PERFORMANCE ENHANCEMENT OF COPY-MOVE FORGERY DETECTION BY USING SHI TOMASI-SURF DETECTOR AND SURF-PSO ALGORITHM

A Dissertation Submitted in Partial Fulfillment of the Requirement for the Award of the Degree of

MASTER OF ENGINEERING

in

Electronics and Communication

Submitted By

ANMOL GUPTA

801561004

Under Supervision of

DR. ANKUSH KANSAL

Assistant Professor, ECED

ELECTRONICS AND COMMUNICATION ENGINEERING DEPARTMENT

THAPAR UNIVERSITY, PATIALA, PUNJAB

JULY, 2017

DECLARATION

I, Anmol Gupta hereby declare that the work presented in this thesis entitled **Performance Enhancement of Copy-Move Forgery Detection By Using Shi Tomasi-SURF Detector and SURF-PSO Algorithm** in partial fulfillment of the requirement for the award of degree of Master of Engineering submitted at ECED, Thapar University, Patiala is an authentic record of work carried out under supervision of Dr. Ankush Kansal (Assistant Professor, ECED, Thapar University) from 2015 to 2017. The matter presented in this has not been submitted either in part or full to any other university or institute for the award of any other degree.

Date: 13-07-17

Anmol Gupta
801561004

It is certified that the above statement made by the candidate is correct to the best of my knowledge and belief.

Date: 13-07-17

13/7/17
Dr. Ankush Kansal
Assistant Professor

ACKNOWLEDGEMENT

It is my proud privilege to acknowledge and extend my gratitude to several persons who helped me directly or indirectly in completion of this report. I express my heart full indebtedness and owe a deep sense of gratitude to my teacher and my faculty guide **Dr. Ankush Kansal** for his sincere guidance and support with encouragement to go ahead.

I am also thankful to **Dr.Alpana Aggarwal**, Professor and Head, ECED, for providing us with the adequate infrastructure for carrying out the work. I am also thankful to **Dr.Hem Dutt Joshi** Associate Professor & P.G. Coordinator, ECED, for the motivation and inspiration and that triggered me for the work.

I would like to express my heartfelt gratitude for my friend **Ishan Chawla**, who helped me to widen the perspective of my research and motivated me to keep my spirits high even in the hardest of the times. I would also like to thank my friend **Gursimar Kaur** for her unconditional care and support in every aspect of my life and career. Last but not the least, I would like to thank my parents who have stood by my side through every thick and thin of life. I owe my gratitude to my sister **Ruchika Gupta** and brother **Parul Gupta** for their unrelenting support and helping me believe in my own self.

This study has indeed helped me to explore knowledge and avenues related to my topic and I am sure it will help me in my future.

ANMOL GUPTA

ABSTRACT

In this era of digital computing, digital images are one of the principal means of communication. With the tremendous utilization of digital images and the accessibility of capable image editing tools such as Adobe Photoshop, GNU Image Manipulation Program "GIMP", it turns out to be very easy to control or alter the digital images and create forgeries without leaving any visual pieces of information. Accordingly, digital images have lost their trust and it has become important to check the originality of content when they are utilized as a part of some basic situations like criminal investigation etc. In this way, Digital Image Forensics emerged as a research field that plans to check the authenticity and integrity of digital images.

Many block-based and key-points based techniques have been proposed so far to detect Copy-Move Forgery in digital images; where a part of an image is copied and pasted elsewhere within the same image. Among all the available forgery detection techniques, the most computationally effective and robust technique is Speeded-Up Robust Transform (SURF) framework. The major advantage of SURF over other prevailing forgery detection techniques is that SURF is fastest among other techniques, has less computational complexity, lesser length of descriptor vector etc. However, the key-points detected by SURF detector are not able to detect forgeries in regions with inconspicuous changes. Therefore, to overcome this issue and further enhance the detection accuracy, in this thesis, SURF detection technique is replaced by Shi-Tomasi detector. Finally, SURF descriptors are deployed to give unique identity to each key-point for matching process. The proposed algorithm has improved the precision and recall from 91.49% and 89.59% to 97.87% and 93.75% respectively as compared to conventional SURF based detection.

Also, the detection results of conventional SURF based framework highly depends upon the value of parameters which are mostly determined with human perception. Henceforth; the predetermined parameter values limit the application of copy-move forgery detection since they are not applicable to all the images. Therefore, a novel approach by integrating SURF based detection with particle swarm optimization (SURF-PSO) has been proposed. This utilizes Particle swarm optimization for each image independently to generate optimized value of parameters for forgery detection under SURF framework. In this thesis, the proposed SURF-PSO is applied on five images separately and the results prove that SURF-PSO performs much better than the conventional SURF technique. The precision of the SURF-PSO is 1 for three images while it is 0 or 0.5 for conventional SURF and for a particular image, SURF-PSO detected 1064 matched points while conventional SURF detected only 132.

TABLE OF CONTENTS

LISTS OF TABLES

LISTS OF FIGURES

LIST OF ABBREVIATIONS

AWGN	Additive White Gaussian Noise
CMFD	Copy-Move Forgery Detection
DCT	Discrete Cosine Transform
DoG	Difference of Gaussians
DWT	Discrete Wavelet Transform
DyWT	Dyadic Wavelet Transform
FMT	Fourier Mellin Transform
FPR	False Positive Rate
HAC	Hierarchical Agglomerative Clustering
JPEG	Joint Photographic Experts Group
k-NN	k-Nearest Neighbors
KPCA	Kernel Principal Component Analysis
LBP	Local Binary Pattern
MMPs	Mis-Matched Points
PCA	Principal Component Analysis
PPV	Predefined Parameter Values
PSO	Particle Swarm Optimization
RANSAC	Random Sample Consensus
SIFT	Scale Invariant Feature Transform
SURF	Speeded-Up Robust Features
SVD	Singular Value Decomposition
SVM	Support Vector Machine
TPR	True Positive Rate
TMPs	True Matched Points
WLD	Weber Law Descriptors
2NN	Second Nearest Neighbour
64-D	64-Dimensional
128-D	128-Dimensional

CHAPTER 1
INTRODUCTION

1.0 PREAMBLE

Images are captured through variety of popular devices like cameras, x-ray devices, radar, electron microscopes, ultrasound and are used for a variety of purposes which includes entertainment, business, medical, military security etc. However, the crude image is not specifically appropriate for extricating the helpful data about the scene being imaged. Hence, Digital Image Processing is introduced which basically captures the nature of an image so that the pictorial information is improved for human interpretation. An image is essentially digitized to store it over to a structure which can be put away in some type of capacity media, for example, CD-ROM or in a PC's memory. Once the picture has been digitized, it can be worked upon by different image pre-processing operations [1]. The different image pre-processing operations can be isolated into three noteworthy classes, namely

- **Image Compression** which includes decreasing the size of memory required to store an image.
- **Image Enhancement and Restoration which** is utilized to amend the imperfections in an image which could be brought upon by the digitization process or by flaws in the imaging set-up.
- **Measurement Extraction** operations which are utilized to get the helpful data from the image if the image is in good condition [2].

1.1 IMAGE FORGERY DETECTION

In present scenario of digital technology and revolution, it has become very easy to access the information, process it accordingly and share it. In this era of digital computing, there is an increase in the necessity and interest of representing information in visual forms. In the past few years, there is an extensive increase in the transmission of advanced pictures utilizing tools like scanners, digital cameras, photo-editing and software packages. However, these tools impose security challenges. Digital images have many applications in different fields including the areas where images are utilized as a matter of proof, for example, in forensic studies and law enforcement. Therefore, verifying the genuineness and integrity of images is of great importance. Since, the advancement in the image processing software tools such as Photoshop, Corel Draw etc. has increased, digital images can be easily manipulated and modified even by ordinary people [3]. For instance, in 2001, after the 9/11 incident, several videos of Osama bin Laden over the social media were found counterfeited through the

forensic analysis [4]. Similarly, in 2008, an official image of four Iranian ballistic missiles was found to be doctored, as one missile was revealed to be duplicated [5]. A case of simple forgery is shown below in Figure 1.1.

Figure 1.1 A case of simple forgery (a) Original image; (b) Forged image

Such a security threat created a wide interest among scholars and researchers for developing methods to detect forged images. Digital Image Forensics is an emerging branch of image processing which deals with validating the genuineness and integrity of the images. Image tampering detection is one of the foremost tasks of Digital Image Forensics. Tampering basically refers to interfering with something with the intent of causing damage or making unauthorized alterations in it. Therefore, Digital Image Forgery has become an emerging issue especially in criminal cases and in public course.

1.2 TYPES OF DIGITAL IMAGE FORGERY

Digital image forgery implies manipulating or changing the significant contents of an image with the intent of changing the semantic meaning of the information present in that image. The contents of the digital image can be modified in numerous ways. Based upon the methods of modification, the digital image forgery can be categorized to various types as illustrated in Figure 1.2.

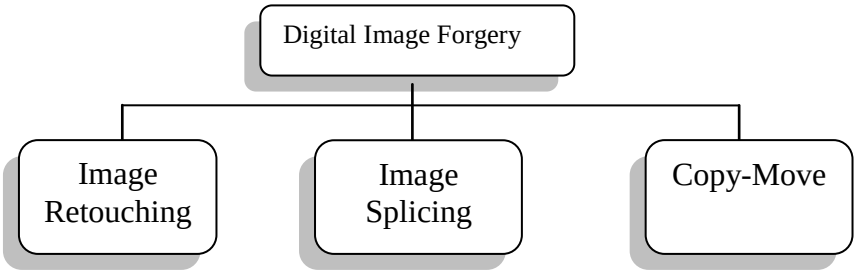


Figure 1.2 Types of Digital Image Forgery

1.2.1 Image Retouching

This can be supposed as less unsafe type of advanced digital image forgery as it doesn't essentially change an image, however it rather lessens or upgrades certain elements or features of an image [6]. Image Retouching is basically applied by magazine or journal cover editors to make it more appealing or attractive. The common case of image retouching is shown in Figure 1.3.

Figure 1.3 An example of Image Retouching Forgery [7]

1.2.2 Image Splicing

Image Splicing is done by copying one part from an image and using it to create a forgery by pasting it to another image. It is more forceful than image retouching. Basically, in image splicing, features from two or more images are merged to create a convinced forgery [8]. A popular case of image splicing forgery where two distinct images are united to create a realistic forgery is shown in Figure 1.4.

