A SUPER-SIFT APPROACH FOR COPY-MOVE FORGERY DETECTION

A Dissertation submitted in partial fulfillment of the requirement For the
Award of Degree of

MASTER OF TECHNOLOGY IN
INFORMATION SYSTEM

Submitted by

DEEPAK
(2K15/ISY/08)

Under the guidance of

Ms Ritu Agarwal
Assistant Professor

Department of Information Technology
Delhi Technological University
Bawana Road, Delhi-110042
2015-2017

CERTIFICATE

This is to certify that Mr. Deepak (2K15/ISY/08) has carried out the major project titled “Super-Sift Approach for Copy-Move Forgery Detection” as a partial requirement for the award of Master of Technology degree in Information Systems by Delhi Technological University.

The major project is a bona fide piece of work carried out and completed under my supervision and guidance during the academic session 2015-2017. The matter contained in this report has not been submitted elsewhere for the award of any other degree.

(Project Guide)
Ms. Ritu Agarwal
Assistant Professor
Department of Information Technology
Delhi Technological University
Bawana Road, Delhi-110042

ACKNOWLEDGEMENT

I express my gratitude to my major project guide Ms. Ritu Agarwal, Assistant Professor in Department of Information Technology at Delhi Technological University, Delhi for the valuable support and guidance she provided in making this major project. It is my pleasure to record my sincere thanks to my respected guide for her constructive criticism, interminable encouragement and valuable insight without which the project would not have shaped as it has.

I humbly extend my word of gratitude to Dr. Kapil Sharma, Head of Department and all the other faculty members and staff of department for providing their valuable help, time and facilities at the need of hour.

Deepak
Roll No. 2K15/ISY/08
M.Tech (Information System)
E-mail: deepakrao.619@gmail.com

ABSTRACT

Today's technological era is described by the outspread of digital images. They are the most ordinary formation of conveying information whether through newspapers, internet, books, magazine, scientific journals or social media. They are used as a powerful proof against various crimes, frauds and as an evidence in various situations. With the evolution of image processing in past few years and many other image editing software, capturing, creating or altering images according to our perspective has become very simple and available. There are several kinds of image tampering like copy-move forgery, image enhancement, image splicing, image morphing, image retouching whereas copy-move forgery is the most frequent and trendy manipulation of digital images. In copy move forgery here, a part of particular image is copied and then pasted into that same image with the motive of veiling some important object or displaying a fictitious scenario. Because the duplicate or in other terms the copied portion comes from the same image, All the image properties like texture, noise, resolution, brightness, contrast will be suited with the original portion of the image making it more difficult for the experts to distinguish and detect the alteration. There are mostly two kinds of forgery detection techniques one is block based method and the other is based on key points. In past few years feature based approach like SIFT gain attention of researchers in the field of image forgery detection.

I proposed a SUPER-SIFT method for copy move forgery detection. This work improves the fundamental concept of SIFT algorithm which is Feature Extraction. We use SISR for improving the quality of image. The proposed work consist of three main tasks, firstly we preprocess the input image with SISR algorithm to get a high resolution image. Then on high resolution image we apply SIFT algorithm for keypoint detection. After that we apply a fast potential based hierarchical agglomerative clustering method on the output of previous step to filter out the false matches and to groups the key points that have the same affine transform. On the basis of number of key points in a particular cluster, it can be said that the image having forgery or not. The experimental outcome shows that the proposed approach for the detection of copy-move forgery is efficient and powerful even when the copied portion undergoes various transformations like rotation, shearing, scaling or other post processing like adding noise and blurring.

Content

List of Figures

List of Tables & Graphs

Chapter-1 Introduction

1.1 Introduction

In the recent years, there is incredible growth in the use of elegant imaging tools, and these imaging tool makes it is very easy to create forged images by manipulating them. It is not so easy to identify that which one is genuine image of which one is altered. The widespread and offensive use of image tampering has become a critical mess now in many areas like news article, spying systems, medical science, research publications, media business and many more. There is emergence of digital data due to the widespread and common use of smartphones and social networking sites. Confirming the authenticity and the integrity of this digital data is very essential in above application. There are several methods which authenticate the digital images and also detect the manipulation done in the images.

Since images are instantaneous and their content can be easily understood - a privilege that is not found in texts - they are considered effective for human communication. Pictorial information can be easily obtained by human visual system damn faster than other kind of information. Such kind of information shapes approximately 75% of the information recognize by the human visual system. The use of such pictorial information has increased and has become easier due to advances in digital photography.

As we all know Nowadays, various applications depends on digital images. These include social media, newspapers, scientific Journals, magazines, medical science, fashion industry, courtrooms and many others.

Today, with easy availability of cost effective devices everybody can capture, store and share a huge amount of digital images that enables the accession of visual data. At the same time, image manipulation tools are commonly available which makes the task of manipulating the content of the image very simple. Currently available tools permits users to frame computer graphics that can not be figure out from real photograph. Such kind of evolution force us to know the answer of following question related to image forensic :-

These questions are:

- How is such an image captured?
- Is such image captured using digital devices such as a camera or a scanner or is it produced with the help of computer software?
- Is the image legitimate or has it gone through any kind of alteration after it has been captured?

In order to answer such forensic questions, the authenticity of the digital images has to be traced and related to its creation process. Such questions have led to the emergence and development of the area of image forensic over the past decade. Digital image's Forensic analysis proved to be helpful in providing information for many fields such as law enforcement, security and intelligence agencies.

1.2 Background on Digital Images

The basic unit of an image is pixel which is formed by combination of picture and elements. The pixels are arranged in such a manner and are brightened and coloured individually to generate a digital image. To represent a coloured image there is a need of three 8-bit numbers whereas each eight bit corresponds to RGB component that a particular pixel embodies. To represent a gray scale image no need of three 8-bit numbers it can be represented by only one 8-bit number to store the gray component in a pixel. Most Common representation is "M x N" for any image's resolution, where 'M', 'N' represents the pixels lies in horizontal and vertical directions respectively. Then the product "MxN" represents the total number of pixels in an image.

On the basis of format in which we use to store them, images can be classified into many categories like JPEG, PNG, TIFF, BMP. The selection of digital image format depends upon the application. For example, BMP and TIFF image formats use a lossless compression technique. That is, in compression process the above formats do not discard any information, thus there is no degradation in image quality over a smaller file size.

At present, the use of digitalization and computerization can be seen everywhere because technology have reached heights of development. Information is mostly conveyed through digital images and videos as the growth of digital devices and technology have incremented. Digital images doesn't hold the unique stature due to wide available range of image-editing software and advancement in processing techniques, as a result, image forgeries have increased at an alarming rate. Images are manipulated in diverse areas as in journalism, forensic investigation, medical imaging etc which have earn lots of attention by researchers. These have resulted into development of techniques to find images that are forged. Creation of many kinds of image forgery has become easy with the help of techniques used in image processing. Therefore, it calls for development of more new and powerful methods for detecting copy move forgery. Image authentication is a vital and important issue of multimedia security which has attracted lots of attention. Among the available technologies for forgery detection, the division can be of two kinds, active and passive. The former needs a prior knowledge to detect the authenticity of an image like digital watermarking where we feed some information prior to detection, whereas the latter performs the same work without any information. It utilizes the distinct properties of original images or changed traces to perform authentication.

1.3 Digital Image Forgery

Image forgery is changing, deleting, or adding some deciding and key features to an image from another image or within the image without leaving any evident trace[1]. At present there are many software are available free of cost on internet which plays crucial role in producing forged image. There are many ways by which images can be manipulated. Based on the ways how the images were manipulated, mainly digital image forgery is categorized into following types:

1.3.1 Copy Move Forgery

Such kind of forgery based on the copy-paste technique here the forgery is done by copying a particular object of portion of an image and then pasting that duplicate portion somewhere in that same image itself to create duplicate portions in that image or to hide some crucial image information. Unlike other type of image forgery for example image splicing, genuine and copied parts both are in the same image itself. In Fig1.1, here the missile part is copied from same image and then pasted to same image itself, creating a different look than the original image . Different post- processing techniques like re-sampling, blurring are applied to make forgery disappear.

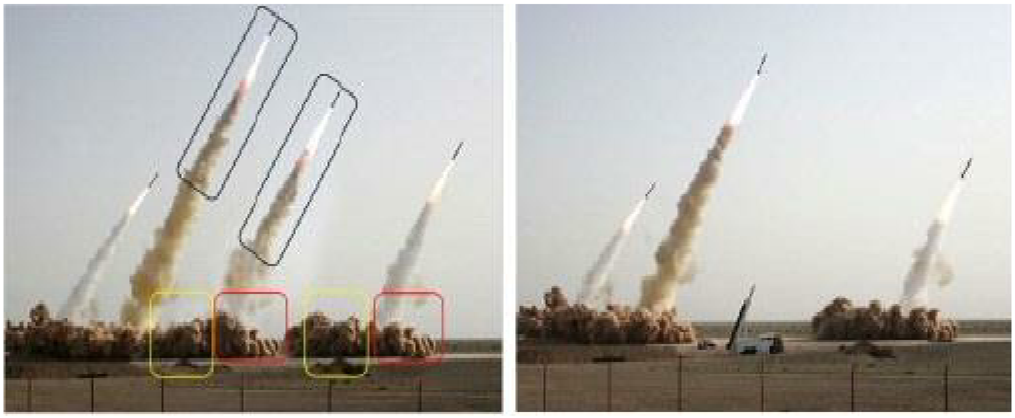


Fig 1.1 Example of Copy Move Forgery

1.3.2 Image Splicing

In Image splicing same cut-and-paste technique is used but in different manner to produce a different dummy image by using two or more than two legitimate images. Here the spliced portion can visually be unnoticeable if the splicing operation is performed very carefully.

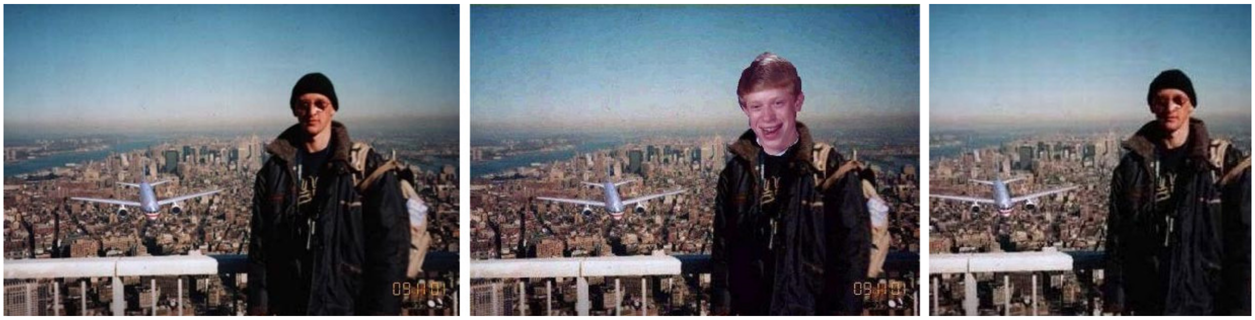


Fig 1.2 Example of Image Splicing

1.3.3 Image Resampling

Geometric transformation like stretching, scaling, flipping, rotation, skewing will be performed on some selected image regions for creating high quality image which is forged one. It is basic technique to make other forgery operations more effective and imperceptible. Resizing is the most commonly used operation applied in any forgery. Suppose we are creating a complex image of two people not from same images, resizing is necessary to maintain their relative heights

