part of the image has been copied. Both have their different way of detection but according to the author of the paper, PCA SURF is best because it detects the object and remove that part of image but DWT SURF do no remove the part of image but only tells which part of image has been copied. Moreover, PCA SURF takes half less time than DWT SURF and provides more clarity.

R. V Roy, "image forgery detection using adaptive over segmentation and feature point matching," vol. 4, no. 4, pp. 640–643, 2016. this paper has used block based technique and feature point method to detect the forgery in the image. In this technique, first adaptive segmentation is performed to divide the host image into non-overlapping and irregular blocks. Then features are extracted called block features. These features are matched to locate the labeled feature point. This way it detects the forgery in the image. To detect the forgery in more accurate way, the author has used forgery region extraction algorithm, it replaces feature point with small super pixel as feature block and then the neighboring block that consists with similar kind of local features into features block to produce forgery region. At last, it applies morphological operation on the merged region. The proposed approach detect copy move forgery in better way under many challenging conditions.

The planned approach uses two techniques: block based technique and key point matching technique. For block based method, DCT, PCA, DWT, and SVD algorithms are used. these methods divide image in multiple principle components. PCA is applies

to reduce the color of the image. Foe key point method, SIFT and SURF algorithms are used to extract the features and then these features are matched. if the shit vector exceeds the threshhold, then the SIFT feature point are defined as forgery region. In the proposed approach of this paper, first input image is divided into rectangular blocks and then DCT (discreate cosine transform) coefficients of blocks are matched for detecting the forged region. To divide the image into various irregular blocks, SLIC (simple linear iteration clustering) algorithm is used. It uses K-means clustering technique to produce super pixels in the image. SLIC segmentation algorithm is calculated with initial size to attain the image blocks. In equation, S is the initial size of super pixel. M*N indicates the size of main image and Means percentage of low frequency distribution.

Y. Li and J. Zhou, "Image Copy-Move Forgery Detection Using Hierarchical Feature Point Matching," pp. 3–6. key points based detection method is used to detect the copy and move forgery but it fails to handle copy move forgery for small and smooth region When the key point in the image are limited. so, to tackle all these problems, the author has proposed copy move forgery detection technique by decreasing the contrast of the image. The contrast threshhold and by rescaling the given image, hierarchical matching is used to solve the problem of key point matching. It provides dominant alignment of each key point of image.

For lowering the contrast threshhold C, a contrast threshhold value is set. Any extrema with less than threshhold C are rejected to SIFT key points. After that resizing of the image is performed to provide more accurate key points, that are distributed densely in image plane. A larger key point is obtained for small and smooth region but it can cause problem in matching. To solve this problem, hierarchical feature point matching is used. It describes the associative key points and their corresponding descriptors.

L. Suresh and P. S. Kumar, "Image Forgery Detection Using Adaptive over," pp. 11544–11550, 2016] detection of cloning forgery image using surf +dwt and PCA. This paper describes the surf technique which act as detector that works with two techniques PCA and DWT to detect the forgery part of image from the tempered image. The image can be tempered by any kind of process such as copy move forgery, cut

paste forgery, cloning, splicing etc. this paper reviews the various reasons to perform tempering and the consequences of changing the image. The main focus is done to detect the forgery by using SURF technique. The comparison is performed in DWT and PCA. PCA SURF improves the performance and takes less time usually half time than SURF DWT. This methodology used in this paper consist with the basically following parts. Discreate wavelet transform(DWT), lexicographic sorting, shift vector calculation, neighbor block matching. The flowchart that represent the methodology is shown as: The process goes in four steps: First part is the original image, second is forged image Third image is the image where the actually detection part of image from black and white image that means 2D color. In the last part, copied part of image is displayed. The experiments performed by the author of the paper shows DWT SURF detecting copy move forgery result and PCA SURF perform detection by performing on parameters.

G. Muhammad, M. S. Dewan, M. Moniruzzaman, M. Hussain, and M. N. Huda, "Image forgery detection using gabor filters and dct," 2014. in this paper, image forgery is detected using Gabor filters and DCT (discreate cosines transform). This technique is used to check the authenticity of the image. The process of detecting forgery from the image consist with the two steps: initially the image is divided into grey image. Secondly numerous types of Gabor filters are applied with different type of scales and orientation is applied onto the image. After filtering output, DCT is applied on it to detect the forgery. Feature vector is formed by concatenating if first N coefficient of DCT. Then SVM (support vector machine) is used for classifier which classify the different types of features in the image. Some features of image are selected to form the optimal set of features.

A 2-dimensional global filter transform(GFT) is applied on the image to find the kind of chrominance components. The main features of GFT is that it consists with optimal type of joints localization for both in case of frequency as well as spatial domain. The two dimensional GFT is applied on the image and the equation is given in the paper [ ]. In the equation, $\imath_x$ and $\imath_y$ are considered as scaling parameter. W is the central frequency and it is known as orientation of filter. In this GFT, is used with three values

of scaling. i.e. 2, 3, and 4. And five types of orientation are used as 0, π/5, 2π/5, 3π/5, and 4π/5.

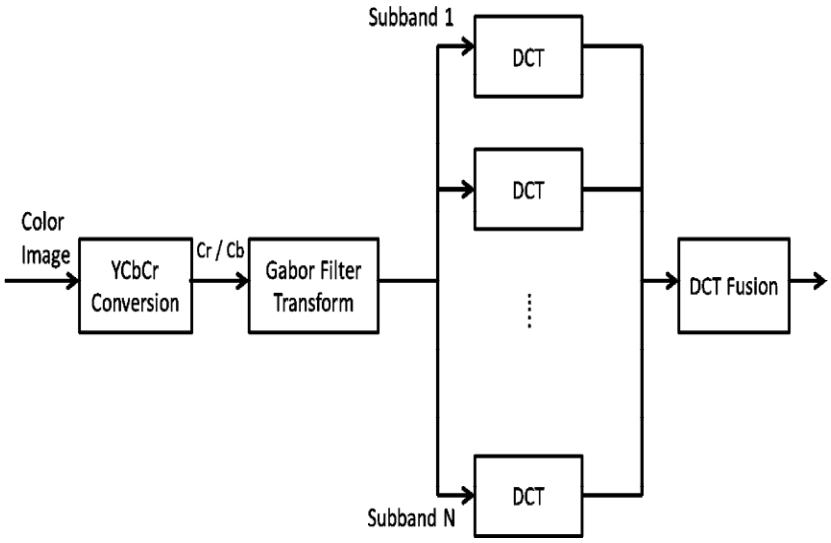

Figure 2.2: Process of DCT

Then features are extracted using discreate cosines transform. DCT is performed on each filter. DCT represents sum of cosines of different image. DCT represents the information only in few coefficient and this is the main feature of DCT. DCT then transform the array of pixel value to array of coefficient of frequency. Then features are selected using two methods: 0-norm and Local learning based. 0-norm provides features based on the statistical consequence. And LLB contains the duplicate info. These two are concatenated to improve the performance.

H. Moradi-gharghani and M. Nasri, "A New Block-based Copy-Move Forgery Detection Method in Digital Images," pp. 1208–1212, 2016. in this paper, block based approach is used to detect copy move forgery. by using this method, feature vectors are extracted using discreate cosines transform from the image blocks. Then these vectors are sorted, copied blocks are selected from similar vector based on some criteria. The main part of this paper is threshhold is considered to eliminate large flat parts of image. For e.g.: sky is removed from the image when detecting the forgery in the image. According to the author of the paper, forgery can be easily detected with small positive rates if compared with other existing techniques.

The proposed technique of detecting copy and move forgery consist with the two similar regions of image. for that similar type of area is compared in shape and size. Hence image is divided into blocks so that it can be compared pixel to pixel. After that features are extracted from each block. All blocks will have some features and similar block will have similar features. Then features are sorted in lexical order before matching process of feature pair of features are tested to test that whether images are matched or not. If features of similar blocks are matched, those blocks are assumed to be similar. Then algorithm set some parameters to delete wrong or invalid matches, to reduce false matches. The features are extracted using DCT and SVD and it is effective method for extracting features from the Image. The process of detecting forgery consist with the following steps: first the image is divided into blocks and all block are of equal and similar size. DCT is applied on each block of the image to determine DCT coefficients. Features are extracted using SVD of each block. Identical pairs of blocks are matched. false matches and outliers are removed and finally image is detected as forged or original image.

V. Bharathi, "An implementation of block and keypoint based forgery detection scheme," pp. 55–60, 2016.this paper detects the forgery by using two techniques SWT (stationary wavelet transforms) and IDCT (inverse discreate cosines transform). hence it reduces the computation complexity if compared with time and cost and also increases the efficiency of image. To detect the forgery, image is initially divided into matrices which consist with the rows and columns. Then SWT is applied on each row and column of matrices and use row reduction and column reduction techniques. The algorithm used to detect forgery by using super segmentation algorithm technique. At last duplicated image is generated based on the threshhold value. SWT is similar to DWT except signal is not sub sampled and filters are up sampled at each level of decomposition.