Figure 1.4 An example of Image Splicing Forgery [8]

1.2.3 Copy-Move Forgery

In copy-move forgery, a region or part from an image is copied and pasted elsewhere within the same image with the intent of hiding or adding some valuable content in an image. In this case, the forgery detection is complicated to detect because certain features of original and forged image are same such as color, texture, source and the destination. Also, to minimize the impact of inconsistencies between the authenticated and the forged regions, some post-

processing operations such as blurring, median filtering etc. are usually applied [9]. An example of copy-move forgery is shown below in Figure 1.5.

Figure 1.5 An example of Copy-move Forgery [10]

1.3 NEED FOR AUTHENTICATION

Utilizing the advanced digital technology, the digital images can be effortlessly altered or exploited to create forgeries without giving rise to any visual clues. Therefore, proving the genuineness and trustworthiness of an image is important in the fields of e-commerce, medical imaging, forensics, industrial photography etc. Diagnosis in medical field is also based on imaging. Also, images and videos are basic elements to describe the product in online marketing.

But, with the enhancement of technology and spread of photo-editing tools, manipulating anything has become so easy. "To believe what you see" no longer holds nowadays. Therefore, to deal with ethical issues of digital images integrity, truth and deception, various forgery detection techniques needs to be developed. Therefore, the dependability of computerized images in numerous zones, for example, forensic investigation, medical imaging, surveillance systems, criminal investigation, intelligent services and journalism [11] make it very important to authenticate digital images, identify their sources and detect forgeries.

1.4 IMAGE FORGERY DETECTION

Every image that has been altered is not necessarily a forged one. Sometimes, some horizon corrections, cropping and blurring is applied to an image without changing the semantic meaning of an image. Hence, these techniques do alter the image but do not necessarily forge it. But, when an image is manipulated intentionally to hide some meaningful information, it becomes a forgery and it is necessary to detect such kind of manipulations. Therefore, to protect digital images, various authentication techniques have been developed and are categorized under two major categories as shown in Figure 1.6.

1. Active Authentication
2. Passive Authentication

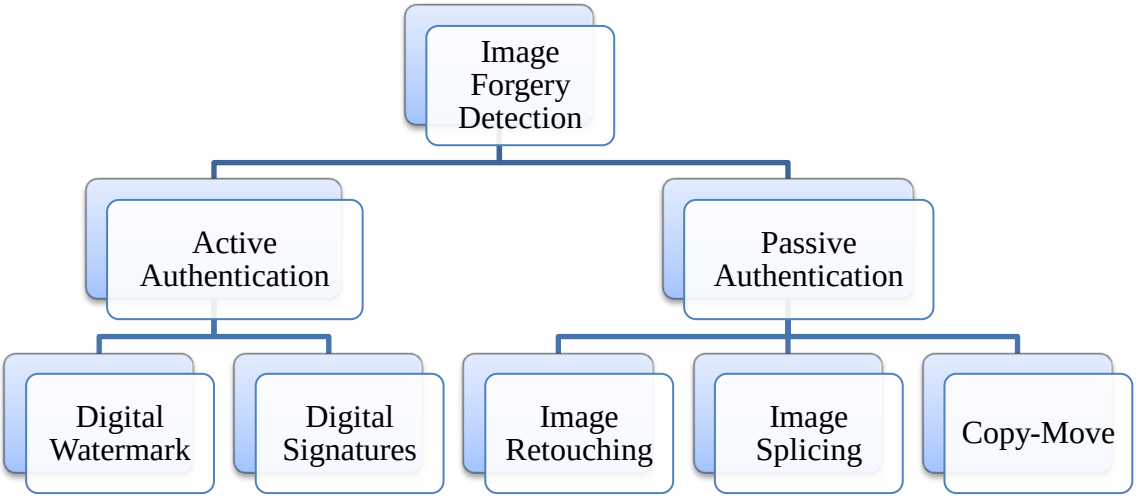


Figure 1.6 Image Authentication Techniques

1.4.1 Active Authentication

In active approach, prior knowledge about the original image is required. It uses a known authentication code sent with the image or embedded into an image in the form of name, signature, date, etc. for assessing the authenticity of the image. In active authentication, data must be embedded during the capturing stage using some special hardware or the authorized personnel may add it at later stage. It is mainly based on- digital signatures and watermarking techniques.

- Digital Watermarking**:** It is composed of embedding a mark or some information in an original image at the capturing stage. Any manipulation will subsequently affect the condition of the watermark. The inserted watermark can be extracted at any time to determine if the tampering has been done or not [12]. If the retrieved watermark differs from the original watermark that was inserted at the acquisition stage, it means tampering has been done after the acquisition time. Therefore, condition of watermark is used to validate the originality of an image. But, inserting watermark requires specially equipped camera and also the original image itself which is basically the main drawback of watermarking process.
- Digital Signatures: At the image capturing end, it separates some kind of unique features or properties as a signature from the image. At the authentication end, digital signature embedded into the image is regenerated using the same technique and then bit by bit

comparison between the encrypted signature and decrypted signature is done to check the authenticity of an image [13].

The active authentication techniques possess the advantage of low computational load. Since, these methods require a priori information regarding the original image, these methods are not automatic. Also, embedding watermarks require specially-equipped cameras for this purpose and transmitting digital signatures requires use of extra bandwidth. Therefore, these methods cannot be used for verifying the authenticity of all images including those on the internet which don't have any digital signature or watermark embedded into it.

1.4.2 Passive Authentication

In passive authentication, no auxiliary information regarding the original image is required to verify the originality of an image. It uses the forged image itself and hence it is automatic. The contents and the binary information of an image are utilized in this method to check the genuineness of images. To detect the forgery, the image function is utilized by these strategies and the point that forgeries can bring about a particular recognizable change into the image itself such as lightning inconsistency. Though passive techniques don't require a priori information about the original image but different statistics of an image are required to detect the forgery which makes this method more complex [14]. Passive authentication can be characterized: the source device identification and the tamper detection [15].

- Source Device Identification: In this, the camera fingerprints are identified, which are basically the left-over hints of image acquiring steps and storage stages. To differentiate among different models of cameras, left-over camera fingerprints are utilized and the origin of the image is determined based on sensor and optical irregularities. This technique can also be used to make distinction between various epitomes of one or same camera model.
- Tamper Detection: This scheme can be either forgery-dependent or forgery independent. The dependent forgery techniques involve copying a part or a particular region from an image and pasting elsewhere within the same image i.e. copy-move forgery or pasting it onto some another image i.e. image splicing. On the other hand, independent type forgery takes into account general manipulations such as re-sampling, compression and lightning inconsistencies.

1.5 COPY-MOVE FORGERY DETECTION (CMFD)

Copy-move forgery is the most prevailing type of forgery as it can easily and effectively modify the contents of an image. It involves copying a region from an image and pasting it elsewhere within the same image. However, in many cases, it is not simply a copy and

pasting process. It may include some intermediate and post- processing operations that can make detection of forgery more difficult and complex. These operations include rotating, scaling, blurring, JPEG compressing, adding Gaussian noise and varying illumination of copied part before pasting it. Therefore, the detection methods need to be robust against such operations to effectively locate the duplicated regions.

Copy-move forgery detection techniques can be categorized into two types:

1. Block based techniques
2. Key-point based techniques

Block-based techniques divide an image into overlapping or non-overlapping blocks for analysis during the pre-processing stage. The features are extracted from these blocks for block-based method and compared against each other to determine the similarity.

Key-point based methods identify and select high-entropy image regions (i.e., the "key-points"). Then, extraction of a feature vector is done per key-point that is further used for comparing against each other to determine the similarity.

1.5.1 Common Workflow

The majority of the algorithms follow the practices of a typical pipeline as presented in the Figure 1.7 beneath, despite the fact that there exists extensive variety of algorithms for copy-move forgery detection.

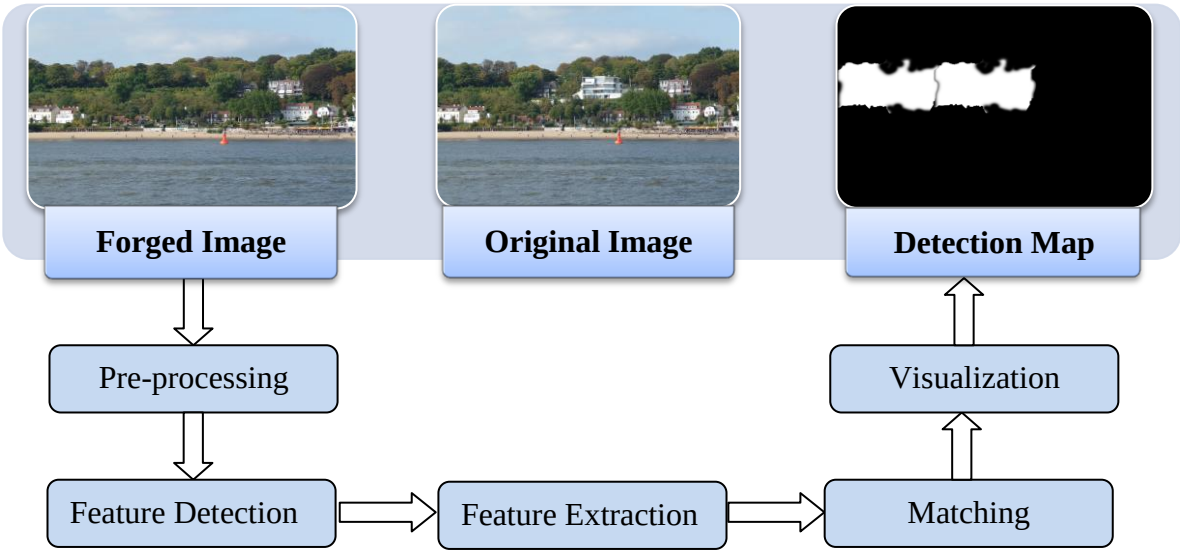


Figure 1.7 Common Pipeline of Copy-move forgery detection techniques

- Pre-Processing: The first and optional stage of CMFD process is pre-processing. In preprocessing, the undesired distortions are suppressed and certain image features are enhanced in order to improve the image data. In most cases, RGB (Red, Green, and Blue) color channels are simply converted to grayscale images in preprocessing.