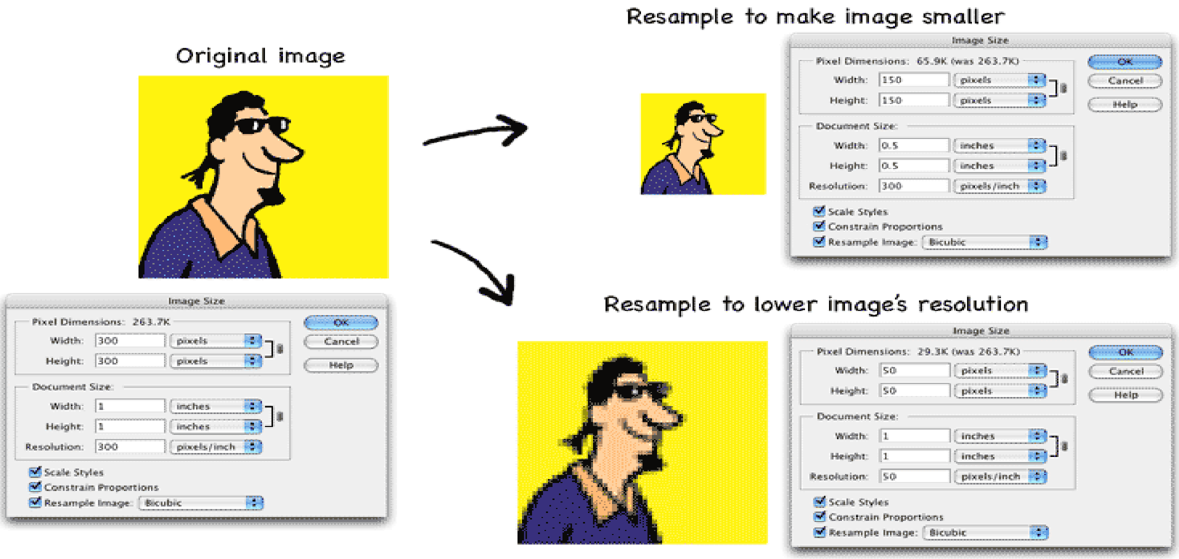

Original image
Resample to make image smaller
Resample to lower image's resolution
OK
Cancel
Help

Image Size

Pixel Dimensions: 263.7K
Width: 300 pixels
Height: 300 pixels
Document Size:
Width: 1 inches
Height: 1 inches
Resolution: 300 pixels/inch
☑ Scale Styles
☑ Constrain Proportions
☑ Resample Image: Bicubic

Image Size

Pixel Dimensions: 65.9K (was 263.7K)
Width: 150 pixels
Height: 150 pixels
Document Size:
Width: 0.5 inches
Height: 0.5 inches
Resolution: 300 pixels/inch
☑ Scale Styles
☑ Constrain Proportions
☑ Resample Image: Bicubic

Image Size

Pixel Dimensions: 29.3K (was 263.7K)
Width: 50 pixels
Height: 50 pixels
Document Size:
Width: 1 inches
Height: 1 inches
Resolution: 50 pixels/inch
☑ Scale Styles
☑ Constrain Proportions
☑ Resample Image: Bicubic

Fig 1.3 Example of Image Resampling

1.3.4 Image Enhancing

Enhancing an image such as blur, saturation and tone etc with any image editing tool like photoshop is called image enhancing. The appearance and meaning of image does not change by these enhancement. But Still, there is slight change in the image interpretation.

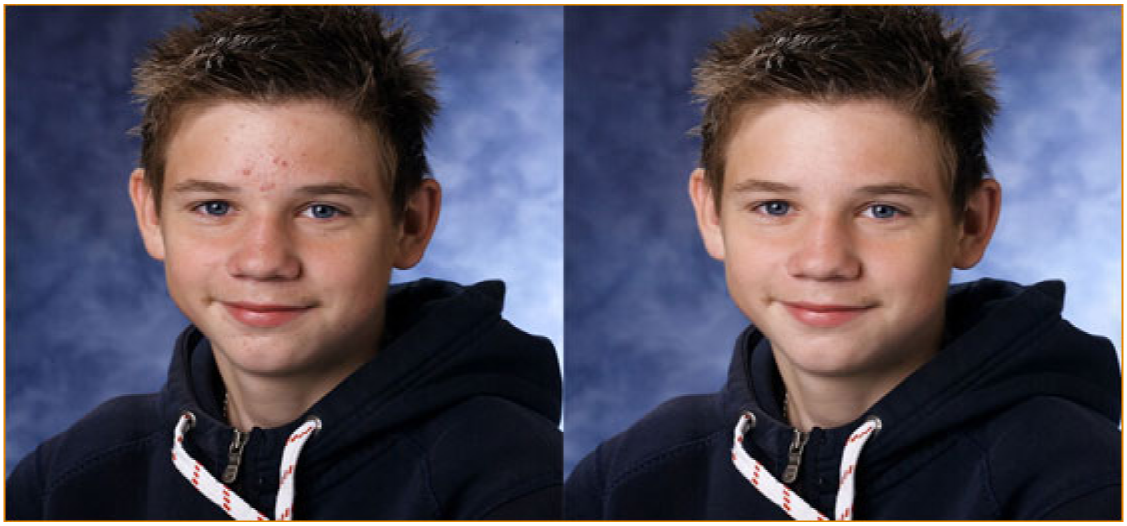


Fig 1.4 Example of Image Enhancement

1.3.5 Image Morphing

Transforming one image into another one by using some smooth transition or by other digital techniques between those two images is called image morphing. Most oftenly morphing of an image is used to portray one individual turning into another individual.

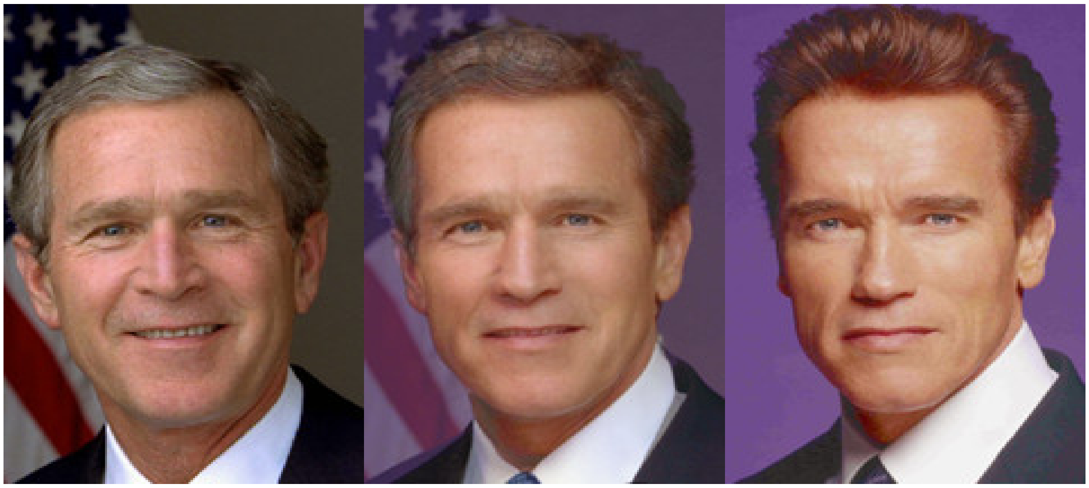


Fig 1.5 Example of Image Morphing

1.4 Image Forgery Detection

This is one of the hot topic of research in digital image forensic to detect any kind of image forgery. As we all know we due to digitalization and computerization can be seen everywhere because technology have reached heights of development. Information is mostly conveyed through digital images and videos as the growth of digital devices and technology have incremented. Therefore, the main goal of digital image forensic is to verify that the particular image is legitimate or not.

The intentional alteration of images to manipulate the visual message in that image is digital image forgery. Not every alteration on image is image forgery. There are various operation like rotation, cropping etc, are commonly used and accepted since they performed some changes but that is not a image forgery. Because nowadays, digital images are used for various purposes and in some cases they can be used as an evidence in courts. So, in the field of image forgery detection it should be our main goal to verify the authenticity of an image.

1.5 Digital Image Forgery Detection Methods

Image forensics approaches falls under two categories.

1.5.1 Active Approach: in this approach for proving the legitimacy of an image there is a need of some watermark or digital signature embedded with the genuine image, in such a manner that those watermarks and digital signature does not affect the meaning of image[2][3]. The main problem or we can say that the limitation with this active approach is that those operation must be performed by authorized person.

1.5.2 Passive Approach: or blind approach is like catching a thief. By finding that there are some marks and some statistical change left by the tool or person who manipulate that image, We can further proceed to detect the image forgery. Unlike active methods, blind approach doesn't require any information regarding authentic image. Blind forensics detection is categorized into following types which are explained below.

1.5.2.1 Pixel-Based Techniques

For CMFD the Statistical changes at the pixel level can also be used. At pixel-level, different correlations that occur due to specific type of forgery are analyzed and examined either in spatial or in some transformed domain. A forensic method may use intrinsic fingerprint of each encoder belonging to. Image coding detector can detect exact image encoder among sub band encoders, DPCM encoders and transform based encoder by the use of intrinsic fingerprint. A group of forensic methods came into existence which was capable to detect local as well as global contrast enhancement. It may also identify where to use histogram equalization and when to not. Key point based method like that of SIFT features are executed very efficiently. Feature based methods are very They are hypersensitive for low contrast regions and repeated content in the image[4]. Therefore, methods of block based criteria came into picture and they clearly brought improvement in performance. Techniques to encode words that are visual and features of indexing give an efficient solution to problems of detecting duplicate images. Histogram of oriented gradients which is a block based technique uses quantization which is non uniform to create a feature for a single image block for detecting forgery purposes. This method executes by using method of encoding the distribution of the features belonging to image to work with patterns that are highly textured.

1.5.2.2 Camera-Based Techniques

During different stages of image processing, numerous artifacts are produced and need to be abused in order to detect tampering traces. Examination of these camera artifacts may include response of camera, color filter array, and chromatic aberration and sensor noise deficiency. Various digital cameras make use of a single sensor with CFA (color filter array). They then interpolate the color samples those are missed in order to get a color image of three channels. The interpolation produces correlations which are specific and which get destroyed when forgery is performed with any image. Interpolation of CFA is done to understand these correlations and quantify them in any region of image[5]. The processing of single chip camera is related to demosaicing regularity. It follows a correlation model which is based on partial second order to detect intra-color as well as demos icing correlations in cross channel. Also a reverse technique of classification is employed for classification of demos iced samples into smaller ones which reveals the original grouping accurately. For this, an EMRC algorithm is executed to resolve the ambiguous demosaiced axes. There also exists unified approach to detect source camera from its images and identifying any alterations using PRNU(Photo-Response Non Uniformity Noise). It is the imaginary fingerprint which is unique to imaging sensors. An estimator to estimate maximum likelihood is used to obtain PRNU. Both the above mentioned tasks of digital forensics are achieved by detecting the existence of sensor PRNU under regions of investigation. The process of detection of manipulations in images works by analyzing a patch of image to decide whether it belongs to a category of authentic or spliced ones. Fusion Boost was incorporated by learning the weight of each classifier in order to construct a strong ensemble detector. The forgery detection based on PRNU works by using the Bayesian Framework to recast the problem, and then accounting for spatial dependencies of decision variables when they are modeled as Markov random field.

1.5.2.3 Format-Based Techniques

Various correlations that occur during any compression methodology is examined to detect forgery. A method to examine low-quality JPEG images and then to detect the region which is compressed at lower level of quality in that image. The region of such a type is detected when the image is resaved at multitude of JPEG qualities and then tries to detects the local minima between JPEG compressed version and original image[5]. 1-D feature was introduced to detect whether a given bitmap image is JPEG compressed previously. The blind approach for detection which is based on estimation of quantization is executed in three steps: pre-screening, selection of candidate region, and then identification of tampered region. Pre screening test is done to detect if the image is JPEG compressed or not. Then, for reducing the impact on tampered regions on quantization table, regions which act as candidate are selected for estimation of quantization table.

1.5.2.4 Geometric-Based Techniques

Here principles of projective geometry are applied to develop robust algorithm for detection. Abnormality in relative positions of an object or a person used to detect objects moved or translated in case of any forgery.

1.5.2.5 Source Camera Identification-Based Techniques

The source camera details can also be used to find out any kind of forgery. These details include sensor noise, color filter array interpolations and lens aberrations.

1.5.2.6 Physics-Based Techniques

While merging different photographs, matching lighting conditions is difficult. Light variations are used as evidence to detect tampering[4]. Inconsistency is detected in order to expose fakeness and used as an evidence of forgery. It performs approximation of lightning environment in low dimensional model and then estimates the parameters.