S. Sodhi, "Surf Technique for Copy Move Forgery Detection," vol. 2, no. Icaet, pp. 10–12, 2016. Images can be edited by using powerful tools like photoshop. The authenticity of images is very important so we need to find the authenticity of images, in this paper SURF technique is used for finding the copy and move forgery detection.

The forged part of image is detected by using SURF technique and MATLAB platform is used to analyze the performance of copy move forgery detection with different type of resolution of images.

Copy and move forgery detection technique is primarily divided into two parts: block based method and key based method. In Block based method images are divided into various irregular blocks and then features ae extracted from each block of image. The extracted features of the image are matched, if the features of corresponding blocks are matched, then the image is considered as forged image otherwise the image is not forged. The block based methods are DCT, DWT, PCA, DFNT, and Zernike moments etc. block based technique also deal with the operations like handling the noise or outliers and compression but it cannot handle with various geometric transformation of the image like rotating image in any angle, scaling etc. hence block based technique is efficient and also takes more time to compute whereas key point based technique find the feature vector and compare them for forgery detection. The algorithms used by key point based methods are SURF, SIFT and ORB (oriented fast and rotated brief). This technique can handle various geometrical transformations but cannot deal with the compression and noise. But key point based technique is faster than block based technique because of computation efficiency. Hence it is good to use hybrid technique that consist with both block based technique and key point based technique to provide better result. The SURF technique consists with the following steps to compute the forgery, image is inputted, then features are extracted using SURF and then features are matched and verification is performed to compute the forged region.

K. Kiruthika, S. D. Mahalakshmi, and K. Vijayalakshmi, "Detecting Multiple Copies of Copy-Move Forgery Based on SURF," vol. 3, no. 3, pp. 2276–2281, 2014. In this paper, the goal of the author is to detect multiple duplicate copies of same and changed region of image. The author has used key point based method and SURF is used for feature mining. G2NN strategy is used for recognizing matched points. And hierarchical clustering is performed on matching key points to detect the false detection rate so that the false detection rate can be decreased. The proposed approach of the author consists with the following steps detecting forgery. First the preprocessing is

performed. in this step RGB image is converted into grey scale image. Then features are extracted using SURF method. SURF features are extracted using the steps: integral part of image is calculated, key point detection is performed, orientation assignment is performed, and at last feature descriptor are generated.

Then features are matched using G2NN strategy. it starts with considering the high dimensional feature space, the feature that are different are very high and similar values among them. The ratio with respect to threshhold. Then filtering is performed to reduce the false matches. The neighboring pixels of image may have similar intensity which leads to the false forgery detection. Then Euclidian distance is calculated. The hierarchical clustering is performed to cluster the forged region of the image. It is performed to avoids the false positives. Hierarchical clustering is performed in three steps: the first step is assigning the key point to the cluster, second step is computing reciprocal spatial distance among cluster. Then closest pair of cluster is found. The last step is merging them into single cluster. The error can be measured as finding the precision and recall rate. In the equation, T_P is the number of exact spotted forged region, F_P is the number of images that have been detected in error and F_N is the Misleadingly missed forgery image.

A. Kaur, "Copy-Move Forgery Detection using DCT and SIFT," vol. 70, no. 7, pp. 30–34, 2013. Image can be tempered in many techniques and it is necessary to detect the forgeries in image. There are many methods which can be used to detect forgery in image. In this paper, DCT is used to detect copy and move forgery. In this method, the image is divided into blocks and then duplicated part of the image is detected by applying DCT on each block. This method is applied on different kind of forgeries and the effectiveness and robustness of the technique is computed by checking the technique on multiple forgeries. The main aim of the paper is to show that DCT is better than PCA hence DCT is applied by the author instead of PCA because the forgery is tested on JPEG images and PCA does not check forgeries for JPEG images efficiently. The result of both DCT and PCA is compared in this paper.

The process of applying DCT on the image is to detect copy and move forgery which consist with the following steps: first the image is taken, and divided into overlapping

blocks. Then DCT is applied on each block of image. The rows are sorted in lexicographical order then it is checked, it will be discarded whose offset value is greater than NF and whose distance is less than ND. At last, those pixels are colored which occurs in duplicated region. In this paper, the author has determined that if block size increases the detection of forgery rate decreases. Because block size technique does not work well when the block size increases. On the other hand, when the block size increases, the execution time also increases.

G. Zhang and H. Wang, "SURF-based Detection of Copy-Move Forgery in Flat Region,"vol. 4, pp. 521–529, 2012. copy move forgery is the main common type of forgery. the existing methods such as block based forgery detection method and key point forgery detection method are used to detect forgery in the image but it cannot detect forgery for both flat and non-flat region. In this paper, these two techniques are combined and a new technique is developed which is known as SURF based method to solve the problem of individual technique. the new technique detects non-flat region as well extract features from flat region in effective way and also extract FMT features after blocking the region. the matching algorithm are used in similar kind of block images. hence forgery is detected in flat region which result for entire temper detection. In the proposed technique of the author, image has two parts: flat and non-flat region. These two regions are separated by using flat region detection algorithm. Then forgery is detected by using block matching and key point matching based techniques. The forgery in non-flat region is detected by extracting key points from the image. these key points are used to reconstruct the parameters of geometric transformation. The detection of forgery in non-flat region consist with the following steps: key points are extracted using SURF. Then features are matched and at last duplicated regions are identified using correlation adjusted factors.

The forgery in flat region is detected by observing the changes performed in local pixel value. The key point is extracted by drawing black square and taking key point in center. Erosion and open operators are used to fill the small holes of the image. in this paper, it has been concluded that key points based method are powerless when there is no key point region. But tempering exists in the image. according to the paper, the

image is separated into two regions hence different methods are used to detect forgery of image. this provides maximum efficiency and provides more effectiveness

L. Kabbai and A. Douik, "Image Matching Based on LBP and SIFT Descriptor."in this paper, two techniques are used to detect forgery i.e. LBP and SIFT. a new approach is proposed which is inspired from SIFT which match features by extracting interest points(IP), But this technique perform bad when background is complex or it contain noise. Hence LBP (local binary pattern) is used with uniform pattern and center symmetric LBP also called CSLBP instead of feature used in SIFT algorithm. Different measures are computed such as precision, recall under different image transformation like blueness, attack, rotation etc. SIFT descriptor extract the most stable interest points(IP) and create a vector descriptor. LBP is used for extraction of texture feature. This is robust under illumination changes and also quick to compute. LBP is widely used in the process like image retrieval, object recognition and provide good performance in face recognition. CSLBP is used as another type of modification of LBP. This method does not test grey level of center with grey level of neighborhood but test center symmetric pair of grey level pixel. In the Feature matching process, the matching of various.

.

CHAPTER 3

PRESENT WORK

3.1 PROBLEM FORMULATION

In Copy-Move forgery a part of image is copied and then pasted on to another portion of the same image. The main motive of such forgery is to hide some useful information of the image from the original image to make it forged image.

The most common type of method used for detecting these types of forgery is called block matching method. In this method, each block of image is matched with all other blocks of the image to find the forgery in the image. The block matching technique consist with many approaches to detect forgery of image. For instance, Fredrick and Lucas [2] used DCT (discrete Cosine transform) have used block matching technique. However, block based method fails for type of operations like geometrical transformations of the query block e.g. rotation of image, scaling of image etc.

A.C. Popescu [3] proposed a major component analysis (PCA) on pictures blocks to give a reduced measurement representation. H. Huang [4] first generated SIFT descriptors of a picture, which does not depend on lighting and rotation of image etc.

Luo [5] applied color information for the various blocks of image. The full block is separated into four sub blocks and is considers average of red, blue and green color values of image. Results show this process to be very vigorous to the various attacks like, JPEG compression, Gaussian blurring and additive noise.

Kumar Vivek [6], proposed an method that divides the blocks of image into sub blocks and some kind of mathematical functions are performed to get some useful feature values. This method is not robust to detect attacks like of rotation by an arbitrary degree and for scaling.

In fact, an effective copy-move technique must be strong enough for the various attacks like losses due to compression, addition of noise, rotation and scaling of image. nowadays, no method appears to have been described which is well-organized with all the above handlings in proper time. MATLAB (matrix laboratory) is a mathematical computing environment established by Math Works, MATLAB allows matrix operations, plotting of functions and statistics, implementation of algorithm, thus MATLAB is used to tool all methods which is easy to usage than other tools. Therefore, Hybrid Copy-Move forgery detection techniques by using MATLAB is aim of my thesis.