- Feature Detection: After pre-processing stage, features are detected either through block-based method or through key-points based methods:

  In **Block-based** approach, the image is divided into overlapping or non-overlapping blocks of square or circle to analyze it for further feature detection process.
  In **key-point based** approach, the distinctive image features are extracted such as corners, edges, and blobs from the image using different key-points detection techniques [16].

- Feature Extraction: After feature detection, the characteristics of interest around the key-point are represented by a feature vector to give unique identity to each key-point separately.

  In **block based approach**, the features such as pixel intensities are extracted from each block separately and then to find the similarity between different blocks, the comparison is made against each other within the image as shown in Figure 1.8.

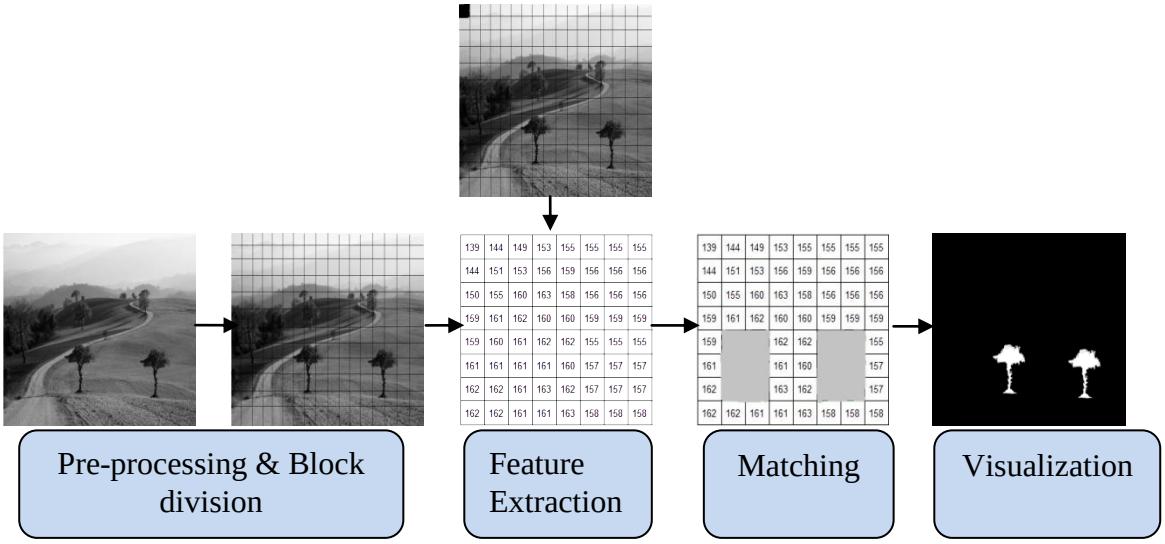


Figure 1.8 Detection Process in Block-based approach

In **key-point based approach**, each keypoint is uniquely represented with a set of feature vector or descriptor considering characteristics within a small region around the keypoint. The reliability of the features to transformations is increased by representing it in the form of a descriptor vector. The key-point detection process is shown in the Figure 1.9.

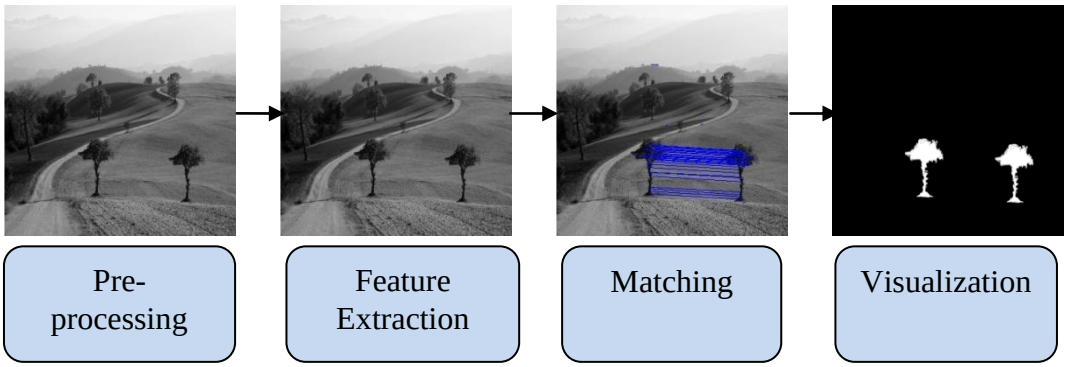


Figure 1.9 Detection process in Key-point based approach

- Matching: Feature extraction is followed by the matching stage to find out the similarities between different feature vectors of an image. In this stage, the modifications made in an image to create a forgery are determined. The matching techniques are mainly executed by block-based methods or keypoint-based methods depending upon the extracted features. For example, block matching is performed for DCT (Discrete Cosine Transform) features while best-bin-first algorithm is applied for keypoint based features to find the nearest neighbor from all the points in the feature space.
- Visualization: Finally, the copied regions are located and displayed in the forged image during the visualization stage. Morphological operations are applied to refine the visualization by utilizing the shape properties such as contours, skeletons and convex hulls [17].

Hence, these basic steps are utilized in both block-based and key-points based techniques to effectively detect the Copy-Move forgery in digital images.

1.6 ORGANIZATION OF THESIS

This dissertation represents how copy-move forgeries in digital images can be detected effectively and accurately. The organization of thesis is as follows:

Chapter 1 includes short summary of the basic concepts of forgery in digital images, its applications in today's digitized world, various types of forgery and the need for authenticating digital images. Then the most prevalent type of forgery i.e. Copy-move forgery is discussed in detail along with basic workflow to detect copy-move forgery and proving the authenticity and integrity of images.

Chapter 2 discusses the work done in the field of copy-move forgery, various active and passive authentication techniques proposed and different methods utilized to detect these forgeries. The techniques proposed so far and the related research papers are also discussed in sequence.

Chapter 3 provides an outline of various key-point based detection methods including Shi-Tomasi corner detector, Speeded-Up Robust Features (SURF) and an optimization algorithm known as Particle Swarm Optimization (PSO). These methods are explained thoroughly with the help of flow diagrams and analytic equations.

Chapter 4 introduces the proposed methodology based on hybrid technique incorporating Shi-Tomasi corner detector and SURF descriptor to detect copy-move forgery in digital images. The results simulated are presented and compared with the standard techniques existing so far.

Chapter 5 presents another proposed forgery detection technique based on SURF algorithm along with PSO. A complete analysis of integration of SURF with PSO has been presented. The results simulated are also provided to prove the effectiveness of proposed algorithm as compared to conventional forgery detection technique.

Chapter 6 provides conclusion of this dissertation as well as directions for future work.

CHAPTER 2
LITERATURE REVIEW

With the tremendous utilization of digital images and the accessibility of capable image editing tools like Photoshop, it has become very easy to modify the contents of the digital images and create forgeries that are not visible to a naked eye. These manipulations may change the entire semantics of an image. Hence, digital images have lost their trust. Therefore, in order to prove the genuineness and integrity of digital images, Digital Image Forensics has been appeared as an investigation field to detect such forgeries in digital images. It has turn out to be very important to verify the uniqueness of content since digital images are utilized in numerous applications including criminal investigation, forensic studies, law enforcement and journalism etc.

For the past few years, several techniques have been developed to identify copy-move forgery in digital images. The various techniques established on active authentication and passive authentication methods are presented in this section. Furthermore, the techniques are also divided into two groups based upon the type of features extracted and used for matching i.e. block-based and keypoint-based approaches.

2.1 ACTIVE AUTHENTICATION

In active approach, prior knowledge about a unique or original image is required. It uses a known authentication code sent with it or embedded into an image in the form of name, signature, date, etc. for assessing the authenticity of the image. It is mainly based on- digital signatures and watermarking techniques. The various active authentication techniques presented so far by different researchers are as follows:

A novel scheme for lossless authentication watermarking, in which zero distortion reconstruction of the un-watermarked images upon verification is empowered has been presented by **Celik** *et al.* [12]. Instead of prior lossless verification techniques that demanded recreation of the original image preceding verification, the new framework permits acceptance of watermarked images before recovery of the original image. This technique offers efficiency in terms of computation, public/private key support and enhanced tamper-localization exactness. This framework can likewise be effortlessly implemented using other fragile authentication and lossless data embedding strategies.

Saha *et al.* [18] specified a popular technique known as Watermarking for image authentication and copyright enforcement. Various types of watermarking such as 1) fragile watermarks 2) semi-fragile watermarks are also discussed. Some conceivable attacks that

may cause harm to the present watermarking procedures are presented. However, how to protect multimedia documents and valuable images is not discussed in detail.

Cao *et al.* [6] demonstrated a survey on Contrast Enhancement-based forgery detection in digital images. In contrast enhancement, the contrast and global brightness of images is changed. Malicious clients may locally create a sensible composite image by performing various Contrast Enhancements. Accordingly, it is crucial to detect contrast enhancement aimlessly to validate digital images. Two algorithms have been proposed to recognize the manipulations based on contrast enhancement in digital images. One in view of detection in which global contrast enhancement is applied to the compressed images and another in light of recognizing the composite image made by authorizing adjustment in contrast on either one or both source and pasted regions. In any case, the proposed strategy could work especially well when contrast enhancement is performed as the last step of manipulation.

2.2 PASSIVE AUTHENTICATION

In passive authentication, no additional information regarding the original image is required to verify the originality of an image. It uses the forged image itself and hence it is automatic. The passive authentication techniques studied by different authors are as follows:

Elwin J *et al.* [11] gave a brief review of a portion of the most recent passive tampering detection methods. A passive method is fit for distinguishing image forgery with no earlier data about the image or its source and it identifies altering by recognizing changes in the image properties like irregularities in lighting and when mathematical properties of original digital images are changed. Despite the fact that each of the strategies examined are equipped for recognizing image forgery effectively, a portion of the techniques are observed to be image sensitive. In addition, they are also observed to be tampering sensitive i.e. they are capable of recognizing just a specific sort of altering and not a wide range of altering.