1.6 Research Objectives

The main objectives of this thesis are:

- To detect copy move forgery with high efficiency and with low computational cost.
- To improve feature extraction process which is the most important part of any CMFD technique.
- To improve the performance measures of proposed copy move forgery detection method.

1.7 Thesis Outline

This thesis is organized in six chapters.

Chapter 2 gives us literature review of currently available methods for CMFD. Here in this chapter literature related to CMFD is mentioned.

Chapter 3 gives the problem statement to better understand the challenges in this field of copy move forgery detection.

Chapter 4 contains detailed description and explanation for each step in the SUPER-SIFT approach. It begins with basic theory of the most important topics in the algorithm.

Chapter 5 demonstrates the results and analysis of our proposed approach. For analysis some comparisons with the other method are also provided.

Chapter 6 sums up the conclusion and future scope of related work.

Chapter 2 Literature Review

The main aim of CMFD is to disclose clone regions in the image, to the very slight difference in each of such regions. Image forensic is one of the hot topic of research as the digital data is growing so fastly over day by day. Because of this many experts and the people who are interesting in this research field published large number of journals and conference papers on CMFD, many of them are explained in our literature. This particular chapter gives us a review of currently available literature of relevant research. The literature is organized in such a way that It begins with a brief background of CMFD techniques, after that some previous works on CMFD are Then some of the previous studies are discussed.

2.1 CMFD Techniques

CMFD can be done very easily and effectively if some common forgery operations are used to can be implemented effectively and easily making it the most frequent forgery process which is used to change the image's content. But CMF is not just copy and paste one of multiple regions somewhere else in that image, it is bit smart work. In practical CMF, there are many other kind of image processing operation are also involved. These image processing operations are classified into mainly two groups

- **Intermediate processing :**These operation are used for providing some kind of analogy and spatial synchronization between the duplicate region and remaining image. Example of some intermediate processing operation are scaling, shearing, change in illumination, rotation, change in chrominance or mirroring etc. To make CMFD more complex sometimes intermediate processing may include a merger of two or more operations.
- **Post-processing:**These operations are mostly used for removing any kind of detectable traces of CMF operation, like removing sharp edges. JPEG compression, additive noise and blurring are the most common post processing operation. It is suggested that any of the CMFD algorithm should have to be vigorous to various kind of post processing operations.

Therefore, the following requirements must be available in any CMFD algorithm :

- The CMFD algorithm should efficiently detect the forgery even when the forgery size is small .
- The time complexity of CMFD algorithm should be reasonable, even after introducing false positives .
- It should be robust against any kind of Preprocessing or Postprocessing operation.

2.1.1 Types of Copy Move Forgery Detection Techniques

Copy Move Forgery Detection techniques are mainly categorized into two types:-

2.1.1.1 Block Based technique divides a particular image uniformly into rectangular, circular, hexagonal blocks. These blocks may be overlapping or nonoverlapping, but the size of the blocks should be fixed.

2.1.1.2 Keypoint Based technique extracts the key-points or simply say features of an image rather than dividing the image into blocks.

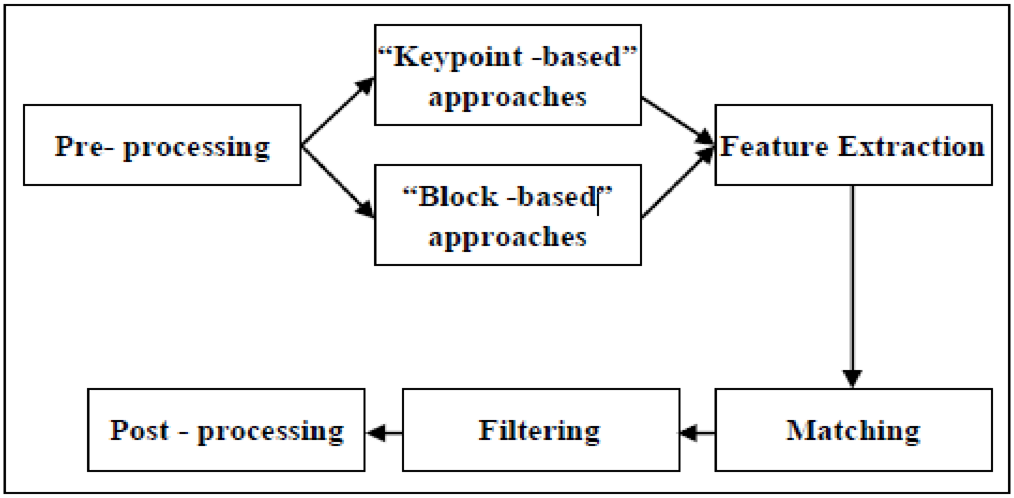


Fig 2.1 Common approach for CMFD.

The general steps involved in the process of CMFD[1] are as follows:

- **Preprocessing:** Simple preprocessing operation is just converting a color image into grayscale image. The aim of pre-processing is the improvement of image data that suppresses unwanted distortions or enhances some image features important for further detection.
- **Feature extraction:** This is the most important phase in the CMFD. The accuracy of CMFD technique depends how well the algorithm extracts image features. The way, how features are extracted is different for both type of CMFD methods whether it is block based or keypoint based. In block based CMFD, first step is to divide the given input image into fixed size segments or we can say that blocks. The division of blocks may be in overlapping manner or in non overlapping manner. Feature vector is then computed for each block. Afterwards, feature vectors which are similar are matched. But in case of key-points based CMFD, there is no such image subdivision like block based CMFD[1]. Here features of whole image are computed using available feature extraction algorithm like SIFT, SURF etc. with high entropy.
- **Matching:** High resemblance between two feature descriptors indicates that there is some duplicate region in the image. If we talk about Block based CMFD methods lexicographic sorting is used by most of the experts to identify similar feature vector. The basic concept of lexicographic sorting is to built a feature vector matrix so that each feature vector represents a particular row of that matrix [1]. After creating a 2-D matrix with all feature vectors each of them represents features of a particular block, the matrix is then sorted along with the direction of this row. As a result of this sorting, the consecutive rows contains the most similar features. In case of keypoint based CMFD method a technique which is derived from k-d tree which is called as Best-Bin-First and that is used to get a close nearest neighbour. Usually, the Euclidean distance is used as a similarity measure for duplicate region .

- **Filtering:**This is used to diminish the possibility of false matches generation. Similar intensities of neighboring pixels may lead to false forgery detection [1].

- **Post Processing:** After matching process is done to The main aim of this step is to safeguard those matches having common behavior is the main aim of this post processing. If we are talking about copied portion the set of matches belongs to it should be very close to both source and target block. Moreover, those match which came from same copy move operation should show identical measure of affine transform.

2.2 Literature Review

In literature, there are many CMFD techniques are explained on the basis of reviewing many research papers one by one that require a huge amount of time and effort. First of all, exhaustive search is the direct answer to this CMFD problem where the same image is compared with its all possible cyclic shifted version. But the main disadvantage of this approach is that it is computationally very expensive and would take M. N whole square steps for an image of size 'M × N'. Moreover, this exhaustive search might not work in the case of having modifications made on the copied area [6]. Other techniques which are explained in this chapter aim to minimize the time complexity and increase the efficiency of CMFD. The currently existing methods for CMFD differs from one another in terms of number of feature extracted, type of features used for matching the image blocks. Few of them are summarized below:

2.2.1 DCT-Based Methods

Among the initial attempts of CMFD, A DCT based CMFD technique is proposed by [8]. DCT coefficients of the image blocks are computed. The computation cost for calculating these coefficient is reasonable. Then these DCT coefficient are lexicographically sorted . After sorting, the adjacent identical blocks pairs are treated as CM blocks.

- **Drawback** of this CMFD method is that it is totally failed in detecting small duplicate regions.

An improved DCT based CMFD algorithm proposed by [9] which exhibits low computational complexity. Here in this approach the quantized blocks are characterized by circular blocks and this is how other DCT based and this proposed technique differs. The circular blocks are then further subdivided into a limited number of segments, for each such segment feature vectors are computed. Then after computation of feature vectors these are lexicographically sorted. Then the euclidean distance between the adjacent pairs of these sorted vectors is calculated. This improved DCT based CMFD method is quite suitable for finding multiple CM region, and robust against many post processing operation like additive noise and blurring but this method has very poor performance when image undergoes geometrical operation and with poor image quality.

A robust CMFD scheme which is a combination of DCT and SVD proposed by [10]. In first step image is divided into fixed size overlapping blocks. After this division of image 2D-DCT coefficients are computed and quantized into blocks. Now, from these quantized blocks we further divides into sub blocks which are in non overlapping manner. After that on each sub block SVD is applied. At last to reduce the block dimension features are extracted for each block to get a large singular value. Finally, these vectors are lexicographically sorted, and by using some predefined shift frequency threshold the duplicated image blocks are matched. By experimental outcomes proposed method can detect CMF even when there are some post processing operation like Noise, blurring, JPEG compression distorted the image.

2.2.2 PCA-based method

A Principal Component Analysis based CMFD method is proposed by Popescu and Farid [11]. First of all in this scheme, conversion of color images into grayscale and after this conversion these gray scale images are further separated into parts and these parts which corresponds to a particular block is represented by vectors. Afterward, lexicographical sorting is applied on these vectors and PCA technique is used to demonstrate the unmatched blocks in a alternate mode. This approach is capable of detecting even a minor variations resulting from wasted compression or noise . Moreover, for grayscale images PCA based approach is quite efficient for finding duplicate regions and it gives very less number of FP. Here in this approach total number of computations and the time complexity is reduced by O(Nt. N logN), where N represents no. of image pixels, Nt; is dimensionality of the truncated PCA representation. This approach performed well for large block size but the performance degrades when the block size is small and does not performed well for low JPEG qualities.

2.2.3 LBP-based method

Local Binary Pattern and neighborhood clustering based CMFD approach is proposed by Al-Sawadi [12], In this LBP based technique what they proposed is that, an input image is first break down into 3 color components. Afterwards, for each overlapping blocks of the 3 color component LBP histograms are calculated. Block-pairs are retained, those having the minimal histogram distance. If the retained block pairs are found in all of the 3 color component, then these are selected as primary candidate. To refine the candidate Eight-connected neighborhood clustering is applied. Experimental result of this proposed work shows improvisation in decreasing the FP rates over some recent CMFD methods. With rotation, scaling and other post processing operation on duplicate regions degrades the performance of this LBP based CMFD method.

2.2.4 Wavelet-Based Methods

A CMFD approach which uses DWT and DCT proposed by [13], this is an non intrusive approach for CMFD problem. Here what happens is the input image is break down into subbands by using DyWT into approximation (LL) subbands and detail (HH) subbands. On the overlapping blocks DCT is applied in LL and HH subbands, and in next step the Euclidean distances between these overlapping blocks are computed using DCT coefficients. Based on the similarity of blocks present in LL subband, and the dissimilarity of blocks present in HH subband decision is made. With dataset having images of different compression quality, size and with or without some transform like rotation before pasting the experimental outcomes shows that this proposed approach works well for CMFD.

2.2.5 Moment-Based Methods

A CMFD method is proposed by Zhong and Xu based on mixed moments. Here before subdividing the image into blocks, low frequency information of the image is extracted by using Gaussian pyramid transform. After this image is subdivided into equal size overlapping blocks. In second step, for each and every blocks the eigen vector composed by the histogram moments and exponent fourier moments are sorted lexicographically. Finally, tampered region was positioned accurately and instantly [14] according to the Euclidean and space distances . Moment based CMFD Experimental outcomes illustrate that moment based method can strongly finds the duplicate region even though there are other kind of manipulation with duplicate region like scaling, rotation, translation. This method is robust to contrast adjustment and variation in brightness. Drawback of this moment based method is that the qualitative evaluation, rotation angle and scaling factor are not mentioned.

2.2.6 Texture and Intensity-Based Methods

A texture based CMFD scheme was proposed by Quan and Zhang (2012). Firstly, this intrinsic dimension estimation approach segments the image and then try to find out the CMF in the regions inside the image having same texture[15]. This texture and intensity based method is robust and efficient to many post processing operation on forged regions like retouching, lossy compression, blurring etc.