3.2 OBJECTIVES

There are many techniques that can be used to detect copy-move forgery. Some of those techniques cannot detect copy-move because of manipulations performed in the edited image such as rotation, scaling, resampling, noise, contrast enhancement. Therefore, in this work I will try to detect the forgery even after those manipulations are made on image. There are many new operations to edit the image and hide the traces of the image. we have the following objectives:

1. Our objective is to combine the different methods SHIFT, LBP and KOLMOGROV SMIRNOV in order to get optimized result in proper time.
2. To divide the image into blocks and to find distance between various blocks using LBP and KOLMOGROV SMIRNOV technique.
3. To implement SIFT and SURF algorithm to detect the key points of the image.
4. To match the key points of original and forged image and detecting forgery.
5. To design an algorithm for detecting forgery in the image using hybrid technique.

3.3 FACILITIES REQUIRED

3.3.1 HARDWARE REQUIREMENTS

Intel core i3 processor

4 GB RAM

3.3.2 SOFTWARE REQUIREMENTS

MATLAB 2013

Windows 7,8,10

3.3 RESEARCH METHODOLOGY

The chapter describes the process followed in conducting the research work. It explains the process used to detect the forgery by matching the various key points of original and forged image. The matching or non-matching part of original and forged image defines the forgery in the image. The methodology and flowchart in the next section explains the whole process that make possible to detect the forgery.

The Methodology involved in this research is of three phases

1. **Deep Investigation:** In this phase, the Research is done for various forgery detection techniques. From the survey, it is cleared that the performance of all the forgery techniques cannot be used to detect all types of forgeries. For e.g. Some forgery techniques can detect copy move forgery but does not support scaling in copy move forgery. So, in this study the copy move forgery can be detected for most of the cases like scaling, rotation and also detect forgery in less time.
2. **Designing and Development:** In this phase, the main emphasis is on the designing and development of the improved forgery detection technique that is to be proposed in this research. In the designing phase, two images are taken that are original and forged. Then key points are extracted from both the image by using SIFT algorithm and find the distance between the various blocks of image which increase performance by providing good forgery detection rate.
3. **Testing:** The images of dataset MICC-F220 is tested on the proposed algorithm. Hence accuracy is achieved by testing more and more images of the dataset.

ALGORITHM

Step1: Load the Input Image

Step2: Resize Image into 200 x 200

Step3: Apply Sift Algorithm Over Image Step by Step

(i) generating key points of the image

(ii) plotting key points onto image

(iii) obtaining key point neighborhoods

(iv) Finding orientation and magnitude of the various key point produced

(v) Forming key point Descriptors.

Step4: Dividing Image into 4x4 blocks

Step5: Calculate Time taken for finding key point Descriptors.

Step6: Divide Red, green and blue Frame Image into Over-Lapping Blocks.

Step7: Generate Histogram on feature generated by LBP.

Step8: Find distance of Each Block of R using Kolmogorov Smirnov Algorithm.

Step9: Divide Green Frame Image into Over-Lapping Blocks.

Step10: Perform Matching between all the Block and Generate the Common Value.

for loop=1: N

for loop2 =1:M

R_Final = {Red Frame(loop) == Red Frame(loop2)} G_Final = {Green Frame(loop) == Green Frame(loop2)}

B_Final = {Blue Frame(loop) == Blue Frame(loop2)}

Common Value = {R_Final == G_Final == B_Final}

end of loop1

end of loop2

Step11: Detect the Forged Portion from the Image.

FLOWCHART

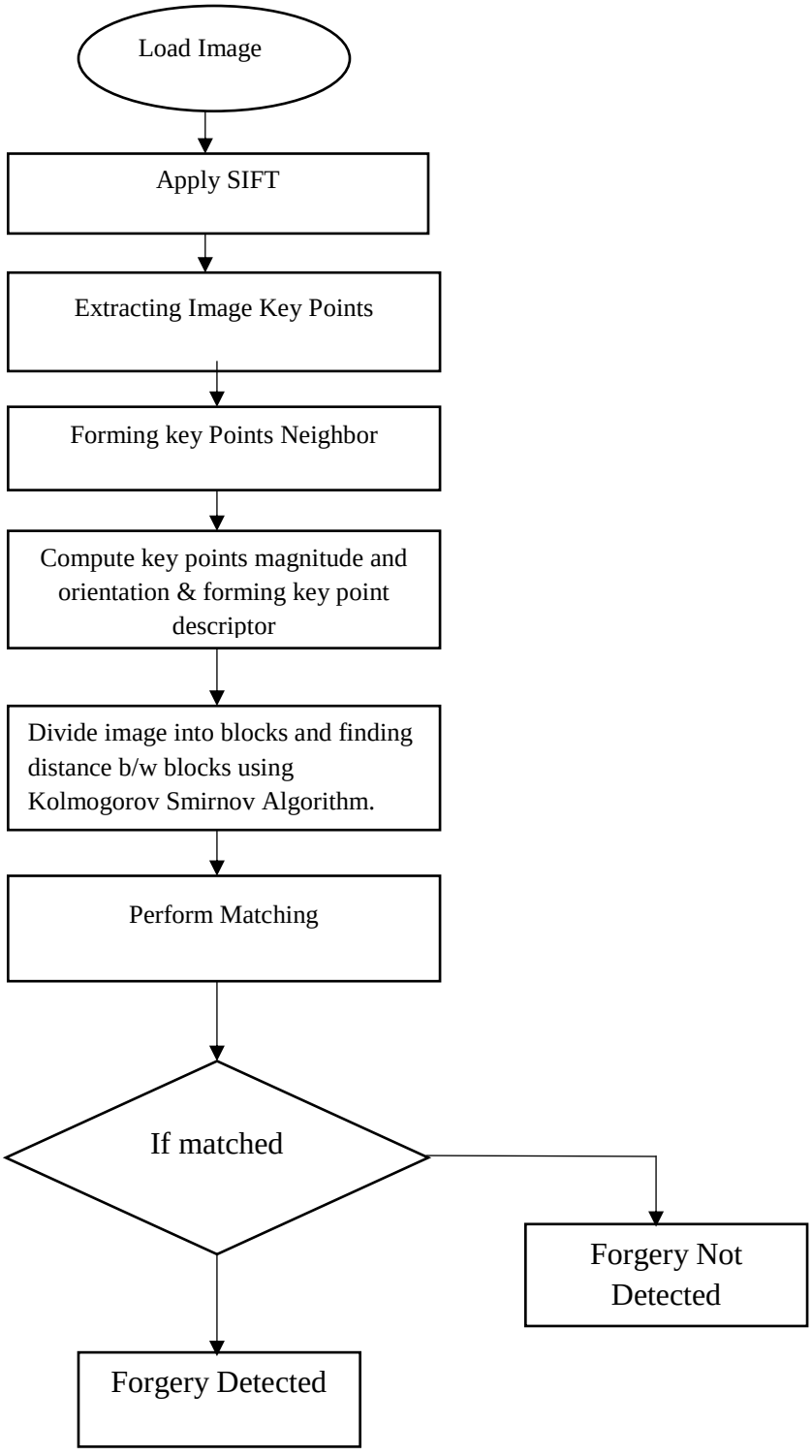

Figure 3.1 FLOWCHART

CHAPTER 4

RESULTS AND DISCUSSIONS

4.1 INTRODUCTION TO MATLAB

MATLAB (matrix laboratory) is a multi-view computing condition and fourth era programming languages. An exclusive software engineer language created by Math Works, MATLAB permits grid controls, plotting of functions and data, execution of calculations, making of UIs, and interfacing with projects written in different languages, including C, C++, Java, Fortran and Python

Despite the fact that MATLAB is expected principally for numerical computing, a discretionary tool compartment utilizes the MuPAD, typical engine enabling access to symbolic computing ability. An extra bundle, Simulink, includes graphical multi-space simulation and model-based plan for dynamic and embedded frameworks.

It is an intelligent program which gives numerical calculation and representation of information. With the assistance of its programming capacities it gives tool which is extremely helpful for all fields of science and engineering.

Tool box gives an exhaustive arrangement of reference-standard calculations, functions, and applications for picture processing, examination, representation, and calculation improvement. You can perform picture improvement, picture de-blurring, feature detection, noise reduction, picture segmentation, geometric changes, etc. Numerous toolbox functions are multithreaded to exploit multi-threaded and multiprocessor PCs.

Picture Processing Toolbox chains a different arrangement of pictures and their sorts, together with high strong range, inserted ICC profile, topographic and gega pixel determination.

4.2 EXPERIMENTAL RESULTS

The results of performing operations in MATLAB to detect the forged image is shown with the help of various images. the graphs are also shown with respect to some parameters used in the implementation of proposed work.