Qureshi *et al.* [9] demonstrated that with the invent of capable image editing tools, manipulating and changing the contents of an image is turning into a minor task. With more than a few million pictures transferred every day to the internet, and the launch of e-Government administrations, it has become critical to invent strong detection methods to identify image forgery operations. Here, the blind image forensics detection methods are classified into six general categories: pixel-based, format-based, camera-based, source camera identification-based, physics-based and geometric-based. In any case, a considerable lot of the techniques talked about here require some type of suspicions to give efficient detection results.

2.3 BLOCK-BASED TECHNIQUES

The block based detection techniques simply divides an image into various overlapping/non-overlapping rectangular or circular blocks of fixed size.

The recent developments in Copy Move Forgery Detection and the entire process involved in Copy-move forgery detection has been described by **Warif** *et al.* [17]. The common detection framework of feature extraction and matching process utilizing block-based or keypoints-based approaches has been characterized. Furthermore, the classification of copied regions to determine their relevancy in existing CMFD techniques has been done. It has been discussed that how advances in big data solutions could be influenced to solve CMFD challenges.

The widely used block based techniques are:

2.3.1 DCT-Based Techniques

The simplest and most common approach that is utilized to find forged regions in an image is exhaustive search presented by **Fridrich** *et al.* [19], where all the cyclic-shifted versions of an image are measured for similarity with the image itself to locate the nearest matching regions. In spite of the fact that this method works for region duplication location, it is not used in practical applications because of its high computational burden. To diminish the computational time, block-matching method is proposed. In this approach, a picture is differentiated into various overlapping blocks of determined size and features extraction is done to further utilize them in matching with other features of each block. A match indicates the probability of forgery. For the first time, the copy-move forgery recognition procedure named Discrete Cosine Transform (DCT) on compact overlapping blocks has been presented in this paper and to recognize the copy-move blocks lexicographic sorting has been adopted.

The enhanced variant of previously presented DCT, utilizing just 25% low energy DCT coefficients was proposed by **Huang** *et al*. [20]**,** figured for each square. To lower the dimension of feature vectors, truncation is done and then the lexicographical sorting of feature vectors is employed to match the similar features in the matching step. Furthermore, a scheme to judge whether two feature vectors are similar is suggested to make the method more robust. This method is robust to various distortions, for example, JPEG (Joint Photographic Experts Group) compression, addition of AWGN (Additive White Gaussian Noise) noise and blurring.

Zhao *et al.* [21] presented a more robust technique to detect forgeries in similar or flat regions in an image. The proposed technique is based on Discrete Cosine Transform (DCT) and Singular Value Decomposition (SVD). Initially, it works by dividing the image into overlapping blocks of fixed size and then applying 2D-DCT to each extracted block. Then,

the quantization of DCT coefficients is performed. Secondly, SVD is applied to each block after dividing the image into non-overlapping blocks of fixed size. Then by using largest singular value, features are extracted, lexicographically sorted and are then finally matched by using predetermined frequency shift threshold to reveal the forged regions. This method is also robust to various distortions and also the mixed operations of compression, blurring and noise addition.

2.3.2 PCA-Based Techniques

To reduce the dimensionality of computed feature vectors of each image block, **Popescu** *et al.* [22] suggested a technique known as Principal Component Analysis (PCA) to increase the speed of feature matching process. In this technique, PCA is implemented on small fixed sized blocks of an image for dimension reduction. This scheme is robust to various minor changes in an image that arise due to some noise or compression. Also, the false positives (i.e. the regions erroneously marked as forged) detected by PCA are very less. But this method is not efficient for detecting low JPEG quality images and small block sizes.

2.3.3 LBP-Based Techniques

AlSawadi *et al.* [23] introduced a detection technique based on Local Binary Pattern (LBP) and neighborhood clustering. Initially, decomposition of the image to three color components is done and then each color component is divided into overlapping blocks of equal size. Then, calculation of LBP histograms is done for each block and also histogram distance is computed between blocks. The minimum distance block-pairs are retained and if the selected pairs exist in all the color components present, they are termed as primary candidates. To reduce the false positive rates, 8-connected neighborhood clustering is applied. However, this method does not perform well when the copied part is rotated to some degree and scaled by some factor simultaneously.

An effective method known as Multi resolution Local Binary Patterns (MLBP) for detecting tampering artifacts has been presented by **Davarzani** *et al.* [24]. This technique is useful in estimating geometric transformations of copy-moved regions and is also robust to illumination and geometric distortions. In this approach, after dividing the image into different blocks, LBP features are extracted for each block and then they are sorted lexicographically. Matching stage utilizes k-d tree algorithm for reducing computational time and also for revealing duplicates regions. Then, Random Sample Consensus (RANSAC) algorithm is applied for estimating geometric transformation and removing outliers.

However, this method does not work when the copied region is rotated through arbitrary angles. Also, for detecting forgery in high resolution images, this method is still time consuming.

2.3.4 FFT-Based Techniques

Bayram *et al.* [25] presented an efficient scale and translation invariant technique based on Fourier Mellin Transform (FMT). Similar to other block-based techniques, image is fabricated into overlapping blocks and then the extraction of features is done using FMT. On applying Fourier transform to each block, the property of translation invariance is ensured. Then to generate feature vectors, the resulting magnitudes are re-sampled, projected and quantized into log-polar coordinates. This method proves to be rotation invariant for only small degrees of rotation. The feature matching process involves lexicographical sorting or using counting bloom filters. The efficient forgery is detected when within the same distance a certain number of similar blocks are present. This method is robust to rotations of up to 10 degrees and is also robust to JPEG compression.

2.3.5 Wavelet-Based Techniques

An arrangement of Wavelet functions for executing image compression framework and the advantages of this transform have been examined by **Grgic** *et al.* [26] The vital elements in compressing still images of wavelet transform, including the degree to which the nature of image is deteriorated by the procedure of wavelet compression and decompression has been studied. The impact of various wavelet functions, image contents and compression ratios have been surveyed. Additionally, comparison has been made amongst DWT and DCT.

Muhammad *et al.* [27] presented a blind forgery detection scheme based on Un-decimated Dyadic Wavelet Transform (DyWT). It is basically more efficient than Discrete Wavelet transform (DWT) technique because it possesses the property of shift invariance. In this, initially the original image is decomposed into two bands knows as approximation (LL1) sub-band and detail (HH1) sub-band. Then the block based technique is applied to these two bands i.e. the LL1 and HH1 sub-bands are differentiated into overlapping blocks. Eventually, resemblance is drawn between different blocks. The blocks from the LL1 band must possess high similarity whereas the blocks from HH1 band must possess high dissimilarity for effective matching. A threshold value is used to decide the matched pairs from the sorted list. Finally, the duplicated regions are localized. The experiments are conducted on images of fixed size with or without rotation applied and it is shown that it performs better than existing

wavelet based techniques. However, it is able to detect forgery up to small rotation angles only.

2.3.6 Moment-Based Techniques

A method based on mixed moments is presented by **Zhong** *et al.* [28] for improving the robustness of detection techniques. Initially, the low frequency information is extracted from an image utilizing Gaussian pyramid transform. Furthermore, the low frequency part is differentiated into overlapping blocks. Secondly, exponential and histogram moments are used to compose the eigen value of block and then it is sorted lexicographically. Thirdly, forged regions are positioned precisely based on space and Euclidean distances. Experimental results proved the robustness of this technique to various operations such as rotation, scaling, translation. Also, it is proved to be robust against mixed operations of contrast adjustment and brightness variation. However, the rotation angle, scaling factors and qualitative evaluation are not specified.

2.3.7 Texture and Intensity-Based Techniques

Hussian *et al.* [29] demonstrated a forgery detection technique based on multi resolution descriptor known as Weber law descriptors (WLD). Here, the conversion of an original image to YCbCr components is done at the first stage. The color information is stored in the form of chrominance and brightness. In the next step, chroma components i.e. Cb or Cr are utilized to extract the features of an image. To detect the texture in an image, Weber law is employed. Finally, SVM (Support Vector Machine) classifier is used to indicate whether the image is original or not. The experimental results prove that the multi-resolution WLD gives better results than single resolution WLD and is robust to various operations. But, it is complex in terms of computation for large sized images.

A technique based on intrinsic dimension estimation scheme is suggested by **Quan** *et al.* [30]. In this, images are considered as high dimensional information and then the image is segmented using estimation scheme to identify regions with same texture in an image. To approximate the local dimension, k-NN algorithm is utilized. The detection is carried out in image blocks rather than the whole image which reduces the computational complexity of the algorithm. The results prove that the technique is robust to various operations including blurring, retouching, filtering, lossy compression etc.

Muhammad *et al.* [31] proposed the same technique as presented by Hussain *et al.* [29] but with the difference that to extract the lower sub-band, un-decimated wavelet transform is

applied to the channel. Weber pattern known as multi-scale texture descriptor is computed from the sub-band. The histogram of Weber pattern is considered as a feature of the image. The classifier used in the framework is SVM (Support Vector Machine). This method proves to be superior in terms of accuracy.

2.4 KEY-POINT BASED TECHNIQUES

The key-points based approach extracts the distinctive local features from the image such as corners, blobs, and edges. Each feature is represented with a set of descriptor vector constructed utilizing a region around the keypoint. These extracted features are then matched against each other to locate the duplicated regions. Several key-point based methods have been developed depending upon the type of detector used to extract corners, blobs or edge-points discussed as:

An impressive number of various algorithms have been presented concentrating on various types of post processed copies by **Christlein** *et al.* [16]. It has been shown that which detection algorithms out of various block-based and key-point based method and processing steps (e.g., matching, filtering, outlier detection, affine transformation estimation) performs better in different post processing situations. The detection performance on per-pixel basis and per-image basis are examined. Experiments have demonstrated that the keypoint-based features SIFT and SURF, and additionally the block-based DCT, DWT, KPCA, PCA, and Zernike features perform exceptionally well. These feature sets exhibit the best robustness against various noise sources and down sampling, while dependably distinguishing the copied regions.

D. Lowe [32] presented a distinctive scale invariant and rotation invariant feature detector and extractor known as Scale-invariant feature transform (SIFT) to match similar objects or scenes of an image. This technique utilizes scale space and difference of Gaussian (DoG) process to identify interest points in an image. At each key-point location, orientation is allocated to each key-point depending upon gradient directions. Then, the scale, orientation and region around the keypoint are used to describe a 128-dimensional feature vector for each key-point uniquely. These feature descriptors are then matched using nearest neighbor search to locate the similarity between different objects or scenes. Features based on SIFT are robust to various illumination changes, addition of noise, 3D viewpoint changes etc.