2.2.7 Key point-Based Methods

A new image forgery detection method is proposed by Hsu and Wang (2012), based on Gabor filter. A Gabor feature representation for an image is generated with the help of gabor filter at different frequencies, with different rotation angle and with different scaling factor. Comparison of two images is done with their Gabor features; to find that is there any kind of analogy between them. Image is further subdivided into smaller blocks to reduce the processing time and to detect small CM area [16]. In each block, a new descriptor is extracted and key points from the Gabor feature of the block image are defined.

Amerini et al. (2014), proposed a novel approach which is combination of Scale Invariant Feature Transform for feature extraction, and localization based on the J-Linkage algorithm for CMFD. After extraction of SIFT features Feature vectors are calculated for an image. Afterwards, the matching process of these feature vectors is done with g2NN algorithm [17]. The matched vector's Coordinates are treated as successor for the clustering, these coordinates are then performed using J-linkage. Clustering result reveals the copied regions inside the image. This method is well suited for detecting all kind of forgery involving rotation and scaling because it uses SIFT features. This method is capable of detecting forgeries involving multiple duplications. This method works well for post-operations on forged region such as Gaussian blurring and JPEG compression.

A novel CMFD technique which uses an adaptive over segmentation method and key point matching is proposed by Chi-Man Pun. This is the fusion of both kinds of methods, block based forgery detection and keypoint based forgery detection methods. The initial step of the proposed method by them is to apply an adaptive over segmentation algorithm that divides the image into non overlapping and irregular blocks [18]. After that block features are extracted for each and every block, then one block features are matched with another block feature to locate the labeled feature points. this localization process can generally indicate the suspicious forgery regions. The experimental results indicate that proposed CMFD method can able to handle many post processing operation on forged region as compared to other CMFD methods such as DCT, PCA and other moment based methods.

Mohsen Jandi (2016), proposed a CMFD scheme that can accurately figure out copied regions within reasonable computational cost. Here in this technique, by utilizing the advantages of both keypoint and block based CMFD approaches a new interest point detector is proposed. Adaptively detected features cover the whole image based on a uniqueness metric[19], even there is a low contrast regions. To efficiently filter out the false positive a new filtering algorithm is proposed. Results of this approach outperforms many CMFD methods.

Chapter-3 Problem Statement

As we all know Creating digital image forgeries has become very easy either it's source is a single image or multiple images because of the availability and ease of powerful image molding tools, and various software, such as "Photoshop". By "Copy Move" forgery; it is based on the copy-paste technique here the forgery is done by copying a particular object of portion of an image and then pasting that duplicate portion somewhere in that same image itself to hide an important image information.

Most of the techniques for CMFD suffer from the issue of computational cost(beside other problems such as robustness to any post or preprocessing operation to deceive the detectors). This is because most of these algorithms divided the tested image into overlapped small blocks (for example 8 x8) shifted by one pixel to the right (or to the bottom). Then some kinds of features also known as keypoint are obtained from each such overlapped block. After the extraction of features these are compared to each other to find a set of resemble blocks. The described process takes a long time and any effort that aims to reduce this time is very important.

3. 1 Problems in Detecting Image Forgery

In this section, we describe some problems associated with image forgery detection.

3. 1. 1 Data Provenance

This is one of the key concern for protection of rights and sometimes as an administrative requirements in many application such as in medical science, financial transaction and other govt. legal pursuit. The data provenance is necessary in many daily situations, wherever the value and trustworthiness of information is mandatory.

One of the biggest threat to the digital information is the obsolescence of technology rather than the built in physical delicacy of digital media. The assumption of moore's law failed in case of development in technology in future, it is much faster than it was assumed. Because of such rapid development it is clear that the currently available technology, software, devices used for data creation, storage, retrieval is going to be replaced within 3-5 years. This makes makes the preservation of digital data and evidences a demanding issue [7].

3. 1. 2 Benchmarking and Standard dataset

The need of open data set is for realistic and some critical conditions such as digital document is required. Let us take an example of digital document like image with different size, different resolution, different camera model and with different types of possible tampering such as image splicing, CM forgery, image retouching, image morphing and other kind of manipulation like color adjustment, blurring, contrast adjustment and various other post processing operation like adding noise, image compression etc. Because of above discussion, the need for evolving benchmarks for forged dataset as well as genuine data set in order to use for experiment, evaluate, and understand the efficiency of the research. [7]. In our proposed research, we build a database containing both kinds of images, authentic as well as forged.

3. 1. 3 Duplicate Regions

The reason of the appearance of duplicate regions in an image is one of two things: first, the presence of two things or two objects with the same size, shape, and color; one of them may be a copy from the other one. Second, the presence of a relatively large area with one color and close in characteristics such as backgrounds (sky, wall, etc.) which leads to the appearance of duplicate regions in the results.

3. 2 Thesis Contribution

The contribution of the thesis is as follows:

- An efficient image forgery detection method based on Super Resolution, SIFT and PHA Clustering is proposed.
- The proposed methods are evaluated on many original and forged images with different types of copy move forgeries.
- We developed a database of more than 100 authentic images taken by different camera models, and added to this database different types of copy-move forged images based on the authentic images.

Chapter-4 Proposed Work

4.1 Proposed Framework

We proposed an efficient methodology to detect Copy-Move Forgery. The following flowchart illustrates the architecture of our approach.

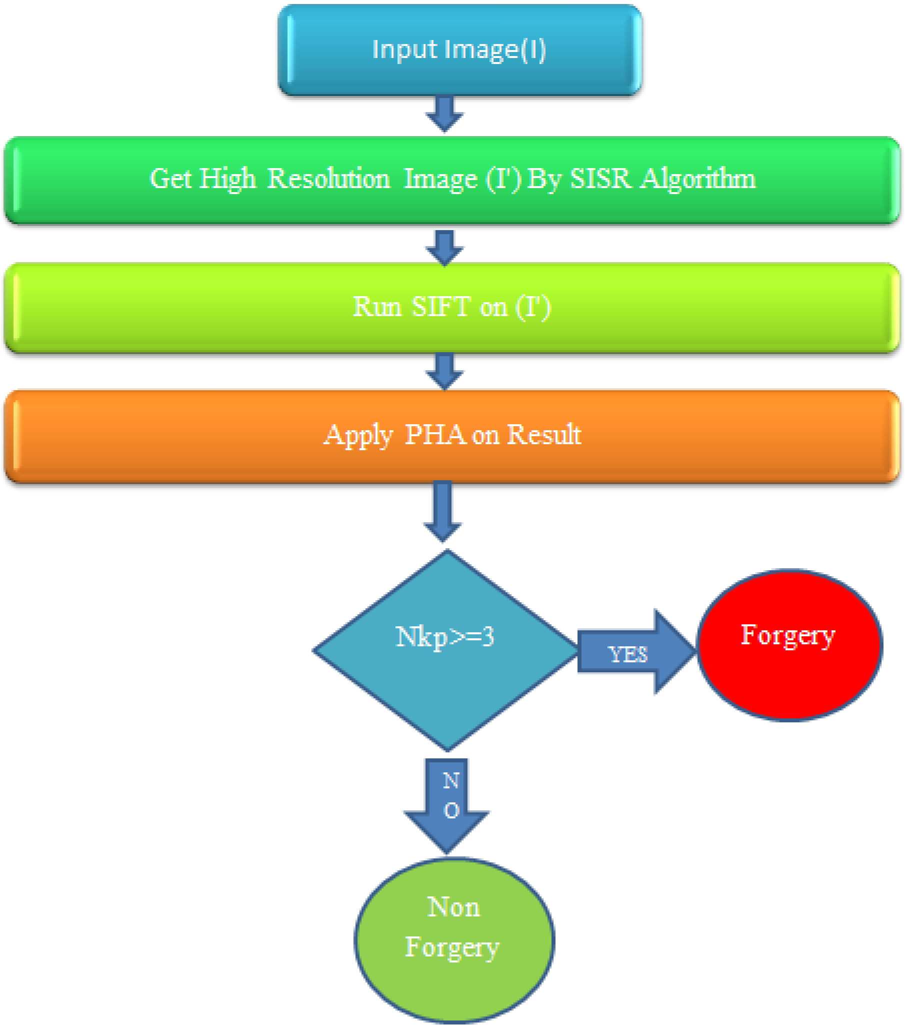


Fig 4. 1 Framework of Proposed Work

As per the first part of above proposed work, on the input test image **I** ; SISR (Single Image Super Resolution) algorithm is applied to produce a high resolution image **I'**. After getting high resolution image, a copy move forgery detection technique based on SIFT method is applied on that **I'** for feature extraction and matching process. Our proposed method **'SUPER-SIFT'** improves keypoint detection by using single image super resolution as a preprocessing step on input test image rather than applying SIFT method directly on input image. Now on the results of SIFT, we apply PHA clustering to filter out false matches and cluster those key points. Those keypoint having same affine transformation pattern are grouped into clusters. At last on the basis of number of key points in a particular cluster it can be said that the image having forgery or not. The detailed explanation for the proposed method is given below.

4. 1. 1 Single Image Super Resolution

SISR is technique by which high resolution image can be produced by taking a single low resolution image as input. By using local binary pattern feature the SISR algorithm interpolates the gradient field of LR images to get a finer gradient field. After that it iterates to the better gradient field term and constraint set to construct one reconstruction energy function [20]. Using gradient descent method a high resolution image can be generated by minimizing such energy equation.

4.1.1.1 Reconstruction Energy Function

First of all a single constraint set 'C' should be constructed which contains the pixels in low resolution image, which are directly copied to high resolution image. Constraint set is mainly used to maintain the high resolution detail in HR image.

Second thing is that, we interpolate gradient field of low resolution image to obtain high resolution gradient field 'V' . At last, via HR gradient field and the constraint set we can define our reconstruction energy function. The error between reconstructed high resolution image and ground truth can be determined by this energy function value approximately.

4.1.1.2 Energy Function Definition

The energy function could be defined by equation given below:

$$\begin{aligned} E(u) &= \frac{\mu}{2}\int_{\Omega} ||\nabla u(x) - V(x)||^2 dx \\ &+ \frac{\lambda}{2}\sum_{i\in C}\int_{\Omega} \phi(p_i)|u(x) - f(x)|^2 dx \end{aligned}$$

4. 1

$$where \quad \phi(p_i) = \delta(||x - p_i||) = \begin{cases} 1, & x = p_i \\ 0, & \text{otherwise} \end{cases}$$

4. 2

where ‘f’ is the HR image which is obtained just by copying LR image, the intensities of other pixels are set to be zero except simple corresponding pixels, and ‘u’ is HR image. Where i represents the index of constraints set C, pi is the position of a particular pixel i, and ui represents pixel value in the HR image and fi is the pixel value in image f at pixel i. First term describes that if the HR gradient field (V) is good enough then the reconstructed HR image is the same smoothness as ground truth. The second term restricts that the corresponding pixel intensities should be approximately equal. The first derivative of function E(u) can be solved as eq(4.1) by calculus of variation.

$$\frac{\partial E}{\partial u} = -\mu(\triangle u - div(V)) + \lambda\sum_{i\in C}\phi(p_i)(u - f)$$

4. 3

In the above equation Δ represents Laplacian and div represents the divergence operator respectively. Therefore, the image u that minimize the energy Eq. (4.1) satisfies the Euler-Lagrange equation ∂E /∂u = 0. Here steepest descent method is used to minimize the function and the following gradient flow is obtained:

$$\frac{\partial u}{\partial t} = \mu(\triangle u - div(V)) - \lambda \sum_{i \in C} \phi(p_i)(u - f)$$

4. 4

So we can define iteration as follows,

$$\begin{cases} u_{t+1} = u_t + \tau * \frac{\partial u}{\partial t} \\ u_0 \quad = \quad f_0 \end{cases}$$

4. 5

From a given single LR image, our goal is to generate a single HR image. The super resolution approach used in proposed work is composed of four stages which are as follows:

1) First step is to calculate gradient field $v = (x, y, v_x(x, y), v_y(x, y))$ of given input low resolution image 'f' by using Sobel operator, main advantage of using Sobel operator is that it is is less sensitive towards isolated high intensity point variations. This is because Sobel operator performs averaging of points over a larger area.