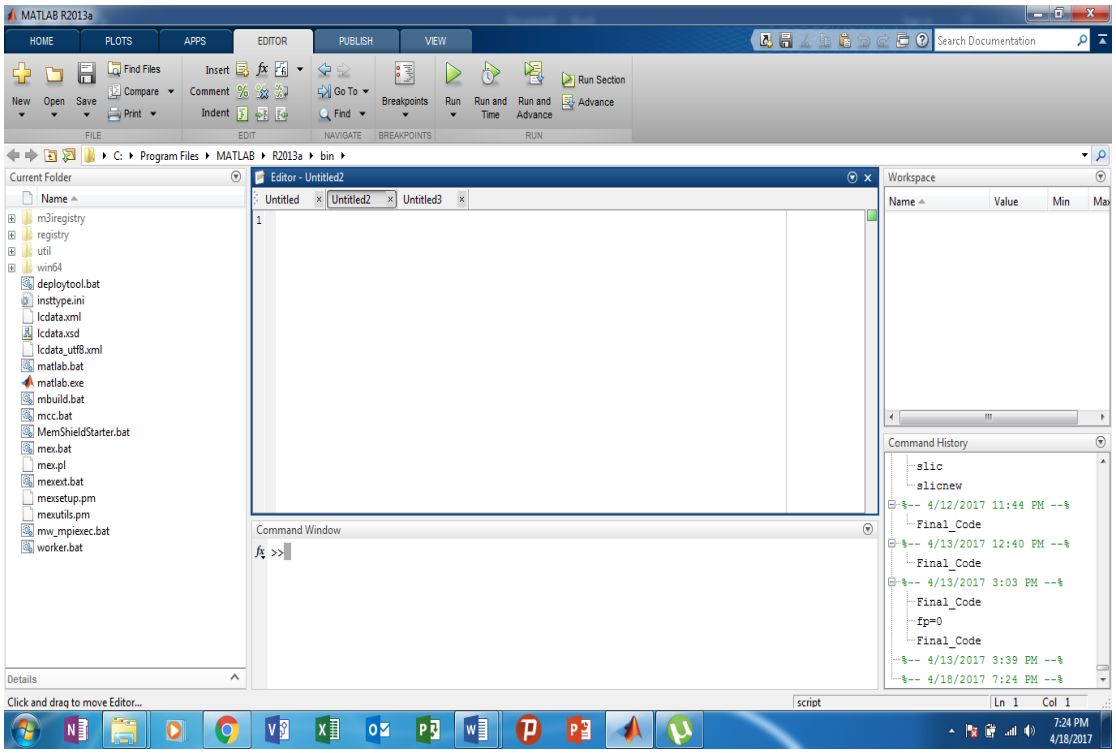

Figure 4.1: MATLAB home page

figure 4.1 represents the home page of MATLAB. The MATLAB. The homepage of MATLAB consists with important features of MATLAB. It displays the menu bar at the top of home page which consists with options home, plots, apps, editor, publish and view. It contains current folder which displays all the files of the user. Editor is used to type the program in MATLAB, before executing MATLAB program the program must be saved somewhere. Command window is used to execute various operations and displays the results of the various operation. Workspace defines the variables used in the MATLAB code and their datatype, value and min and max values. Command history describes the history of various commands executed. We can use command history to execute any previous executed command again.

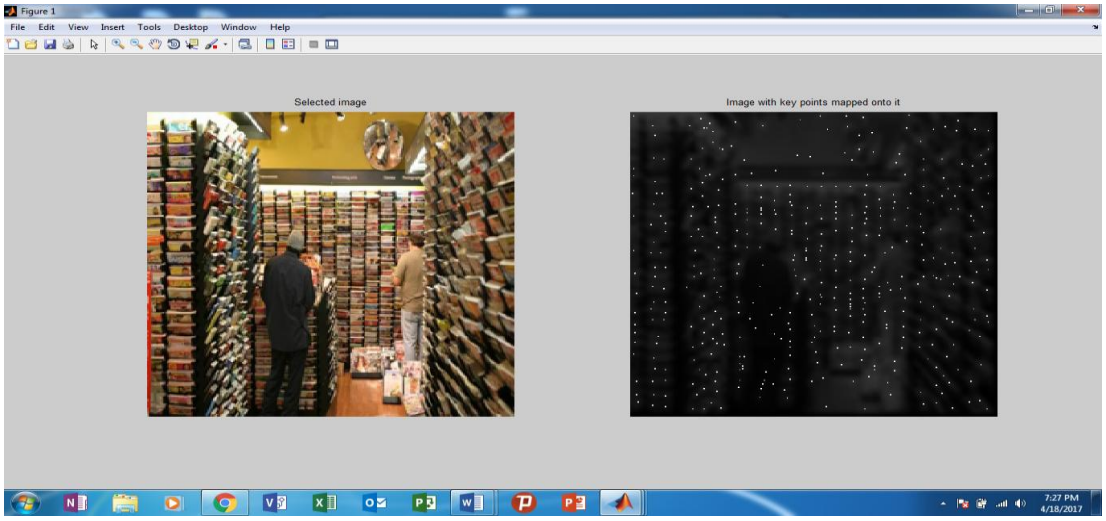

Figure 4.2 original image and key points

Figure 4.2 displays the two images. first is the original image. the original image is taken from the data set MICC-F220. In the second image the key points of original image is shown. The key points of the image are the interest points of image that does not change in each scenario whether the image rotates, shrinks or expands i.e. affine transformation. The key points of tempered image must be same with the original image. The key points of image in the proposed work are extracted using the SIFT algorithm. The SIFT technique is applies on image and key points are plotted onto image. the orientation and magnitude of various key points. Then key point descriptor is formed.

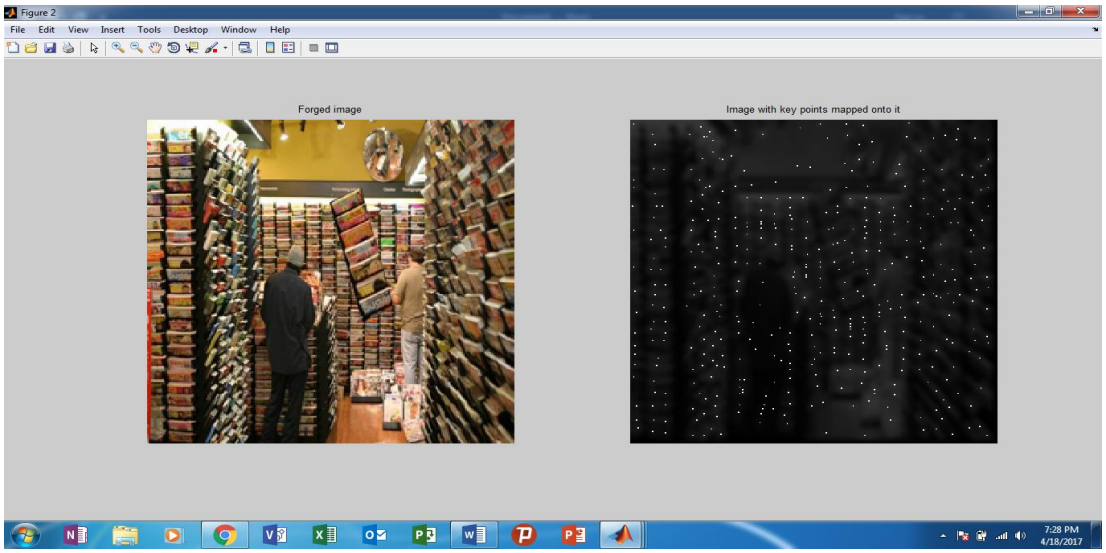

Figure 4.3 Forged Image and key points

Figure 4.3 represents the forged image and its key points. forged image is taken from the same data set MICC-F220. The dataset contains both original and forged images. one original image is tempered in seven to eight ways in the dataset. The key points of the forged image are calculated same as original image by using SIFT algorithm. The matched key points of forged image with the original image defines the forged region of the image.

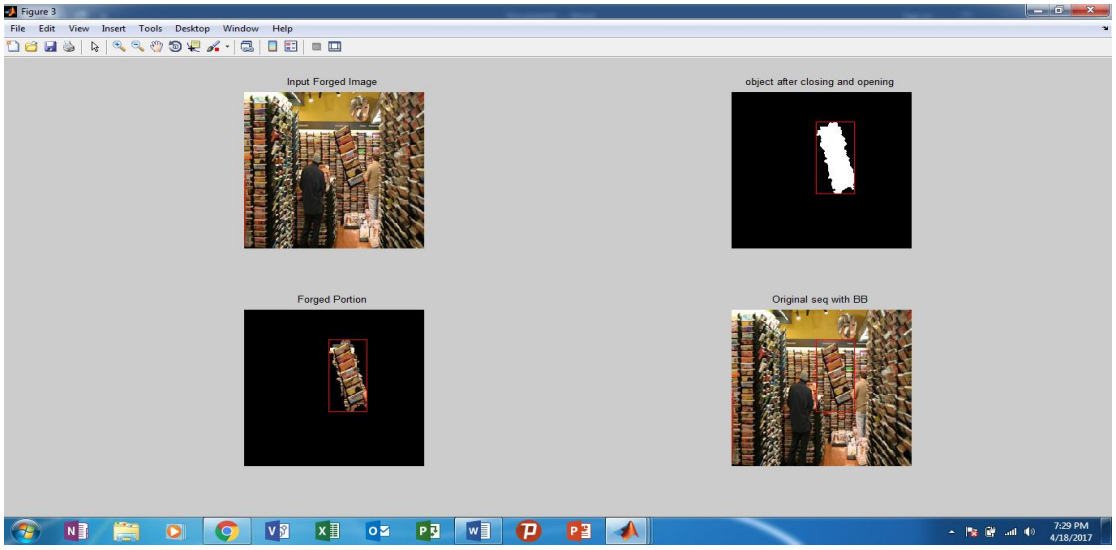

Figure 4.4 Original and Forged Part of Image is Detected

Figure 4.4 represents the four images; the first image is the forged image. the second images describe the forged part of image in the form of white patch over the black background of the image. the third image describes the part of image which is forged. And the last image shows highlight the forged image in the original image