A detailed description of scale-invariant and rotation-invariant detector and descriptor based on Speeded-Up Robust Features (SURF) is presented by **Bay** *et al.* [33]. It inhibits

advantages in terms of distinctiveness, robustness and computational complexity. This method can be compared and computed much faster than existing key-point based techniques. In this, image convolutions are performed by using integral images which drastically reduce the computational time. On the other hand, detector is computed using hessian matrix because of its good accuracy. Then, Haar wavelet responses are used to assign an orientation to interest points. Finally, 64-dimesional descriptor vector is calculated by utilizing circular region around the interest point. This method discovers great applications in the field of object recognition and camera calibration.

Amerini *et al.* [34] investigated the issue of identifying if an image has been forged or not. For the most part, to adjust the image patch to the new context, a geometric modification is required. To identify such manipulations, a novel approach in view of scale invariant features transform (SIFT) has been proposed. Utilizing such strategy, it can be comprehended if a copy-move attack has happened and, besides, to recover the geometric transformation used to perform tampering. Broad exploratory results are displayed to affirm that the method can accurately designate the altered area and furthermore to evaluate the geometric transformation parameters with high dependability. The strategy additionally deals with multiple cloning.

Pan *et al.* [35] demonstrated a region duplication detection technique for detecting forgeries when the regions have undergone some geometric or illumination transformations or distortions. Instead of matching image pixels directly to locate the forged regions, this method estimates the transform between the matched pairs of copied and pasted regions. SIFT based algorithm is employed for detecting and locating keypoints that are not sensitive to any kind of illumination and geometric distortions. RANSAC (Random Sample Consensus) algorithm is applied to estimate the affine transform between pairs of matched points. It is used to classify the matched pairs into inliers (truly matched keypoints) and outliers (falsely matched keypoints). Finally, duplicated regions are localized using region-correlation maps. The effectiveness of this technique is proved through series of experiments.

Pun *et al.* [36] presented a novel forgery detection scheme utilizing adaptive over-segmentation and feature point matching. First, host image is segmented into irregular and non-overlapping blocks adaptively as indicated by the given host images. Further, an appropriate block initial size is resolved to upgrade the accuracy of forgery detection results furthermore to decrease the computational costs. Then, feature points are extracted and Block Feature Matching calculation is proposed. This technique roughly shows the suspected

forgery regions. Then Forgery Region Extraction algorithm is proposed. Next, the morphological operation is connected to create the identified forged regions.

A region duplication detection technique robust to various geometrical transformations is proposed by **Chen** *et al.* [37]. The proposed method used Harris corner detector to detect interest points from an image. Then each key-point detected by Harris detector is represented in the form of feature vector by utilizing a small circular region around an interest point based on a method known as step order statistics. Furthermore, matching is performed by using Best-bin-first scheme to locate duplicated regions. The small circular regions are matched to reveal the forgery in this method. Moreover, this method performs very well even when the image has undergone some degradations or geometrical transformations.

Harris *et al.* [38] proposed a combined edge and corner detector constructed on auto-correlation method for image regions that contains isolated and texture based features. A corner is characterized as an area that manifest a strong gradient value in different directions at the same time. Edge hysteresis is carried out by applying various low and high threshold values and with these the continuity of edges is enhanced. This combined edge and corner detector performs better with good uniformity on natural imagery.

A technique based on SURF (Speeded up robust features) and HAC (Hierarchical agglomerative Clustering) is presented by **Mishra** *et al.* [39]. To reduce the time complexity, SURF utilizes integral images and less dimensions of descriptor vectors. Hence, matching process executes faster with less computational complexity. Feature descriptors are computed using Haar wavelets to make them invariant to illumination variations. HAC is implemented to describe the regions of forgeries from matched key-points. Although HAC is implemented easily but results obtained are not satisfactory in terms of TPR (True positive rate).

2.5 GAPS IN STUDY

Gaps found in reported literature on copy-move forgery detection techniques are listed below:

1. The block-based approaches posses high computational time than key-point based methods because in block-based scheme, the image is divided into number of overlapping/non-overlapping blocks and features are extracted and matched from each block separately which increases the computational time significantly [19, 25].

2. Many block-based approaches are not robust to various geometric transformations such as rotation, scaling, illumination changes, blurring, Gaussian noise addition and JPEG compression [25].

3. The key-point based methods are computationally less complex than block-based methods. But, due to high dimensional feature vector of key-point based technique SIFT, it becomes computationally expensive, in particular, for high resolution images [32].

4. The key-point based methods i.e. SIFT and SURF are unable to detect enough key-points in flat regions of an image. That is, if an image contains regions with inconspicuous changes, there exists limitation of detecting reliable keypoints [17].

5. Sometimes, forgery detection techniques are unable to differentiate between regions that are inserted intentionally to create a forgery or are naturally similar [40].

6. The accuracy of key-point detection techniques highly depend upon the pre-defined parameter values which are mostly determined with human perception and experience. Using pre-defined parameter values highly limits the application of copy-move forgery detection techniques [41].

2.6 OBJECTIVES

1. To study the basics of copy-move forgery and the different block-based and key-points based techniques that are used to detect forgeries in digital images.

2. To propose an effective methodology that can detect copy-move forgery when existing key-point based methods fails to detect any reliable key-points in flat and smooth regions.

3. To compare the results of the proposed methodology with the conventional techniques on the basis of number of truly matched points, detection accuracy, precision and recall rate.

4. To propose an adaptive and self-learning algorithm for optimization of the pre-defined parameters that are usually determined with human perception because of the limitations these pre-defined parameters impose on the detection accuracy of detection technique.

2.7 METHODOLOGY

The key contribution of this dissertation is to present an efficient copy-move forgery detection technique that is able to locate forgeries in flat and smooth regions in addition to detecting multiple forgeries in the same image. For this, a novel hybrid approach based on Shi-Tomasi detector and SURF descriptor has been proposed in this thesis. This approach works by detecting points of interest or key-points using Shi-Tomasi detector which is basically a modified version of Harris corner detector. Then the region description method based on SURF descriptor is employed to give unique identity to each detected key-point. The proposed method is proved to be better than the conventional SURF algorithm in terms of detection accuracy and the number of matched key-points. The proposed method not only detects copy-move forgeries in flat and smooth regions but also improves the accuracy and precision of detection. Also, the method is robust to various geometric transformations like rotation, JPEG compression, noise addition and illumination changes.

Another method is proposed in this thesis to deal with the limitation of pre-defined parameter values. The main reason behind such case is that the detection results of key-point based methods highly depend upon the parameter values which are mostly determined with experience. Therefore, the application of copy-move forgery detection gets limited due to these pre-defined parameter values (PPV) since they cannot be applied to each image. Therefore, a novel approach integrating SURF-based detection with Particle Swarm Optimization (SURF-PSO) has been presented. In this thesis, the performance enhancement of copy-move forgery detection by proposed algorithm has been validated by considering five different images. The results prove that the proposed algorithm outperforms the conventional copy-move forgery detection technique.

CHAPTER 3

SHI-TOMASI DETECTOR, SURF AND PSO

In the section, various key-point based techniques such as Shi-Tomasi corner detector, Speeded-Up Robust Features (SURF) has been explained and discussed thoroughly. Also, an optimization algorithm known as Particle Swarm Optimization (PSO) has been demonstrated in this section. The details are as follows:

3.1 SHI-TOMASI CORNER DETECTOR

A corner is characterized as an area that manifests a strong gradient value in different directions at the same time. The Shi-Tomasi Corner Detector is entirely based on Harris [38] corner detector. However, a slight variety in its choice criteria made this better than the original. The initial step is to acquire the first partial derivative i.e. I_x , I_y in both horizontal and vertical directions of the image function *I(a,b)*, based on the approximations (3.1) and (3.2).

$$I_x(a,b) = \frac{\partial I(a,b)}{\partial x} \tag{3.1}$$

$$I_y(a,b) = \frac{\partial I(a,b)}{\partial y} \tag{3.2}$$

The autocorrelation matrix M is obtained by convolving I_x^2, I_y^2 and I_xI_y with a Gaussian window as represented by (3.3) and (3.4).In the following equations, the convolution operator and Gaussian window are represented by $*$ by W, respectively:

$$I_x^{2'} = I_x^2 * W;\;\; I_y^{2'} = I_y^2 * W \;;\; I_xI_y' = I_xI_y * W \tag{3.3}$$

$$M = \begin{bmatrix} I_x^{2\prime} & I_xI_y{}' \\ I_xI_y{}' & I_y^{2\prime} \end{bmatrix} \tag{3.4}$$

The determinant and trace of matrix M are utilized to calculate the cornerness value C(x,y) as shown in Eq. 3.5 and Eq. 3.6:

$$Det(M) = \alpha\beta = \left(I_x^{2'} I_y^{2'}\right) - (I_xI_y)^2, Tr(M) = \alpha + \beta = I_x^{2'} + I_y^{2'} \tag{3.5}$$

Here; $\alpha \; and \; \beta$ are eigen values of M.

Therefore cornerness value can be determined as:

$$C(x,y) = Det(M) - k \times Tr^2(M) \tag{3.6}$$

where C(x,y) is positive, negative and very small in corner regions, edge regions, and flat regions, respectively. The coefficient k, in practice, has a fixed value in the range of say 0.04 to 0.06. The conceptual idea of Harris corner detector is shown in Figure 3.1.