2) Second step is interpolating the LR gradient field. This is done with the interpolation on gradient field V by using bilinear interpolation method.

3) In third step we have to construct an energy function. Eq (4. 1) defines that energy function. The energy function is defined with constraint set and constructed HR gradient field.

4) In the final step after solving the energy equation we Obtained a sharp HR image by solving energy function using Eq. (4. 5).

4.1.2 Generating the image features

The Distinctive features which are invariant to image rotation, scaling and other affine transform and these features are robust against illumination, viewpoint, noise and other type of distortion of local image patches are extracted by SIFT algorithm [21]. This phase of feature extraction consists of 4 main steps which are explained below one by one:

4.1.2.1 Scale Space Extrema Detection

For an input image **I(x, y)**, feature extraction process which is the initial step, is to find out the extrema value over all possible scales and over entire locations of the image. Equation (5) defines scale space for an input image which is given below :-

$$L(x, y, \sigma) = G(x, y, \sigma) * I(x, y) \qquad 4.6$$

where; * represents convolution in both x, y directions,
G; is the Gaussian function

$$G(x, y, \sigma) = \frac{1}{2\pi\sigma^2} e^{\frac{x^2+y^2}{\sigma^2}} \qquad 4.7$$

Where; σ is used as scale space factor. In order to detect potential interest points that are invariant to scale and orientation efficiently, the method used the scale-space extrema in the difference-of-Gaussian(DoG) function. For DoG computation first, calculate the difference scales separated by a constant multiplicative factor k and then convolved with the image I(x, y). Interest points generated by DoG are called as SIFT keypoints.

$$D(x, y, \sigma) = [G(x, y, k\sigma) - G(x, y, \sigma)] * I(x, y) \qquad 4.8$$

$$D(x, y, \sigma) \; = L(x, y, k\sigma) - L(x, y, \sigma) \qquad 4.9$$

Hence the DOG image is the difference of the Gaussian blurred image at different scales.

4.1.2.2 Keypoint localization

We get too many candidate keypoints after Scale-space extrema detection, among them many candidate keypoints are unstable . This keypoint localization step filtered the key points,to retain only stable keypoints. At the same scale, each pixel in the DoG image is compared to its 8 neighbors and at neighboring scales to its 9 corresponding neighbors. In case the pixel is either local minima or maxima, it is considered as a key point. Interpolation of neighboring data is applied to determine the position of each candidate keypoint more accurately.

4.1.2.3 Orientation assignment

Based on local image gradient directions, each key point is assigned orientation in order to achieve robustness against rotation of image. For a Gaussian smoothed image the magnitude of gradient ‘m’ and the orientation ‘θ’ is calculated by following equations.

$$m(x, y) = \sqrt{L_1^2 + L_2^2} \qquad 4.10$$

$$\theta(x, y) = arctan(L_2/L1) \qquad 4.11$$

Where $L_1 = L(x+1, y, \sigma) - L(x-1, y, \sigma)$, and $L_2 = L(x, y+1, \sigma) - L(x, y-1, \sigma)$.

4.1.2.4 Keypoint descriptor

Neighborhoods of 4*4 pixels with 8 bins each are chosen to build a set of orientation histograms. The orientation and magnitude values of 16 x 16 block samples neighbourhood to the key point, are used to compute the histogram so that every histogram contains samples from a 4 x 4 sub region of the original neighborhood. To weigh the magnitude, Gaussian function with a scale value equal to 1. 5 times of the width of the descriptor window is used. The descriptor is then a vector of all the histograms values.

4.1.3 Potential based Fast Hierarchical Agglomerative Clustering

This type Clustering done under hypothetical potential field which is a new and interesting idea [23]. The Potential model used for clustering is described here in this section. Let us take two points i and j, if rij is defined as distance between these two points, we can define the potential at point i from point j is given below

$$\Phi_{ij}(r_{ij}) = \begin{matrix} -\frac{1}{r_{ij}} \ \text{if} \ r_{ij} \geq \delta \\ \\ -\frac{1}{\delta} \ \text{if} \ r_{ij} < \delta \end{matrix} \tag{4. 12}$$

Where parameter ‘d’ is used to avoid the singularity problem when r_{ij} becomes zero. The total potential at point i is the sum of the potentials from all the data points

$$\Phi_i = \sum_{j=1...N} \Phi_{ij}(r_{ij}) \tag{4.13}$$

where N represents the data points. Different distance measures can be used for computing r_{ij} in this potential model. As a distance measure both the Euclidean distance and the Euclidean squared distance are used in this model. To satisfy the Scale-Invariance condition [16], the parameter ‘d’ is a good practice according to the distribution of the data points. Distance matrix of dataset is a good solution

$$MinD_i = min_{r_{ij \neq 0, j=1...N}}(r_{ij}) \qquad 4.14$$

$$\delta = mean(MinD_i)/S \qquad 4.15$$

In the above equation MinDi represents the minimum distance from point i to all the other points, and S corresponds to scale factor. But it is very important to adjust S for different data sets, empirically it is found that there is a good trade-off between robustness and sensitivity when S=10. In the following, we show that the potential model is closely related to nonparametric probability density estimation; the negative potential value of a data point i computed using eq(4.11) and eq(12)can be viewed as the likelihood of the point i under the probability density function estimated using a non-parametric approach similar to the Parzen window method. First, we modify the Parzen window method to make the window a hyper sphere with a fixed radius.

$$r_N = max_{ij}(r_{ij}) \qquad 4.16$$

The window with the size defined above is always large enough to include all N data points. Then we define a new window function as follows:

$$\Phi(r) = \begin{matrix} 0 & \text{if} & r > r_N \\ \frac{\alpha}{r} & \text{if} & r_N \geq r \geq \delta \\ \frac{\alpha}{\delta} & \text{if} & r < \delta \end{matrix} \qquad 4.17$$

where a is the normalization factor which is used to make sure that the integral of the window function over all the feature space equals to 1. The probability density at data point i estimated using the above new settings is then

$$\widehat{P_N}(i)=\frac{1}{N}\sum_{j=1}^{N}\Phi(r_{ij}) \tag{4.18}$$

It follows that $\Phi_i = (-N/\alpha)\widehat{P_N}(i)$ which shows that the total potential value is negatively proportional to the probability density estimated by the non-parametric method. The connection between the potential field and the estimated probability density function indicates that the potential field can provide valuable global data distribution information for the clustering process, which is one of the key ideas of the PHA method.

4.1.3.1 PHA Clustering Algorithm

```
PHA_Clustering $(Dist[1....N,\ 1....N])$
{

$\delta \leftarrow$ the value computed from $Dist[1....N,\ 1....N]$
Using (4. 16) and (4. 17)

$(parent[1....N],\ weight[1....N]) \leftarrow$

Build_Edge_Weighted_Tree $(Dist[1...N,\ 1....N],\ \delta)$

$dendrogramRoot,\ dendrogramParent[1...2 \times N - 2] \leftarrow$

Build_Dendrogram $(parent[1....N],\ weight[1....N])$

Return $(dendrogramRoot,\ dendrogramParent[1...2 \times N - 2])$
```

Build Edge Weighted Tree Algorithm:

```
Build_Edge_Weighted_Tree $(Dist[1....N,\ 1....N],\ \delta)$
```

```
{
  for $i \leftarrow 1$ $to$ $N$ do
  {
    $\Phi[i] \leftarrow$ the potential $\Phi_i$ computed using (3) and (4)
  }
  $sortedIndexP \leftarrow$ the sorted index of $\Phi[1...N]$ from the lowest value to highest value
  $root \leftarrow sortedIndexP[1]$
  $parent[root] \leftarrow root$
  $weight[root] \leftarrow \infty$
  For $i \leftarrow 2$ $to$ $N$ do
  {
    $ci \leftarrow sortedIndexP[i]$
    $minDist \leftarrow \infty$
    for $j \leftarrow 1$ $to$ $i-1$ do
    {
      if $Dist[ci, sortedIndexP[j]] < minDist$ then {
        $p \leftarrow sortedIndexP[j]$
        $minDist \leftarrow Dist[ci, p]$
      }
    }
    $parent[ci] = p$
$weight[ci] = minDist$
}
Return ($parent[1...N]$, $weight[1....N]$)
}
```

Build Dendrogram Algorithm:

```
Build_Dendrogram ($parent[1....N]$, $weight[1....N]$)
{
$sortedIndexW \leftarrow t$ the sorted index of $weight[1....N]$ from the lowest value to highest
for $i \leftarrow 1$ $to$ $N - 1$ do
{
$dendrogramParent[i] \leftarrow i$
$clusterLabels[i] \leftarrow i$
}
for $i \leftarrow 1$ $to$ $N - 1$ do
{
  $ci \leftarrow sortedIndexW[i]$
  $pi \leftarrow parent[ci]$
$dendrogramParent[clusterLabels[ci]] \leftarrow N + i$
$dendrogramParent[clusterLabels[pi]] \leftarrow N + i$
for $j \leftarrow 1$ $to$ $N$ do
{
```

```
            if ($clusterLabels[j] = clusterLabels[ci]$)
            or $clusterLabels[j] = clusterLabels[pi]$ then {
                $clusterLabels[j] \leftarrow N + 1$
            }
        }
    }
    $dendrogramRoot \leftarrow 2 \times N - 1$
    Return ($dendrogramRoot,\ dendrogramParent[1....2 \times N - 2]$)
}
```

The purpose of PHA on the output of SIFT is to filter out false matches and group key points. Those keypoints follow the same affine transformation pattern are grouped into clusters. Finally, on the number of keypoints in the clusters (N_{KP}), the test image is identified as a forged image or authentic image. If N_{KP} for all clusters is less than 3, then the image is said to be a authentic image which means“not doctored by any copy-move attack”.

Chapter-5 Results And Analysis

The proposed method is evaluated on many original and forged images with different types of Copy Move forgeries. We developed a database of 100 images including authentic images and different types of copy-move forged images based on the authentic images taken by different camera models and from two well known datasets "CoMoFoD" and MICC-F2000. To test and compare the performance of our proposed method with other forgery detection methods these datasets are used. In this study the performance of copy move forgery detection system will be tested on (100) images that selected from these datasets.

5.1 "CoMoFoD" Dataset

"CoMoFoD" was released in 2013(Tralic, et al. (2013). This dataset contains a total of 10400 images. The number of authentic images in this dataset are 260, while remaining 10140 are tampered images [24]. Fig 5. 1 shows some examples of authentic and tampered images from "CoMoFoD" datasets, where all the images in top row are authentic and the images in the bottom row are all tampered.