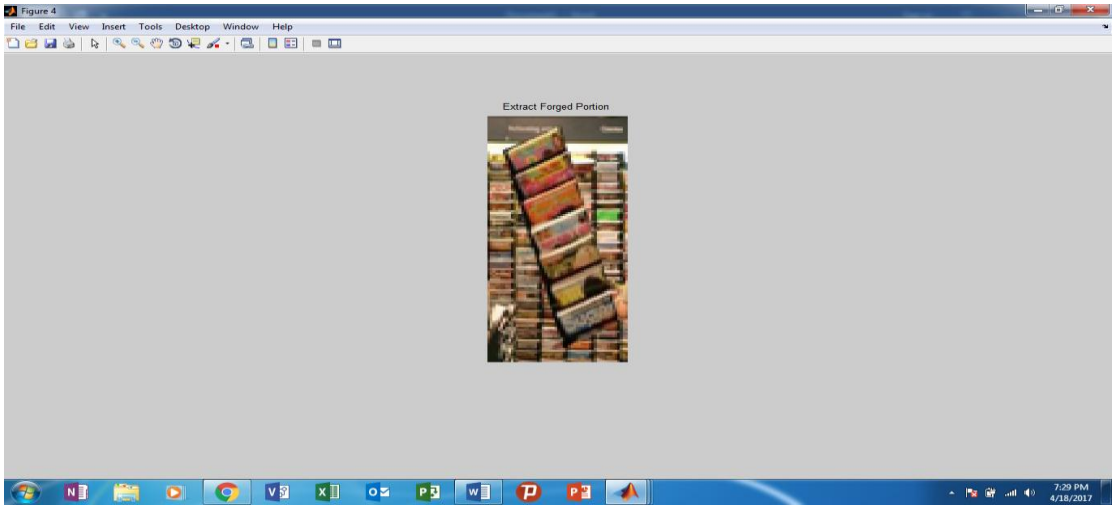

Figure 4.5: The Extracted Forged Part from Image

Figure 4.5 shows the forged part of the picture which is been taken out from the full forged image. hence it clearly describes the image forgery. the forged part of image indicates that image orientation is changed to create the image forgery.

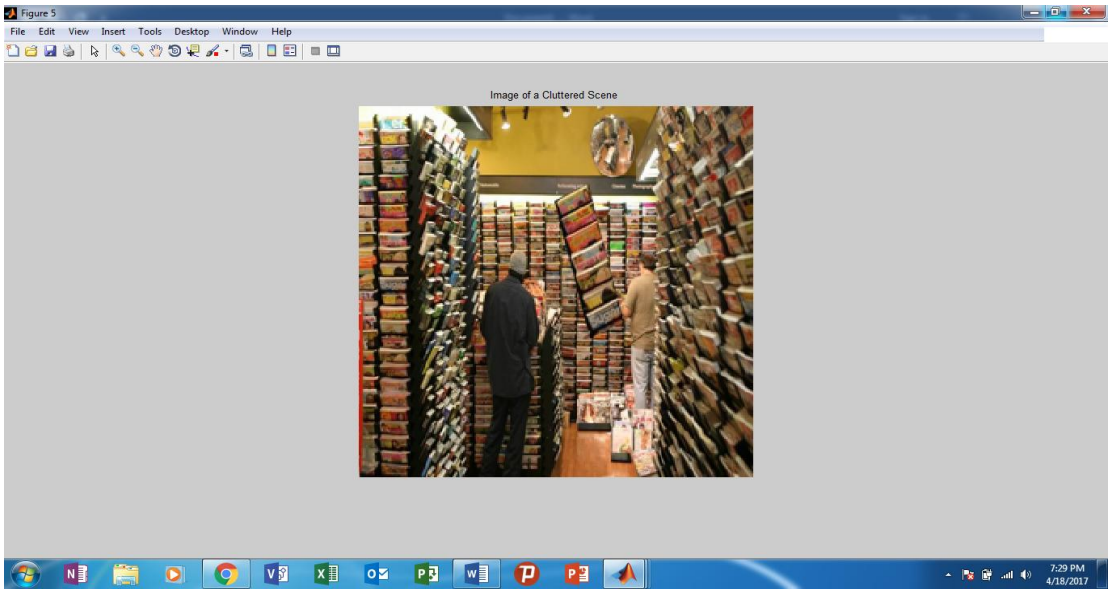

Figure 4.6 Image of a cluttered scene

Figure 4.6 shows the image in cluttered scene. Hence it is difficult to detect the forgery through eyes. The other parts of image make confuse to detect the forgery contained in the image.

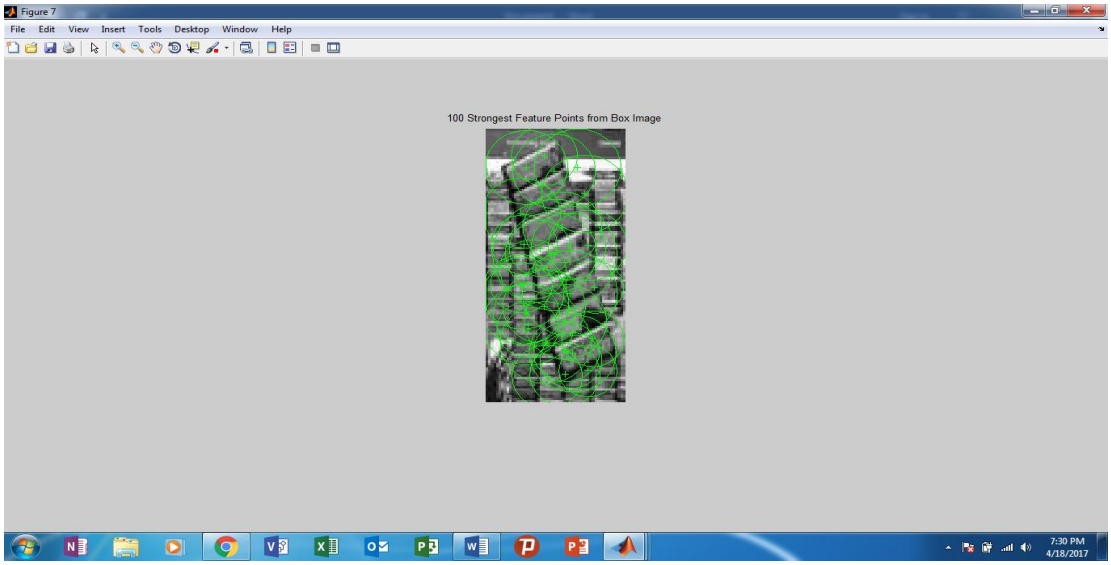

Figure 4.7 Feature Point of the Forged Part of Image

Figure 4.7 shows the feature point of forged part of image. as it is just a part of image hence only 100 feature points are calculated. Feature points are basically the points of images that are invariant under changes like zooming, lightning condition etc. in our proposed work, SURF algorithm is used to extract the feature points of image.