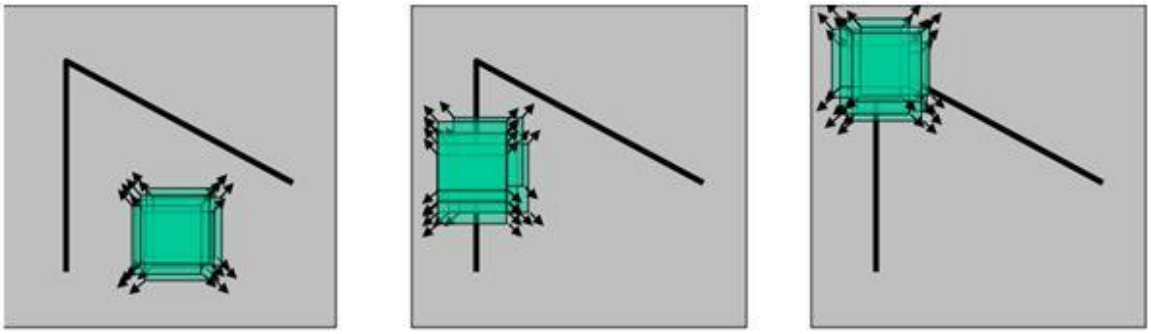


Figure 3.1 Conceptual idea of the Harris corner detector. Left: flat area, no change. Middle: Edge, no change along the edge. Right: Corner, change in all directions.

Shi and Tomasi [42] modified the response function C(x,y) a little and it is given by Eq. 3.7

$$C(x, y) = \min(\alpha, \beta) \tag{3.7}$$

If C(x,y) is greater than a given threshold λ, a corner is found. It can also be written as if min(α,β) > λ, corner or keypoint is detected.

3.2 SPEEDED-UP ROBUST FEATURES (SURF)

Speeded-Up Robust Transform is an interest point detector and descriptor which is basically scale and rotation invariant. It is faster version of Scale-Invariant Feature Transform (SIFT) descriptor. It has many applications in the field of object recognition, classification or 3D registration and image registration. SURF algorithm consists of two main steps: Key-point Detection and Feature extraction which are explained as follows:

3.2.1 Key-Point Detection

Keypoint Detection involves detecting points of interest from an image by utilizing the concept of integral images. For obtaining Gaussian-smoothed images, square-shaped filters are used in SURF and using integral images makes the process of filtering much faster.

$$S(i,j) = \sum_{x=0}^{x \le i} \sum_{y=0}^{y \le j} I(x,y) \tag{3.8}$$

Sum of all the pixels within a rectangular region in the input image I can be quickly computed using Integral image $S(i,j)$ using the location (i,j) and the origin. It requires evaluating the sum of four corners of the rectangular region.

The interest points in SURF are found using a blob detector established on Hessian matrix. The blob-like structures are detected at the points where the value of determinant of Hessian

matrix is maximum. Also, the determinant of this matrix is utilized for the selection of scale. For a point $t = (a, b)$ in any image I, the matrix *H(t,σ)* based on Hessian at point t and scale σ is demonstrated as:

$$H(t,\sigma) = \begin{bmatrix} L_{xx}(t,\sigma) & L_{xy}(t,\sigma) \\ L_{xy}(t,\sigma) & L_{yy}(t,\sigma) \end{bmatrix} \quad (3.9)$$

Here, convolution of Image $I(x, y)$ with second derivative of Gaussian at point x is denoted by $L_{xx}(t, \sigma)$. To find the approximation of Gaussian smoothing with σ=1.2, the box filter of particular size i.e. 9×9 is used. This is basically the highest spatial resolution for blob-response maps.

To incorporate scale invariance, the interest points or key-points are found at various scales. For constructing image pyramid, Gaussian filter is applied to repeatedly smooth the images. In SURF, box filters of various sizes are applied to construct the scale spaces. Instead of reducing the image size, the size of filters is up-scaled for analyzing the scale-space. The filter size of 9×9 is viewed as an initial layer of scale space with scale = 1.2. The higher levels of scale space are obtained by using filters of bigger masks. The sizes of filters used are 9×9, 15×15, 21×21, 27×27 and so on. The interest points are localized in a 3×3×3 neighborhood of an image and over scales by non-maximum suppression. Then, the maximum value of the determinant of *H(t,σ)* are interpolated in scale space to localize the interest points.

3.2.2 Feature Extraction

This section represents the region description method which describes how the intensity content is distributed within the neighborhood of interest point. To describe each feature, the pixel data within a local neighborhood around a keypoint is outlined. At first, the convolution of the pixels in the neighborhood of a keypoint is performed with the Haar wavelet filters as shown in Figure 3.2 i.e. both the horizontal and the vertical filters are used to calculate the orientation for each feature. Using these filters, the directional derivatives of the image intensity are calculated. By utilizing intensity changes to characterize orientation, features are described by this descriptor in the similar way paying little heed to the specific orientation of camera or of the objects and hence making it rotation invariant. Since, to represent each feature and its neighborhood, a unit vector is generated by using Haar wavelet responses, acquiring two attractive properties: lighting and contrast invariance.

Figure 3.2 Haar wavelet filters [33] for computing the responses in x (left) and y direction (right).

To compute the orientation, the convolution of two directional Haar wavelet filters of size 4s is computed with 12s×12s square region positioned about location of each feature where s is the scale at which the key-point is detected. After computing the Haar wavelet responses, they are Gaussian weighted utilizing standard deviation of 2s. Then, they are translated as points in two dimensional planes. The algorithm then searches for a contiguous region, for which the sum of all the horizontal and vertical responses are maximal, spanning 60^0 within this plane. Finally, the dominant orientation is recognized as the centre of 60^0 window containing the strongest response.

Once the orientation direction has been determined, descriptor vectors are constructed using the square regions around the interest points. To retain some spatial data, the windows are split up in 4 × 4 sub-regions. Haar wavelets are extracted in each sub-region at regularly spaced sample points. To provide robustness against geometric deformations and localization errors, the responses of the Haar wavelets focused at the interest point are weighted with a Gaussian. Finally, the summation of the wavelet responses is done over each sub region in horizontal and vertical direction denoted as d_x and d_y respectively. Furthermore, the summation of absolute values $|d_x|$ and $|d_y|$ is computed to acquire data about the polarity of the image intensity variations. Subsequently, the underlying intensity pattern is traced by a vector for each sub-area,

$$V = \left(\sum d_x, \sum d_y, \sum |d_x|, \sum \left|d_y\right|\right) \tag{3.10}$$

The final descriptor vector is of length 64. This way of representing the descriptor vector for distinctive image intensity patterns is displayed in Figure 3.3.

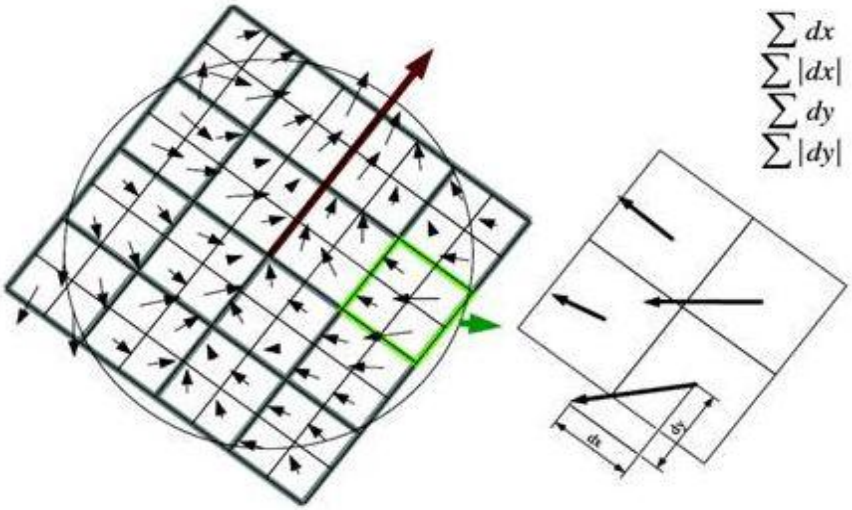


Figure 3.3 To build SURF descriptor, over the keypoint [33], an oriented quadratic matrix is laid with 4 × 4 square sub-areas (left). The wavelet reactions are processed for each square, from 5 × 5 samples (for illustrative purposes, 2 × 2 sub-divisions are presented here). For each field, the summations dx, |dx|; dy, and |dy | are figured relatively to the orientation of the grid (right).

Thus, SURF implementation reduces the length of descriptor vector and hence the speed of computation is improved and matching can be performed way faster than SIFT.

3.3 PARTICLE SWARM OPTIMIZATION (PSO)

Particle Swarm Optimization is swarm intelligence meta-heuristic algorithm inspired by the social hunting (foraging) behavior of some animals, in particular, flocking act of birds and schooling conduct of fish [43]. Particles of the swarm generally follow the fittest members of the swarm then they fly and bias their movement toward global best areas of their environment.

The main aim of the PSO algorithm is to locate the optimum value of all the particles in a multi-dimensional search space. The algorithm starts by creating initial swarm of particles and then assigning random initial positions and velocities to all the particles in search space. The objective function is evaluated at each particle's position to determine the best value of function and best location of the particle. The new velocities are chosen based on the current velocity, individual best location of the particles and their corresponding neighbor's best positions. Then, the locations, velocities and neighbors of the particles are iteratively updated till the algorithm reaches the stopping criteria. At the end, the particles converge or cluster together around an optimum best value or several optima.