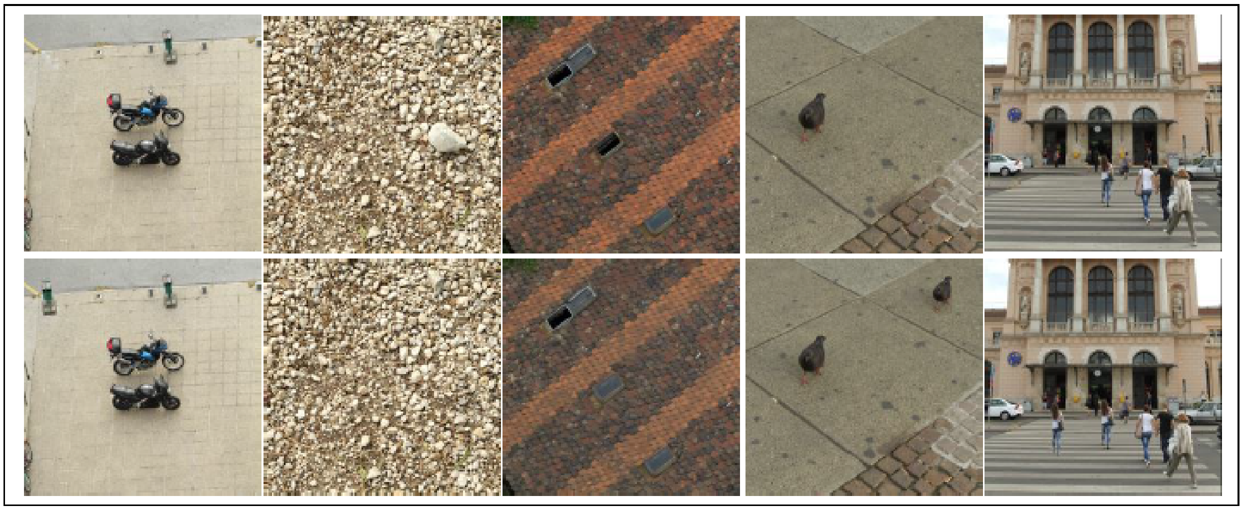


Fig 5.1 Examples of images from "CoMoFoD" dataset

5.2 “ MICC-F2000” Dataset

“MICC-F2000” dataset was released in 2011 (Amerini, et al. , (2011). It contains a total of 2000 images, in which 700 images are authentic and 1300 are tampered. All of the 200 images have a uniform size of 737×492 pixels and having the same JPEG format [21]. The forged images are obtained, in both datasets, by randomly selecting a rectangular patch and copy-pasting it over the original image after several different attacks (rotation, scaling, translation, etc.). Fig 5. 2 illustrates some examples of authentic and tampered images from “MICC-F2000” datasets, where all the images in top row are authentic and the images in the bottom row are all tampered.