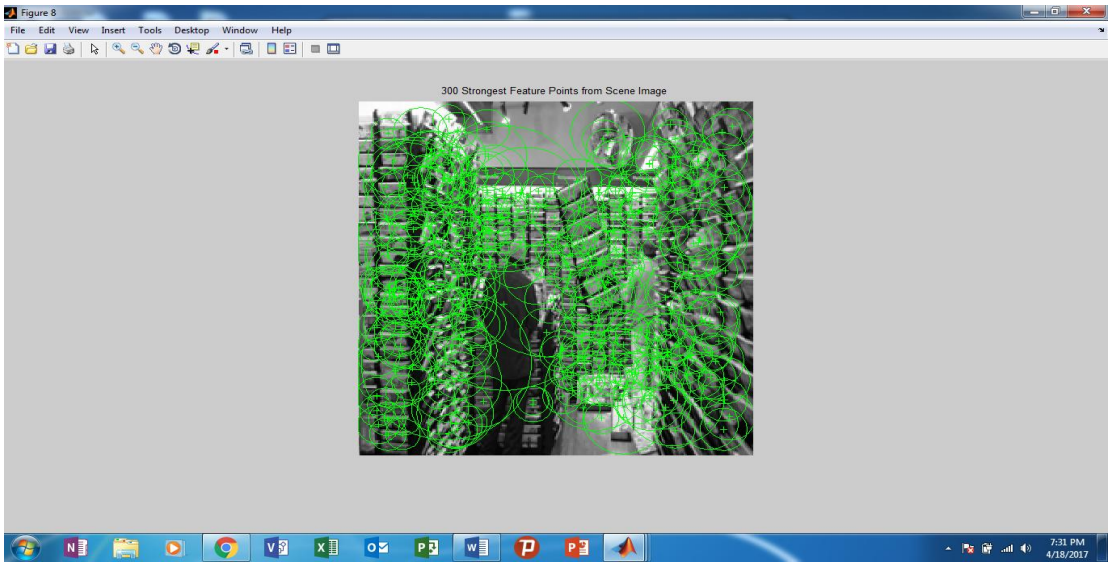

Figure 4.8 Feature Point from Scene Image

Figure 4.8 shows the feature point of forged part of image. as it is complete image including forged part of image hence more number of feature points are extracted. 300 feature points are calculated in this image. Feature points are basically the points of images that are invariant under changes like zooming, lightning condition etc. in our proposed work, SURF algorithm is used to extract the feature points of image.

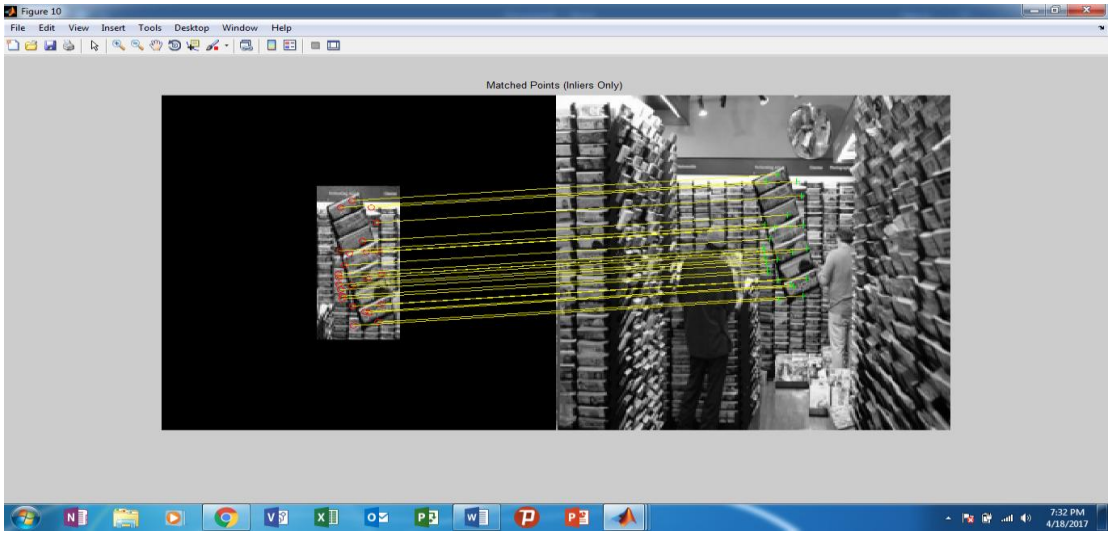

Figure 4.9 Matched Points Inliers Only

Figure 4.10, this image shows the matched key points including inliers key points only. The matched key points including outliers are not displayed. Hence the more focus is on the forged part of the image rather than containing all the key points.

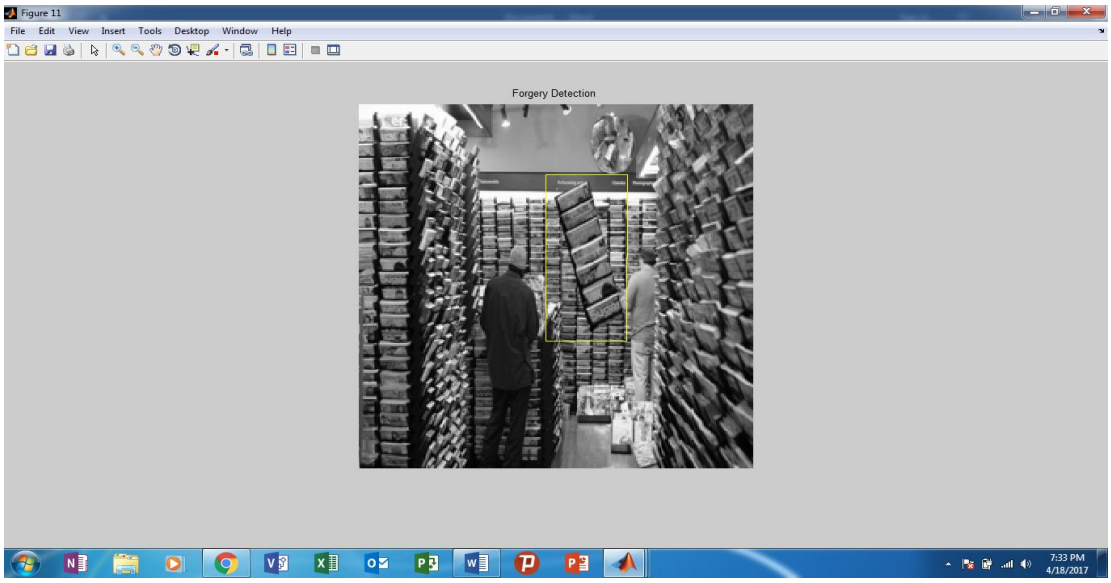

Figure 4.10: Forgery Detected

Figure 4.11, this is the final step of detecting the forgery. this image is the actual forged part of image in the target image. the forged part of image is highlighted with the red boundary of rectangle so that it becomes easy to see the forged part of image over the whole image.

4.3 GRAPHS

Image graphs is the collection of several functions to make and visualize graphs based on pixel neighbor relationship in an image. the images can be represented in any type of chart like bar chart, pie chart, or any type of 2D or 3D chart. In our work, we have used bar chart to represent the various parameters of image like precision, recall, F1 running time.

The value of these parameters is compared with the result of existing techniques. This is shown with the help of following graphs.