3.1.1 Algorithm of PSO

The PSO algorithm [44] consists of group or swarm of particles continuously moving around the search space in search for optima. The particle's position and velocity is updated based on two best values in each iteration. The first one is *pbest* which means the best fitness value

achieved by the particle so far. Another one is *gbest* which means the global best value achieved by any particle in the search space so far. Based on these best values the particle's velocities and positions are updated are shown in Equations (3.11) and (3.12)

$$v_i(a+1) = v_i(a) + c_1 \times rand() \times \left(p_i^{Best} - p_i(a)\right) + c_2 \times rand() \times (p_{gBest} - p_i(a)) \quad (3.11)$$

$$p_i(a+1) = p_i(a) + v_i(a+1) \quad (3.12)$$

Where $v_i(a+1)$ represents new or updated velocity of i^{th} particle, the weighing coefficients are represented by c_1 and c_2 for the personal and global best positions respectively. $p_i(a)$ is the position of i^{th} particle at time a, $p_i^{Best}$is the best known position of i^{th} particle and p_{gBest} is the global best position known to the swarm and $rand()$ creates a random variable $\in$ [0,1]. The flowchart of PSO algorithm is shown in Figure 3.4

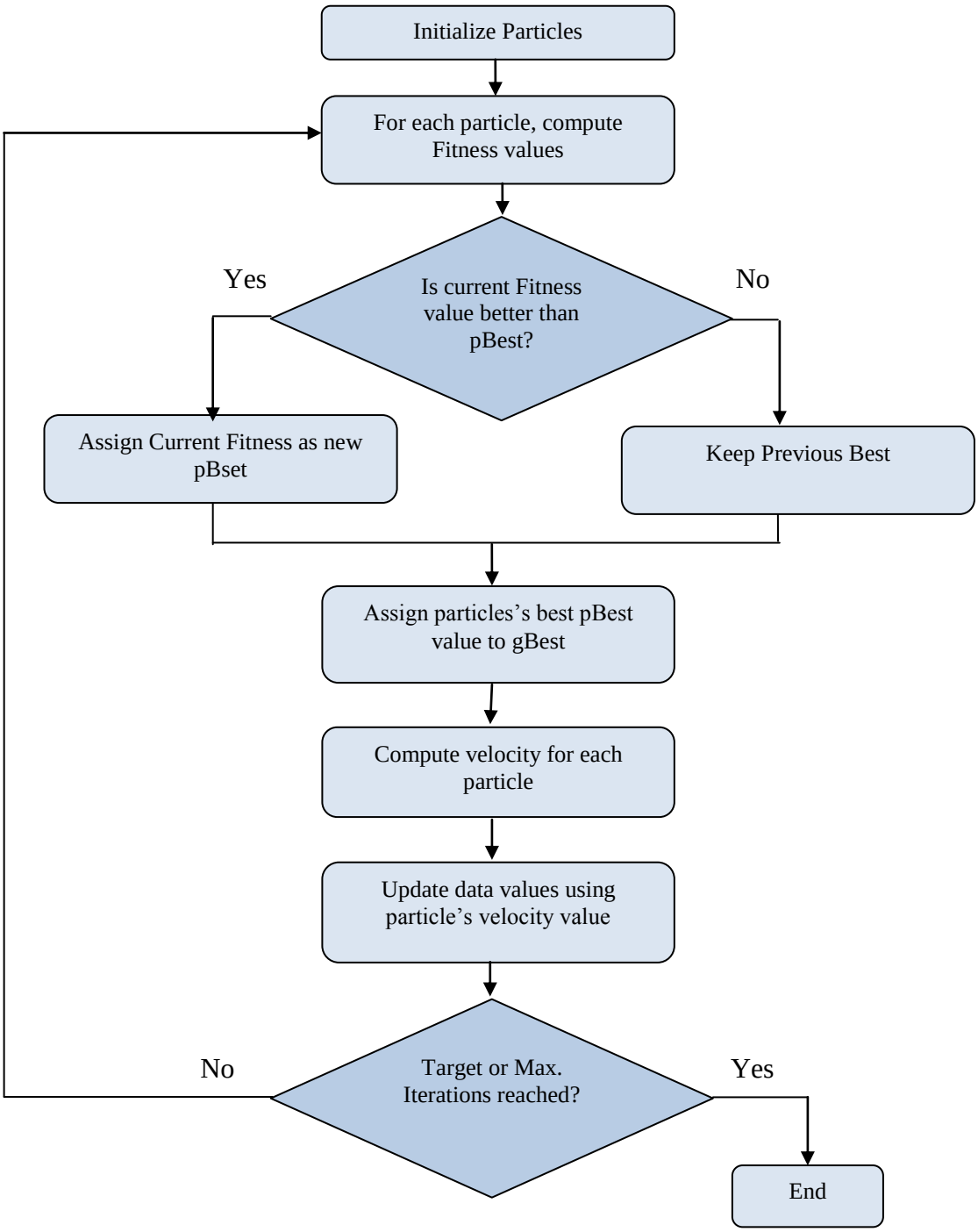


Figure 3.4 Flowchart of Particle Swarm Optimization Algorithm

This algorithm works as follows:

Initially, a population of particles uniformly distributed over search space is created. The size of the population is usually set between 10 and 50. Then, the objective function on the basis of which optimization is to be performed is defined. The particle's position, velocity, pBest and gBest values are initialized to random values. After that, each particle's position according to the objective function is evaluated. If a particle's current position is better than its previous best position, it is updated as its pBest. Then, the best particle according to the particle's previous best positions is determined. The particle's velocities are updated and

particles are moved to their new positions according to the evaluation criteria. The process is repeated until stopping criteria is satisfied.

In this way, the optimized solution is obtained. Therefore, PSO is utilized in numerous applications in the field of training neural networks and performing structural optimization.

Hence, the key-point based detection method Shi-Tomasi, SURF and an optimization technique PSO has been explained in this section. These methods are further utilized to create new methodologies: One based on hybrid of Shi-Tomasi detector and SURF descriptor and the other one based on integrating SURF based framework with PSO algorithm to detect copy-move forgery effectively. The proposed methods based on these algorithms are discussed in the next sections.

CHAPTER 4
HYBRID OF SHI-TOMASI DETECTOR AND SURF DESCRIPTOR

One of the major drawbacks of existing keypoints based method SURF is its inability to detect a small copied region in an image. Also it fails when keypoints detected are too less. A very introductory work based on SURF features was proposed in [39]. However, no estimation of applied geometric transformation parameters is performed and furthermore, no results are provided to evaluate the real performances of the methodology (e.g. TPR, FPR). Most of the methods based on SIFT and SURF features lack reliable keypoints to mark the regions as forged.

The SURF algorithm detects the keypoints only around the regions with significant changes while for the regions with inconspicuous changes, very few keypoints are detected. Also, the detected keypoints are scattered unevenly throughout the image making it difficult to identify the proper shape of the forged region.

Therefore, a hybrid technique based on Shi-Tomasi detector (Minimum-Eigen value detector) and SURF descriptor for detecting forgery in digital images is proposed in this section. Minimum-eigen value interest points are dispersed almost equally through the entire image and also it is able to detect sufficient keypoints for successful forgery detection where SURF almost fails to detect any. Thus, the proposed strategy can effectively identify regions with unnoticeable changes with enhanced accuracy and high detection efficiency. This method is likewise powerful to different operations, for example, Gaussian noise addition, JPEG compression, light or illumination changes and rotation.

4.1 PROPOSED HYBRID DETECTION TECHNIQUE

This section presents the proposed method to identify duplicated regions in the forged images in detail. The first step consists of image keypoint detection using Shi-Tomasi Detector. The second step includes region description method using Haar wavelet responses, while the third one is devoted to extracting features using SURF and keypoint matching followed by geometric transformation estimation and detection of multiple copy-move forgeries. The whole procedure is summarized in Figure 4.1 which illustrates the main steps of proposed detection technique.

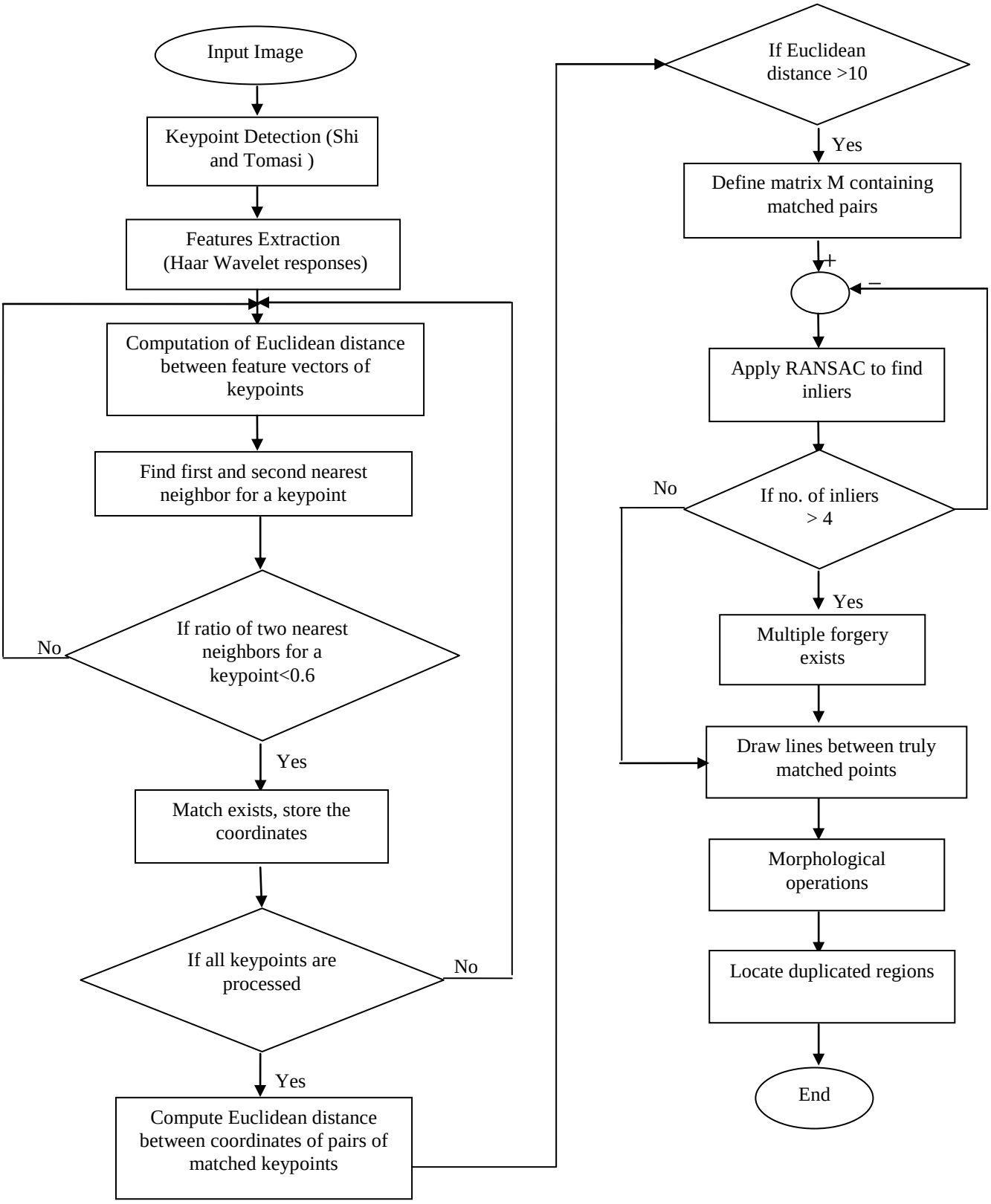


Figure 4.1 Algorithm of Hybrid Detection Technique

In this proposed methodology, the points of interest or keypoints are detected by using modified version of Harris corner detector i.e. Minimum Eigen value detector or Shi-Tomasi detector as explained in Section 3.2. This method utilizes partial derivatives of image function, convolution with respect to Gaussian window to calculate the autocorrelation matrix. Hence, the eigen values of this matrix are further utilized to decide whether a given point is a corner or not.