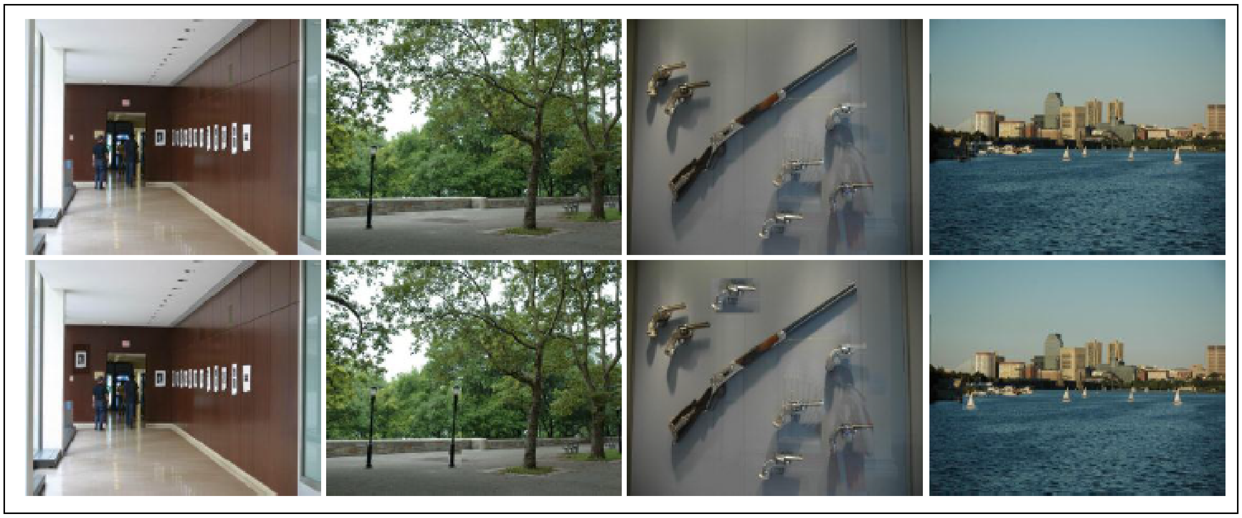


Fig 5.2 Examples of images form “MICC-F2000” dataset

5.3 Experimental Results:

5.3.1 Original image

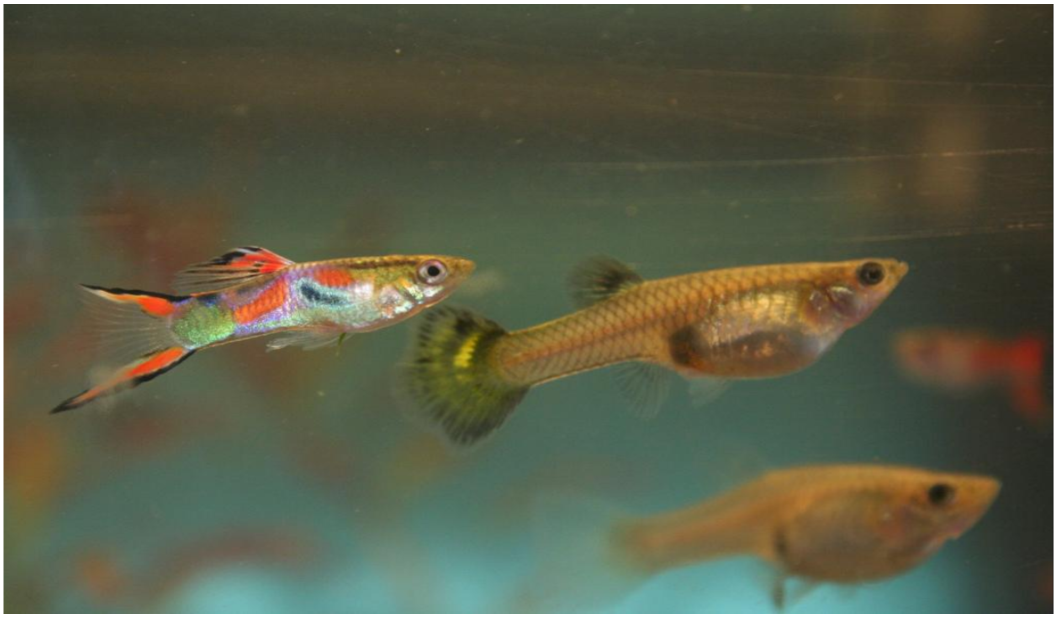


Fig 5.3 Original image

5.3.2 Forged image

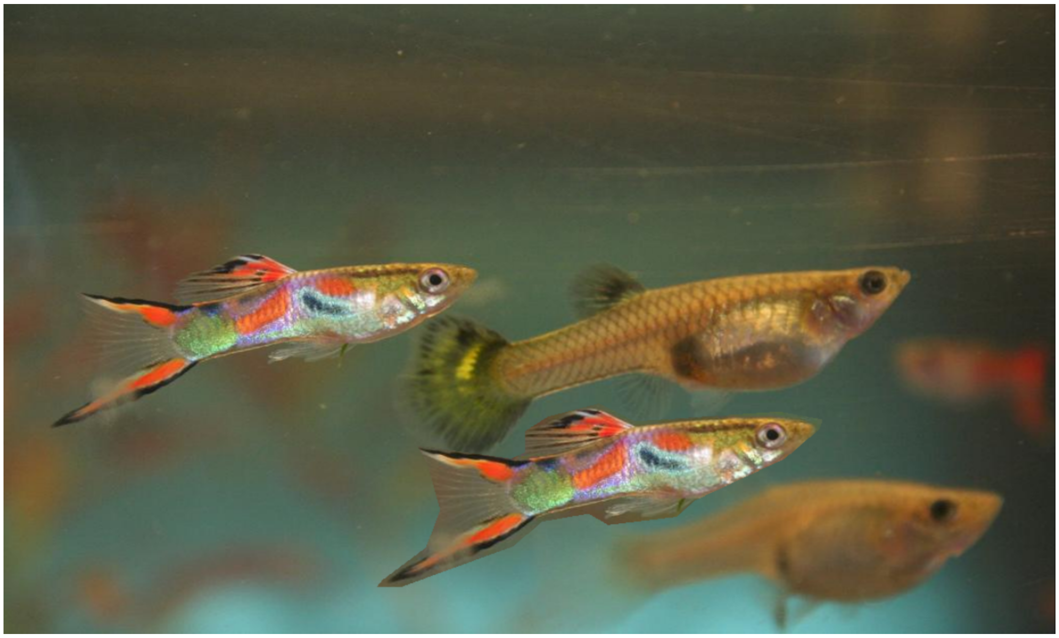


Fig 5.4 Forged image

5.3.3 High resolution image

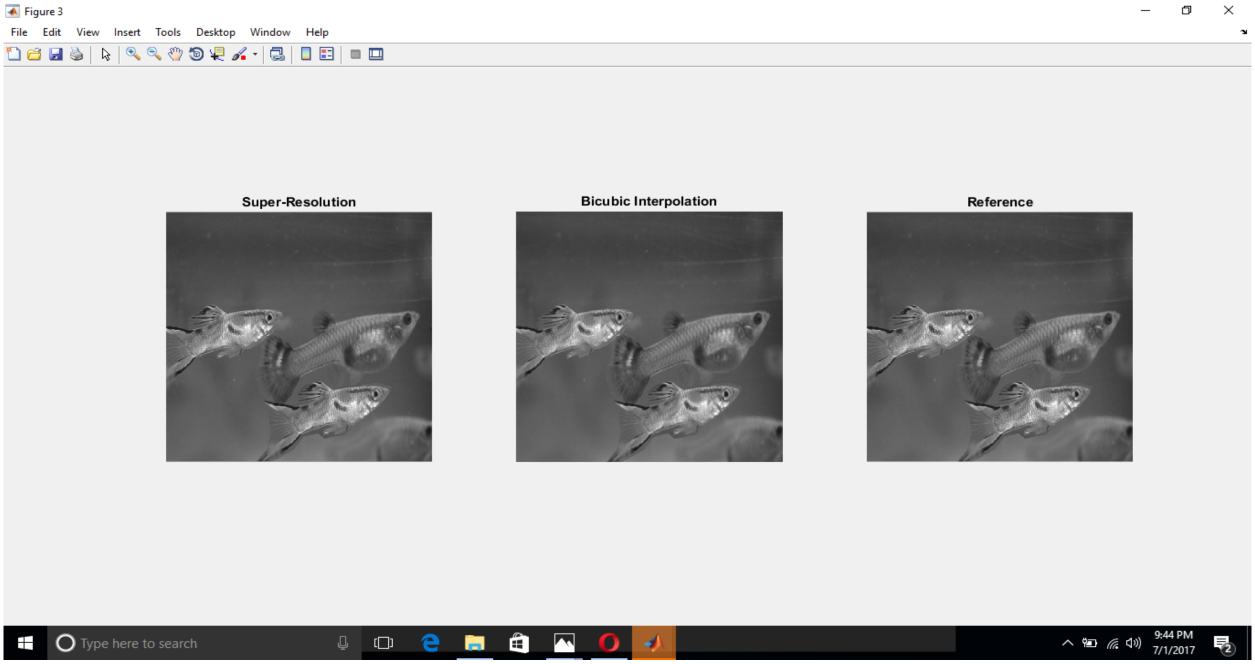


Fig 5.5 Results of super resolution

5.3.4 Result after Feature Extraction and Matching

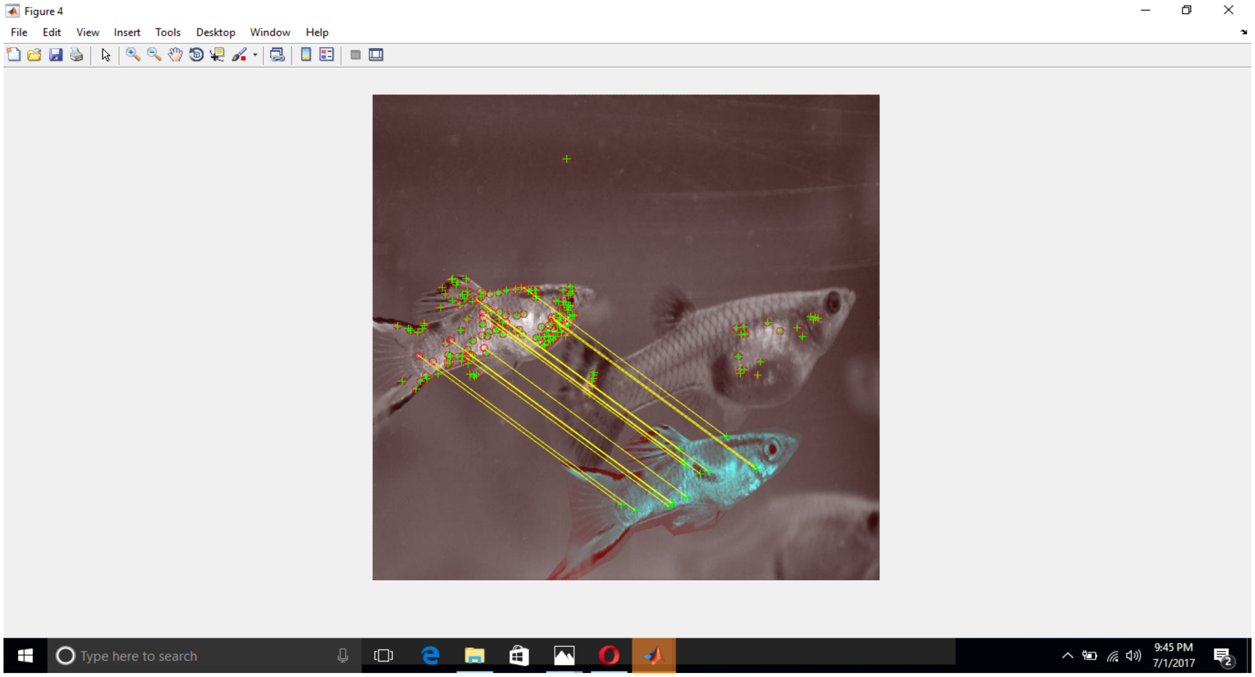


Fig 5.6 Feature Extraction and Matching

5.3.5 Final Forgery detection Result

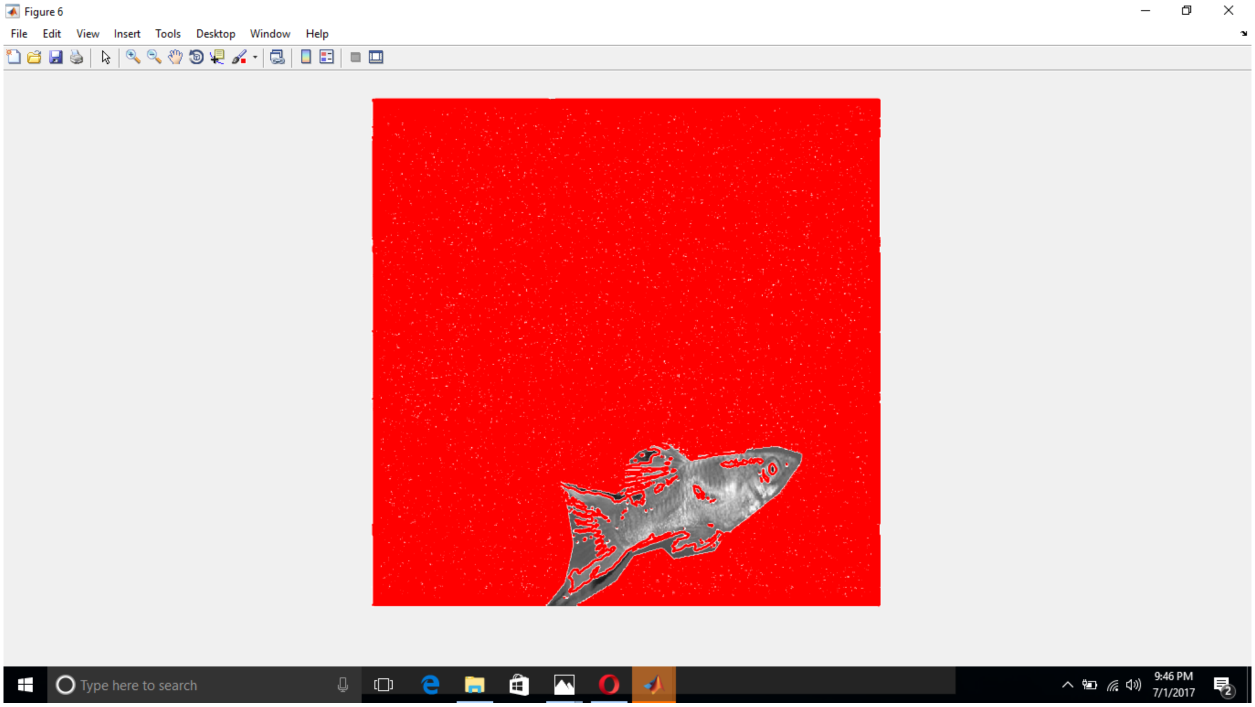


Fig 5.7 Final result of proposed approach

5.4 Performance Measures

Performance can be measured in terms of Precision, Recall and Accuracy of a method or algorithm. Accuracy is the percentage of exactly distinguished images from total number of images. The precision is the ratio between correctly detected images and the sum of false positive plus correctly detected images. The Recall is the ratio between the correctly detected images to the sum of false negatives plus correctly detected images.

$$Accuracy = \frac{T_P+T_N}{T_P+F_P+F_N+T_N} \qquad 5.1$$

$$Precision = \frac{T_P}{T_{P+F_P}} \qquad 5.2$$

$$Recall = \frac{T_P}{T_{P+F_N}} \qquad 5.3$$

$$Average = 2 * \frac{(Pecision*Recall)}{(Precision+Recall)} \qquad 5.4$$

Whereas; T_P is true positive which means the total number of images successfully detected as tampered.

T_N is true negative which means the total number of images successfully detected as non tampered.

F_P is false positive which means the total number of images unsuccessfully detected as tampered whereas actually the images are not tampered.

F_N is false negative which means the total number of images unsuccessfully detected as non-tampered.

Label associated with each state-of-the-art method

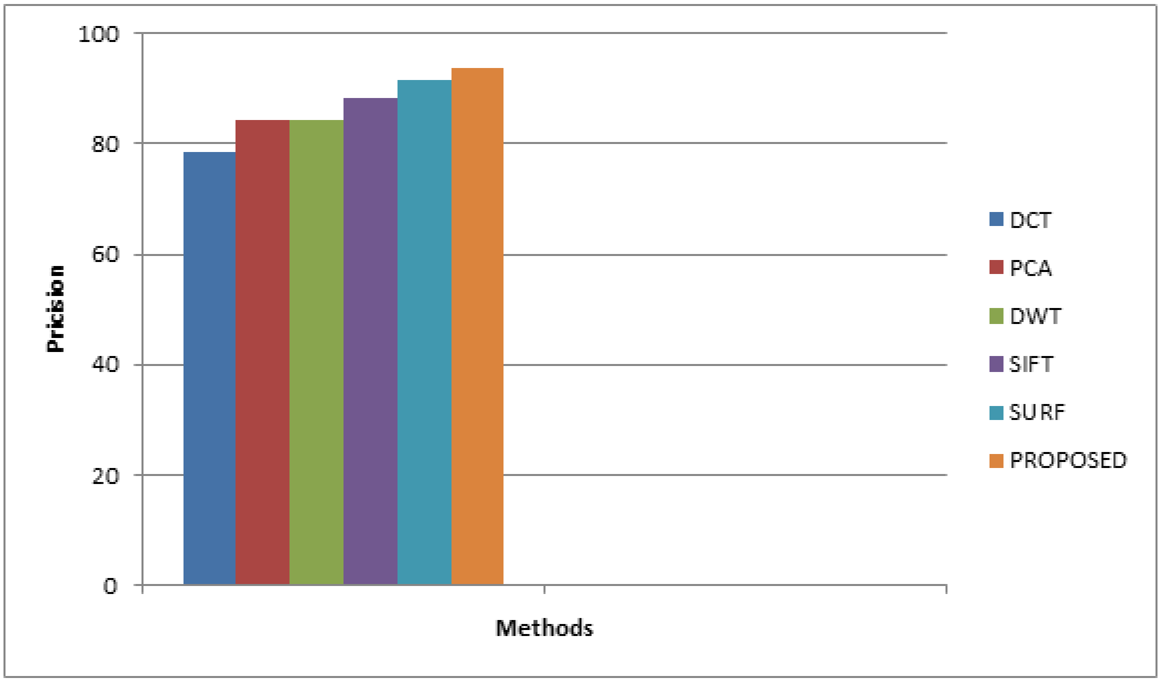
S. No.	Method	Label
1	Fridrich et al. [8]	DCT
2	Popescu and Farid [11]	PCA
3	Bashar et al. [13]	DWT
4	Amerini et al. [21]	SIFT
5	Wang Jun[22]	SURF

Table 5.1 Labels associated with some popular CMFD methods

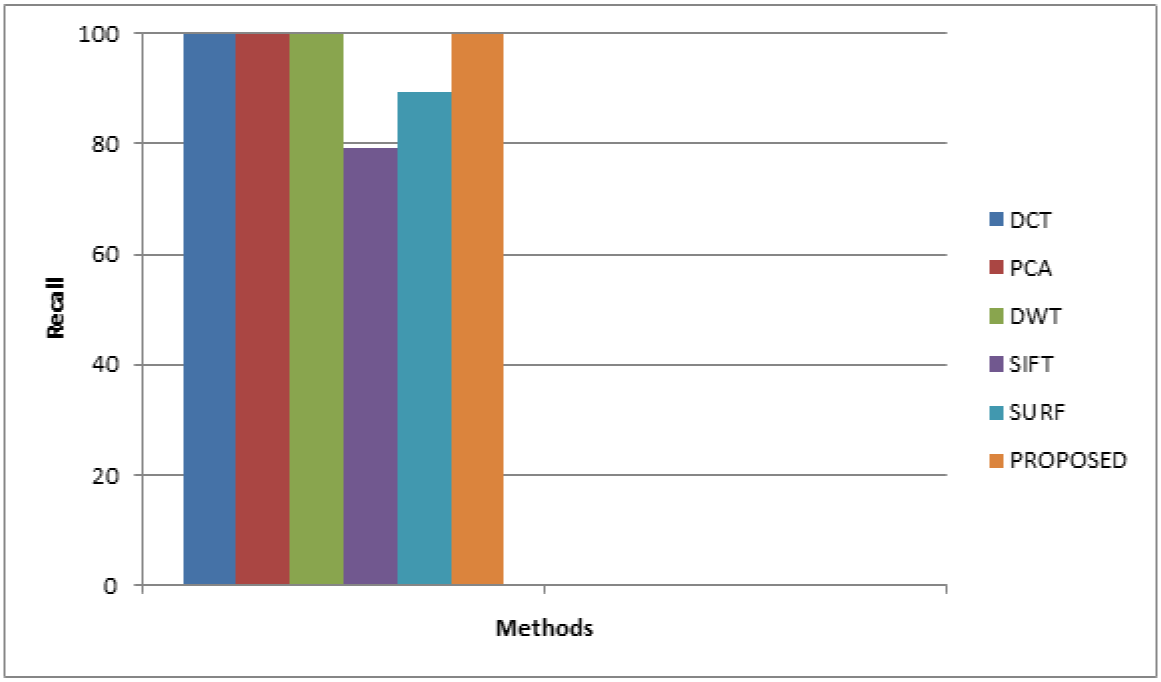
Comparing the precision, recall and average of other popular CMFD methods (Strategy by Amerini[21]) and our proposed method.