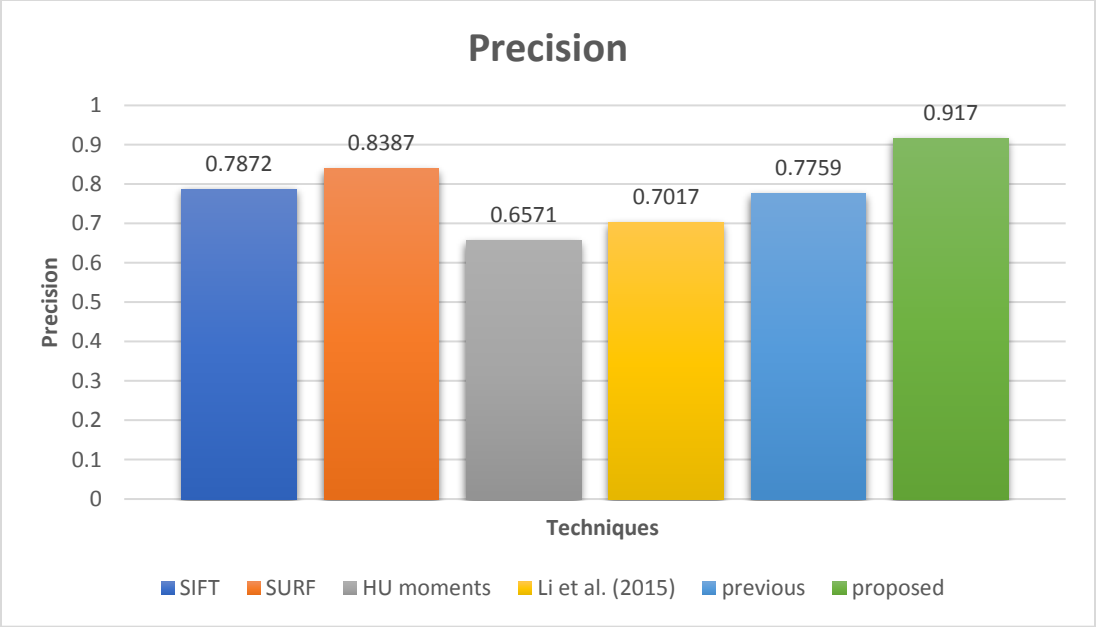

Figure 4.11 Precision Value

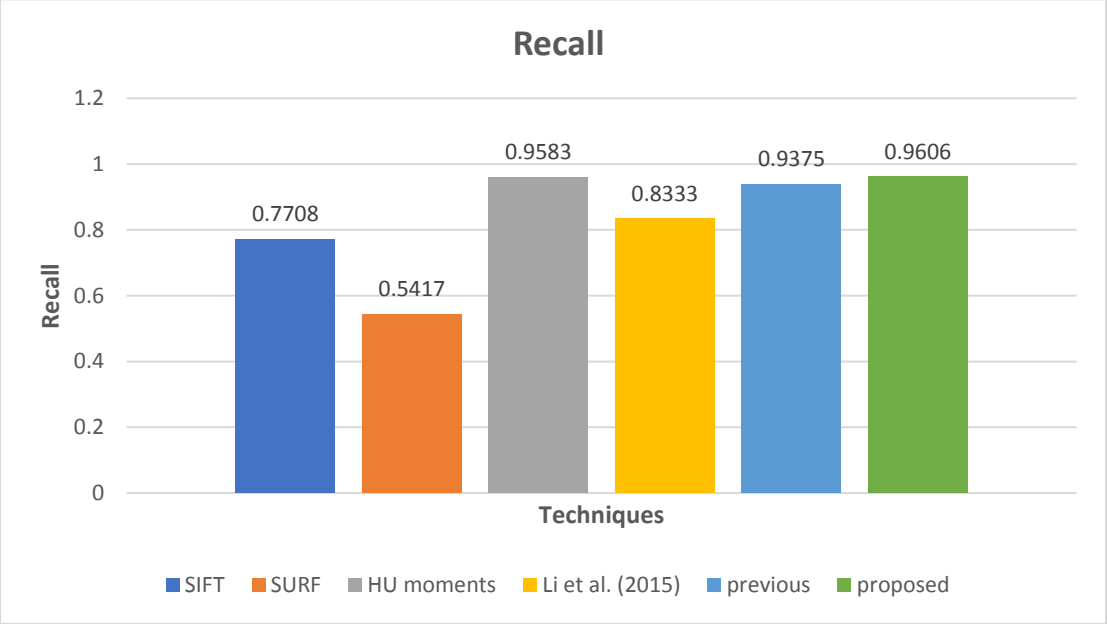

Figure 4.12 Recall Value

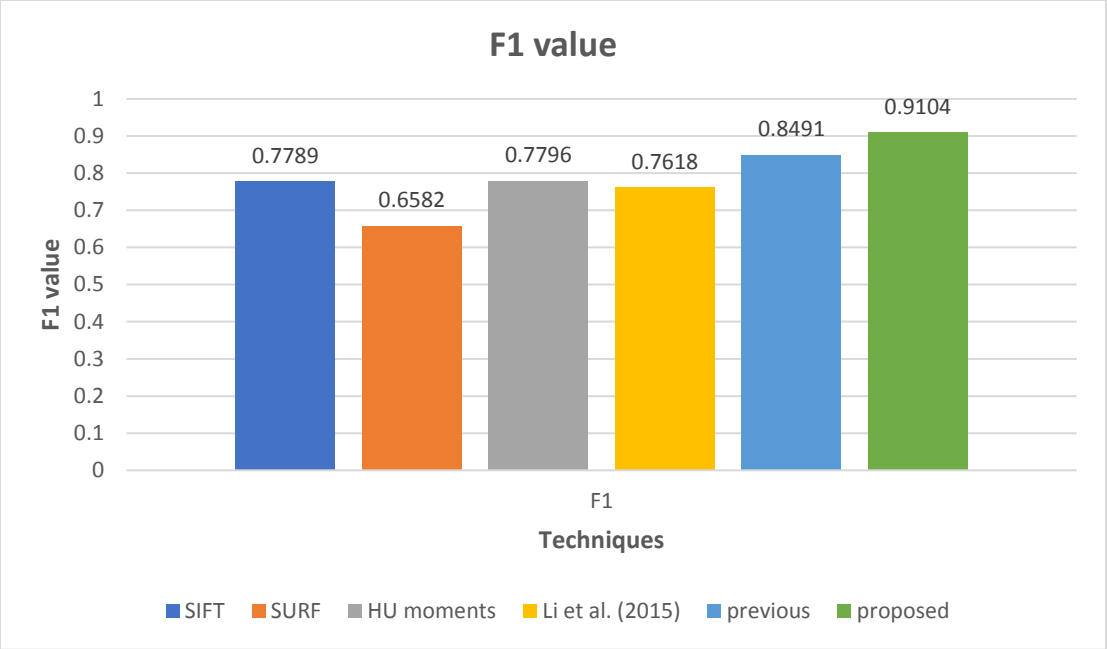

Figure 4.13: F1 value

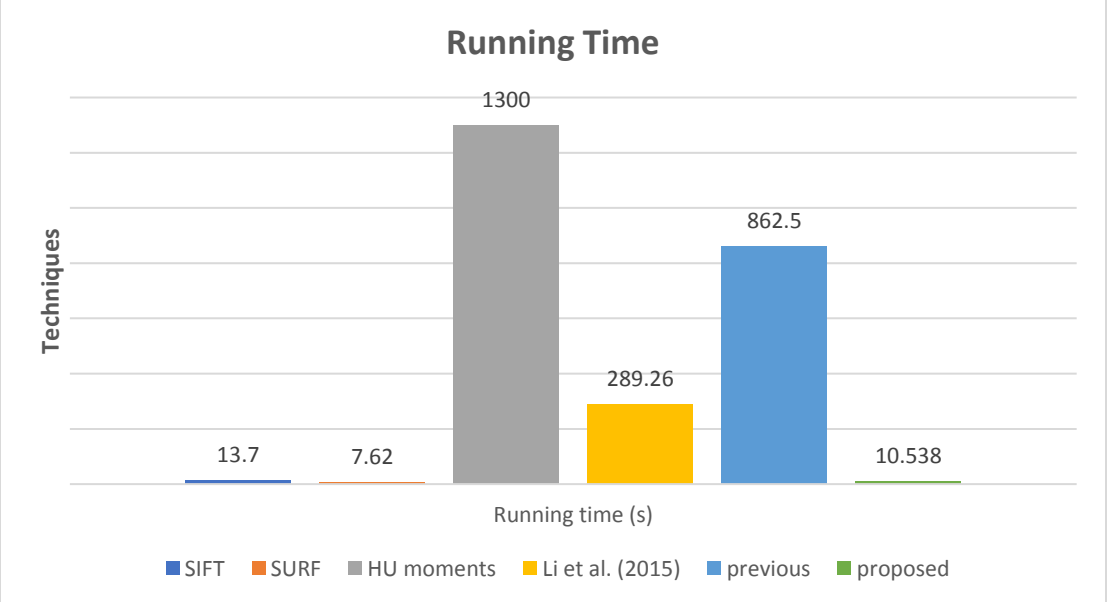

Figure 4.14: Running time

COMPARISON OF PARAMETERS OVER VARIOUS TECHNIQUES

Table 4.1: Comparison of Various Parameters

Parameters / Techniques	PRECISION	RECALL	F1	RUNNING TIME(S)
SIFT	0.7872	0.7708	0.7789	13.7
SURF	0.8387	0.5417	0.6582	7.62
HU MOMENTS	0.6571	0.9583	0.7796	1300
LI.ET.AL	0.7017	0.8333	0.7618	289.26
PREVIOUS	0.7759	0.9375	0.8491	862.5
PROPOSED	0.9090	0.9565	0.9321	10.538

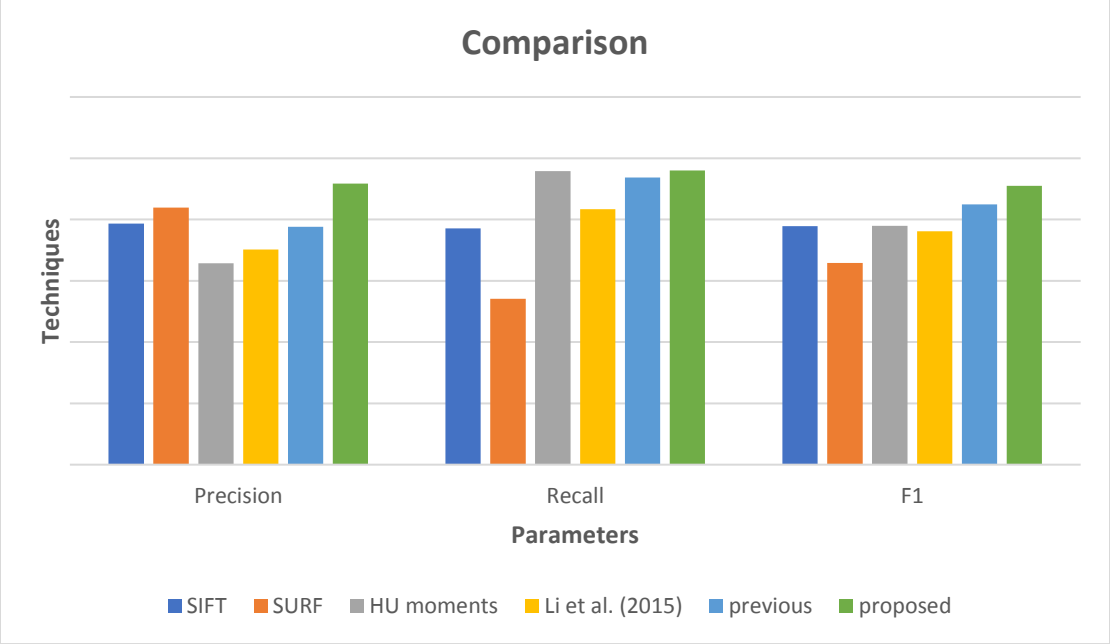

Figure 4.15 Comparison of Various Parameters

CHAPTER 5

CONCLUSION & FUTURE SCOPE

6.1 CONCLUSION

In our proposed work, we have discussed about image tempering, approaches to temper the image, how tempered images can be recognized, forensic image analysis, and what tools and methods used to distinguish the tempered image. We have examined impacts of tempered image in our general community. The aim of the work is to recognize the tempered image by utilizing some procedure. In our proposed work, we have used combination of different strategies SIFT, LBP and KOLMOGROV SMIRNOV in order to get more optimized result in proper time. SIFT technique is used extract the various image key points. These image key points are then matched with the target image for finding changes performed in the target image. the matching key points describes the forged part of the image. then LBP and KOLMOGROV SMIRNOV techniques is used to find the distance between the various blocks of image that helps to find the more accurate result. These techniques help in increasing accuracy of detecting forgeries and also decrease the running to perform the computation.

6.2 FUTURE SCOPE

Digital images are very common source for communication in today's world. Earlier the images were used as the evidence for some event but now-a-days due to advancement of technology the images are altered according to need. Thus, digital image authentication has increased. Copy-move forgery is the most common and easy way to temper an image. Copy-move is easy to perform but it could be easily detected by the eyes so to make this forgery undetectable various operations are made on the image.

In the future scope of this study the other types of forgeries can be detected like splicing, cut paste forgery etc. the accuracy can be more achieved in future. The technique can be checked on more images and more datasets. The time to detect forgery can be reduced more in future to get the optimized result in better way and in less time.

REFERENCES

[1] M. D. Ansari, S. P. Ghrera, V. Tyagi, M. D. Ansari, S. P. Ghrera, and V. Tyagi, "Pixel-Based Image Forgery Detection : A Review Pixel-Based Image Forgery Detection : A Review," *IETE J. Educ.*, vol. 55, no. 1, pp. 40–46, 2016.

[2] G. B. Chittapur and B. S. Anami, "comparison and analysis of photo image forgery detection techniques," no. 6, pp. 45–56, 2012.

[3] H. Farid, "Image Forgery Detection ," no. March, pp. 16–25, 2009.

[4] G. K. S. Gaharwar, P. V. V Nath, and R. D. Gaharwar, "comprehensive study of different types image forgeries," pp. 146–151.

[5] C. S. Gupta, M. T. Scholar, F. Detection, and C. Forgery, "' A Review on Splicing Image Forgery Detection Techniques ,'" vol. 6, no. 2, pp. 262–271, 2016.

[6] R. B. Hanji and V. S. Rajpurohit, "Forensic Image Analysis - A Frame work," pp. 13–19, 2013.

[7] A. Jagtap and H. A. Hingoliwala, "Survey Paper on Advanced Techniques for Image Forgery Detection," vol. 4, no. 12, pp. 2014–2016, 2015.

[8] A. E. V. J. A. Karthick, "Forensic Technique for Detecting Tamper in Digital Image Compression," vol. 2, no. 3, 2013.

[9] D. N.Pande, A. R. Bhagat Patil, and A. S. Bhattacharya, "Detection of Image Tampering over Diverse information Security Schemata: A State-of-the-Art," *Int. J. Comput. Appl.*, vol. 89, no. 2, pp. 35–47, 2014.

[10] N. Parashar and N. Tiwari, "A Survey Of Digital Image Tampering Techniques," vol. 8, no. 10, pp. 91–96, 2015.

[11] M. Rajawat and D. S. Tomar, "A Secure Watermarking and Tempering Detection Technique Using 2 Level DWT," vol. 1, no. 1, pp. 7–16, 2014.

[12] G. Sahu and U. Kiran, "Survey of Different Techniques for Image Tamper Detection on Digital Images," *Int. J. Adv. Res. Comput. Eng. Technol. (*, vol. 2, no. 12, pp. 3215–3218, 2013.

[13] D. Sharma and P. Abrol, “Digital Image Tampering – A Threat to Security Management,” vol. 2, no. 10, pp. 4120–4123, 2013.

[14] N. Singhal and S. Gandhani, “Analysis of Copy-move Forgery Image Forensics : A Review,” vol. 8, no. 7, pp. 265–272, 2015..

[15] S. Baboo, C. Applications, C. Applications, and C. Forgery, “Detection of Region Duplication Forgery in Digital Images Using SURF,” vol. 8, no. 4, pp. 199–205, 2011.

[16] M. M. Fegade, “Image Forensics for Forgery Detection using Contrast Enhancement and 3D Lighting,” pp. 257–260.

[17] J. Zheng, Y. Liu, J. Ren, T. Zhu, Y. Yan, and H. Yang, “Fusion of block and keypoints based approaches for effective copy-move image forgery detection,” *Multidimens. Syst. Signal Process.*, 2016.

[18] S. Sodhi, “Surf Technique for Copy Move Forgery Detection,” vol. 2, no. Icaet, pp. 10–12, 2016.

[19] G. Zhang and H. Wang, “SURF-based Detection of Copy-Move Forgery in Flat Region,” vol. 4, pp. 521–529, 2012.

[20] L. Kabbai and A. Douik, “Image Matching Based on LBP and SIFT Descriptor.”

[21] L. Suresh and P. S. Kumar, “Image Forgery Detection Using Adaptive over,” pp. 11544–11550, 2016.

[22] V. Agarwal, “Reflective SIFT for Improving the Detection of Copy- Move Image Forgery,” pp. 84–88, 2016.

[23] R. V Roy, “image forgery detection using adaptive over segmentation and feature point matching,” vol. 4, no. 4, pp. 640–643, 2016.

[24] A. Dada, R. V Dharaskar, and V. M. Thakare, “A Survey on Keypoint Based Copy-Paste Forgery Detection Techniques,” *Procedia - Procedia Comput. Sci.*, vol. 78, no. December 2015, pp. 61–67, 2016.

[25] H. Moradi-gharghani and M. Nasri, “A New Block-based Copy-Move Forgery Detection Method in Digital Images,” pp. 1208–1212, 2016.

[26] D. P. Patil, “Forensic Technique for Detecting Image Tampering using Statistical Intrinsic Fingerprints- A Survey,” vol. 920, no. 3, pp. 919–920, 2014.

[27] K. Kiruthika, S. D. Mahalakshmi, and K. Vijayalakshmi, “Detecting Multiple Copies of Copy-Move Forgery Based on SURF,” vol. 3, no. 3, pp. 2276–2281, 2014.

[28] P. Mishra, N. Mishra, S. Sharma, and R. Patel, “Region Duplication Forgery Detection Technique Based on SURF and HAC,” pp. 1–12, 2017.

[29] B. R. Reddy and P. R. Kumar, “Image Forgery Detection Using Adaptive Over Segmentation and Feature Point Matching,” vol. 3, no. 4, pp. 305–310, 2016.

[30] M. Singh and E. H. Singh, “Detection of Cloning Forgery Images using SURF + DWT and PCA,” pp. 1–10, 2016.

[31] X. Bi, C. Pun, and X. Yuan, “Adaptive Polar based Filtering Method for Image Copy-Move Forgery Detection,” pp. 953–957, 2016.

[32] N. R. Shenoy, C. Kamala, and K. Vindhya, “a matlab gui : designed to perform basic image processing operations,” pp. 88–96.

[33] P. G. Student, “Feature Extraction and Adaptive Over,” pp. 14723–14729, 2016.

[34] B. Liu, C. Pun, and X. Yuan, “Digital Image Forgery Detection Using JPEG Features and Local Noise Discrepancies,” vol. 2014, 2014.

[35] A. M. Venitta and V. S. Kumari, “Matching,” vol. 5, no. 3, pp. 21–31, 2016.

[36] G. S. Chandel, “Analysis of Image Segmentation Algorithms Using MATLAB,” vol. 1, no. 1, 2012.

[37] A. Gupta, N. Saxena, and S. K. Vasistha, “Detecting Copy move Forgery using DCT,” vol. 3, no. 5, pp. 3–6, 2013.

[38] J. K. Dhillon and J. Rani, “Detecting the Image Forgery from Color Images Using SURF and DWT,” vol. 6, no. 1, pp. 363–367, 2016.

[39] I. Amerini, L. Ballan, S. Member, R. Caldelli, A. Del Bimbo, and G. Serra, “A SIFT-based forensic method for copy-move attack detection and transformation recovery,” pp. 1–12, 2011.