S. No.	**Method**	**Precision**	**Recall**	**Avg**
1	DCT	78. 69	100	88. 07
2	PCA	84. 21	100	91. 43
3	DWT	84. 21	100	91. 43
4	SIFT	88. 37	79. 17	83. 52
5	SURF	91. 49	89. 58	90. 53
6	Proposed Method	**93. 75**	**100**	**96**

Table 5.2 Comparison in terms of Precision, Recall and Average of them

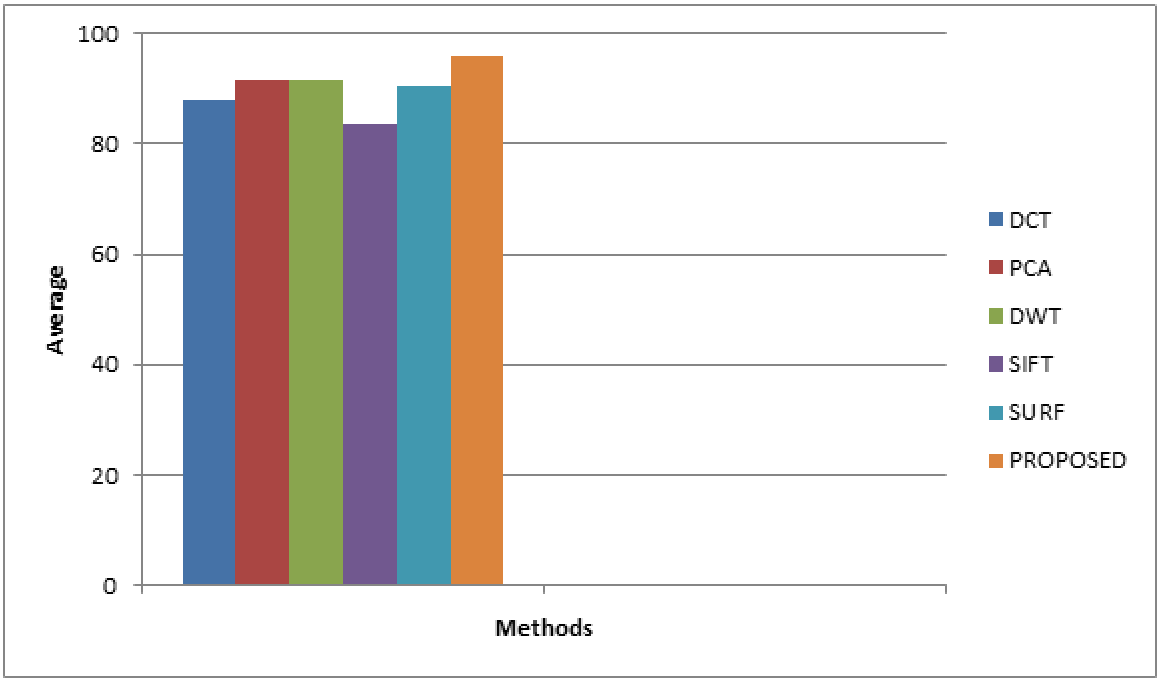


Graph 5.1 Comparison in terms of precision



Graph 5.2 Comparison in terms of Recall

The average which is calculated by combining precision and recall is represented by the following graph



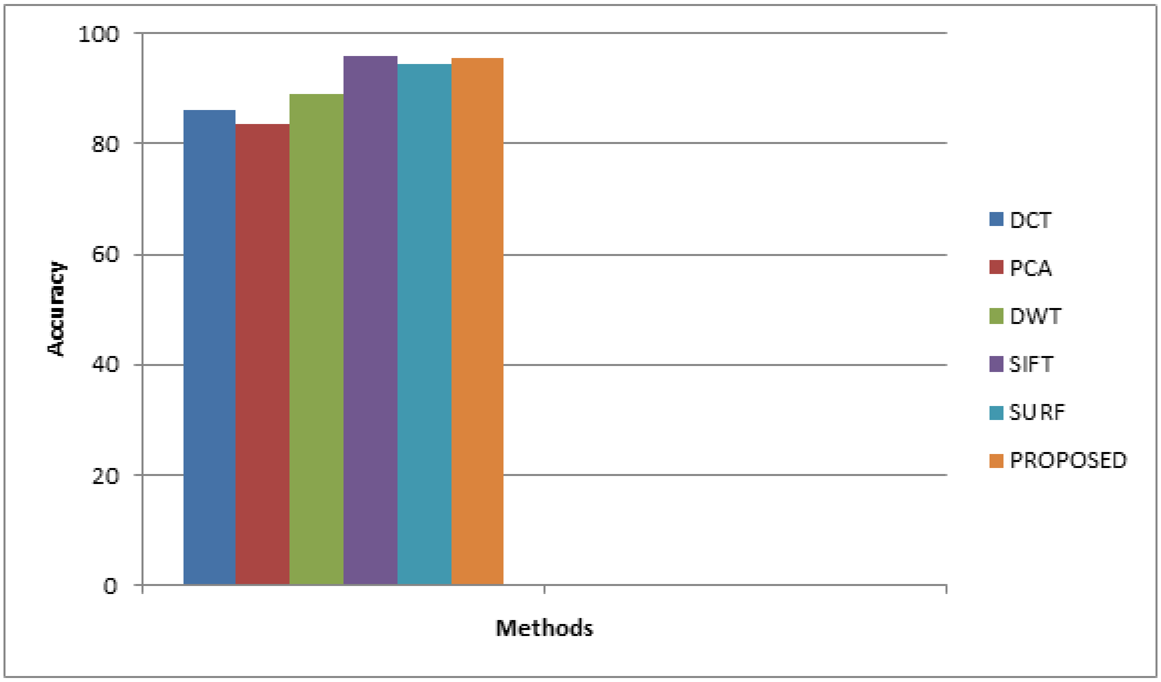
Graph 5.3 Comparison in terms of average of precision and recall

Following table shows the comparison between proposed method and other state-of-the-art method in terms of Accuracy

S. No.	**Method**	**Accuracy**
1	DCT	86. 00
2	PCA	83. 47
3	DWT	89. 22
4	SIFT	96
5	SURF	94. 41
6	**Proposed Method**	**95. 45**

Table 5. 3 Comparison of our method and others in terms of Accuracy

The following graph clearly illustrates that our approach is comparable with other popular methods for CMFD.



Graph 5. 4 Comparison in terms of Accuracy

Chapter-6 Conclusion

6.1 Conclusion

In digital images one of the most frequent manipulation is Copy Move. In this field a compelling research has been done and thus there are lots of methods exist. But to achieve a low complexity in terms of computation and high performance in terms of Precision, Recall and Accuracy are the most challenging factors for all the methods which are currently available for the image CMFD. A good CMFD approach should be robust to various types of operation such as scaling, compression, rotation etc.

In this thesis such type of a system is designed with the help of Super resolution and SIFT to get more accurate results even when the test image is a low resolution image. The proposed approach is comparable to some popular existing methods for copy move forgery detection. Better results are being obtained through proposed methodology as compared to the traditional methodology in terms of various performance measures such as accuracy, precision and recall.

Advancement is done in proposed method, and that is the use of super resolution of test image before applying feature extraction algorithm, which will improve the feature extraction and because of this we will get more accurate results. The use of super resolution as a preprocessing step helps to resolve finer details in small size forgeries.

.

6.2 Future Scope

In future we would like to reduce the computation complexity the algorithm. It is one of the major issue that false positive rate of detection results in keypoint based copy move forgery technique is high, so this can be resolved in future. The exponential growth in technology makes image forensics very sophisticated. Hence there is a need of exhaustive study and research in the area of forgery detection.

References

[1]Christlein, V. , Riess, C. , Jordan, J. , Riess, C. , & Angelopoulou, E. (2012). An evaluation of popular copy-move forgery detection approaches. *IEEE Transactions on information forensics and security*, *7*(6), 1841-1854.

[2]C Rey and J-L Dugelay, "A survey of watermarking algorithms for image authentication. , " EURASIP Journal on Applied Signal Processing, pp. 613-621, 2002.

[3] V M Potdar, S Han, and E Chang, "A survey of digital image watermarking, " in 3rd IEEE International Conference on Industrial Informatics, Perth, Western Australia, 2005, pp. 709-716.

[4] Granty Regina Elwin J, Aditya T S, and Madhu Shankar S, "Survey on Passive Methods of Image Tampering Detection, " in Proceedings of the International Conference on Communication and Computational Intelligence, 2010, pp. 431-436.

[5] B Mahdian and S Saic, "A bibliography on blind methods for identifying image forgery, " in Signal Processing:Image Communication, 2010, pp. 389-399.

[6]Bayram, S. , Sencar, H. T. , & Memon, N. (2008, September). A survey of copy-move forgery detection techniques. In *IEEE Western New York Image Processing Workshop* (pp. 538-542). IEEE.

[7]Al-Qershi, O. M. , & Khoo, B. E. (2013). Passive detection of copy-move forgery in digital images: State-of-the-art. *Forensic science international*, *231*(1), 284-295.

[8]J. Fridrich, D. Soukal, J. Lukas, Detection of copy-move forgery in digital images, in: Digital Forensic Research Workshop (DFRWS), Cleveland, USA, 2003, pp. 134–137.

[9]Cao, Y. , Gao, T. , Fan, L. , & Yang, Q. (2012). A robust detection algorithm for copy-move forgery in digital images. *Forensic science international*, *214*(1), 33-43.

[10]Zhao, J. , & Guo, J. (2013). Passive forensics for copy-move image forgery using a method based on DCT and SVD. Forensic science international, 233(1), 158-166.

[11]A. C. Popescu, H. Farid, Exposing Digital Forgeries by Detecting Duplicated Image Regions, Tech. Rep. TR 2004-515, Dept. of Computer Science – Dartmouth College, Hanover, USA, 2004.

[12]Ustubioglu, B. , Ulutas, G. , Ulutas, M. , Nabiyev, V. , & Ustubioglu, A. (2016). LBP-DCT based copy move forgery detection algorithm. In Information Sciences and Systems 2015 (pp. 127-136). Springer, Cham.

[13]Bashar, M. K. , Noda, K. , Ohnishi, N. , Kudo, H. , Matsumoto, T. , & Takeuchi, Y. (2007, May). Wavelet-Based Multiresolution Features for Detecting Duplications in Images. In MVA (pp. 264-267).

[14]Zhong, L. , & Xu, W. (2013, May). A robust image copy-move forgery detection based on mixed moments. In Software Engineering and Service Science (ICSESS), 2013 4th IEEE International Conference on (pp. 381-384). IEEE.

[15]Quan, X. , & Zhang, H. (2012, June). Copy-move forgery detection in digital images based on local dimension estimation. In *Cyber Security, Cyber Warfare and Digital Forensic (CyberSec), 2012 International Conference on*(pp. 180-185). IEEE.

[16]Hsu, H. C. , & Wang, M. S. (2012, August). Detection of copy-move forgery image using Gabor descriptor. In *Anti-Counterfeiting, Security and Identification (ASID), 2012 International Conference on* (pp. 1-4). IEEE.

[17]Li, J. , Li, X. , Yang, B. , & Sun, X. (2015). Segmentation-based image copy-move forgery detection scheme. *IEEE Transactions on Information Forensics and Security*, *10*(3), 507-518.

[18]Pun, C. M. , Yuan, X. C. , & Bi, X. L. (2015). Image forgery detection using adaptive over segmentation and feature point matching. *IEEE Transactions on Information Forensics and Security*, *10*(8), 1705-1716.

[19]Zandi, M. , Mahmoudi-Aznaveh, A. , & Talebpour, A. (2016). Iterative copy-move forgery detection based on a new interest point detector. *IEEE Transactions on Information Forensics and Security*, *11*(11), 2499-2512.

[20]Guo, Q. , Liu, H. , Chen, W. , & Shen, I. F. (2008, September). Super resolution based on gradient field. In Cybernetics and Intelligent Systems, 2008 IEEE Conference on (pp. 164-168). IEEE.

[21]Amerini, I. , Ballan, L. , Caldelli, R. , Del Bimbo, A. , & Serra, G. (2011). A SIFT-based forensic method for copy–move attack detection and transformation recovery. IEEE Transactions on Information Forensics and Security, 6(3), 1099-1110.

[22]Bo, X. , Junwen, W. , Guangjie, L. , & Yuewei, D. (2010, November). Image copy-move forgery detection based on SURF. In Multimedia information networking and security (MINES), 2010 international conference on (pp. 889-892). IEEE.

[23]Lu, Y. , & Wan, Y. (2013). PHA: A fast potential-based hierarchical agglomerative clustering method. Pattern Recognition, 46(5), 1227-1239.

[24]Tralic, D. , Zupancic, I. , Grgic, S. , & Grgic, M. (2013, September). CoMoFoD—New database for copy-move forgery detection. In ELMAR, 2013 55th international symposium (pp. 49-54). IEEE.