Once the keypoints are obtained, the region description method is utilized to describe the distribution of intensity content within the neighborhood of interest point. Therefore, the detected keypoints are represented by a 64-D descriptor vector based on Speeded-Up Robust Features (SURF) and further matching is done based on these descriptor vectors.

The matching of the detected keypoints based on their descriptor vector is tentatively done using the Best-Bin-First algorithm [37]. A set of keypoints $K= \{k_1, k_2, \ldots k_n\}$ with their corresponding feature vectors $V=\{v_1, \ldots\ldots v_n\}$ are extracted for the test image, where n is the number of keypoints. A matching operation among the feature vectors is performed to detect same regions in the test image. For each keypoint k_i, the Euclidean distance with respect to all the other (n-1) keypoints in the search space is computed and then based upon minimum Euclidean distances; its nearest neighbor is listed. This criterion of finding the minimum distance between two descriptors and then comparing it with some global threshold does not yield good results. Therefore, a more efficient method that computes the ratio of first and second nearest neighbors of every keypoint is compared with a threshold T (often fixed to 0.6), as suggested in [18]. For every keypoint, a similarity vector $D = \{d_1, d_2, \ldots d_n\}$ is defined in which the distance with respect to other keypoints is listed in sorted manner i.e. in ascending order. The condition for keypoints to be matched is:

$$\frac{d_1}{d_2} < T \text{ where } T \in (0,1) \tag{4.1}$$

In this, d_1 and d_2 are first and second elements of the sorted matrix for every keypoint This procedure is popularly defined as 2NN test. Finally, a set of matched points is obtained after performing different iterations.

Furthermore, the matched points that are lying very close to each other needs to be eliminated because they represent the areas that are similar but not copied. This elimination is done by computing the Euclidean distance between coordinates of matched descriptors. Only those matches are retained for which the computed distance is greater than some particular threshold value (taken as 10) and are saved for further processing.

At the point when an image has been declared as forged, the next step is to estimate the geometrical transformation utilized between the first copy-moved pair. The transform estimation function estimates an affine transform matrix H when inputted by a set of matched points. The geometric relationship is described by H which is a 3×3 matrix, between two points (a,b) and (a',b') as:

$$\begin{bmatrix} a' \\ b' \\ 1 \end{bmatrix} = \mathrm{H} \begin{bmatrix} a \\ b \\ 1 \end{bmatrix} \tag{4.2}$$

At least three matched points are needed to compute this matrix. However, the estimated homography can be severely disturbed by mismatched points (outliers). For this reason, Random Sample Consensus algorithm (RANSAC) [45] is presented to perform the previous estimation. In this, a set (usually three pairs) from the matched points is selected to estimate the homography H, then all the remaining points are transformed according to H and comparison is done with respect to their corresponding matched points in terms of distance. Inliers or outliers are catalogued according to this distance, if it is below or above a certain predefined threshold β respectively. Number of iterations N_{iter} is listed and then the estimated transformation which gives higher number of inliers is chosen. Here, N_{iter} has been set to 1000 and the threshold β to 0.05.

For images, containing multiple duplicated regions, a separate algorithm is proposed where RANSAC method is run iteratively and in each iteration, matched points satisfying particular type of geometric transformation known as inliers, are selected. After identifying a pair of duplicated region, RANSAC algorithm is run again and the new transformation matrix satisfying the second pair of duplicated region is calculated giving new inliers but this time with inliers in previously detected duplicated regions rolled out from the search. In other words, inliers from previous iteration are excluded from the next round of detection. Hence, more significant duplications which give more no. of inliers are detected first, followed by the ones which are less significant and with smaller area. Finally, when numbers of inliers left are less than 3, the RANSAC algorithm stops because this algorithm needs at least three non-collinear pairs to estimate the transformation between original and forged areas. As the last step, all matched pairs corresponding to different duplicated regions are combined together and mapped to the original image coordinates. As a final post processing step, coordinates of matched points are used to localize the forged regions. The keypoint based techniques utilize mathematical morphological operations [45] to connect and fill the boundaries of the detected forged features as a final step of detection.

4.2 METRICS FOR PERFORMANCE EVALUATION

To assess the adequacy and robustness of the proposed detection technique, a series of tests are performed. In the accompanying analyses, to test the proposed strategy, the image dataset in [27] is utilized. This dataset depends on 48 high-determination uncompressed PNG genuine color images and the normal size of the images in the dataset is 1500 × 1500. In the dataset, the copied regions extend from excessively smooth to exceedingly textured and are from the classifications of living, nature, man-made and blended. Likewise, the copy-move forgeries are made by duplicating, scaling and rotating semantically significant image regions. In summary, the dataset has 1826 pictures altogether, which are practical copy-move forgeries. Along these lines, we picked this dataset to objectively test our method.

Practically, the most significant property of a detection technique is its capability to discriminate forged and authentic images. In addition to this, the power of locating the forged area correctly is also very important to expose digital forgeries. Accordingly, the validity of our method is calculated at two levels: at image level, where we are anxious about the way that the detected image is really a forged image, and at pixel level, where we assess how precisely the forged areas can be found. To demonstrate the effectiveness and accuracy of the proposed strategy at image level, the calculation of precision "p" shows the likelihood that an identified forgery is for sure a forgery; and recall "r" signifies the likelihood that really a forged image is detected.

$$p = \frac{T_p}{T_p + F_p} \tag{4.3}$$

$$r = \frac{T_p}{T_p + F_n} \tag{4.4}$$

Here; T_p represents the total number of accurately detected forged images, F_p denotes the aggregate number of authentic images erroneously detected as forged, and F_n represents the total number of forged images incorrectly missed.

To demonstrate the exactness at pixel level the true positive rate (TPR) and the false positive rate (FPR) are figured as follows:

$$TPR = \frac{|\emptyset_s \cap \emptyset_s^{'}| + |\emptyset_f \cap \emptyset_f^{'}|}{|\emptyset_s| + |\emptyset_f|} \tag{4.5}$$

$$FPR = \frac{|\emptyset'_s - \emptyset_s| + |\emptyset^{'}_f - \emptyset_f|}{|\emptyset'_s| + |\emptyset'_f|} \tag{4.6}$$

Where; $\emptyset_s$ represents the pixels of original area, $\emptyset_f$ denotes the pixels of forged area, $\emptyset_s^{'}$ represents the pixels of detected original area, and $\emptyset_f^{'}$ denotes the pixels of detected forged area. Hence, the TPR shows the performance of technique by correctly identifying the pixels of the copy-moved areas in the duplicated image, while FPR reflects the pixels which

are not contained in forged region but are rather erroneously included by the implemented technique. Therefore, both the above parameters point out how accurately the proposed technique can locate duplicated areas. The more the TPR is near to 1 and FPR to 0, the more precise and effective the method would be.

In addition to precision and recall, the performance of proposed scheme is also evaluated on the basis of number of matched points detected. The comparison of the results of our proposed algorithm is done with previously existing detection method based on SURF. The main problem of keypoints based method SURF is its weakness to detect the forgery if forged region does not accommodate any significant keypoints.

4.3 RESULTS AND DISCUSSION

- Detection under Plain Copy-Move Forgery: In this part, the forged region is just copied, moved and pasted somewhere else in the same image without any distortion. The visual results of both the proposed and SURF method are presented in Figure 4.2. The number of matched keypoints is also given to compare the methods figuratively. Table 4.1 shows the detection results of 48 images when under plain copy-move, at the image level. No. of matched keypoints are also listed to compare the methods quantitatively. The results show that the SURF based forgery detection method matches total 256 keypoints for a particular image whereas the proposed method matches 580 keypoints. Visual results also support the numeric results.

	Image1		Image 2		Image 3	
	SURF	PROPOSED	SURF	PROPOSED	SURF	PROPOSED
TPR	0.801	0.862	0.717	0.856	0.878	0.891
FPR	0.0333	0.0303	0.0198	0.0021	0.0099	0.0048
Matched points	256	580	106	169	64	141

Table 4.1 Detection under plain copy-move forgery

(a1) (b1) (c1)

(a2) (b2) (c2)

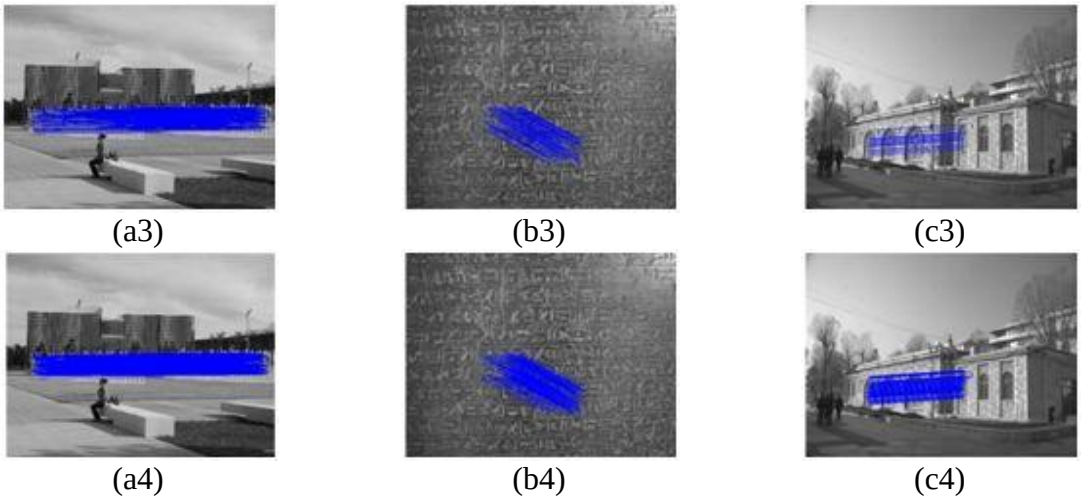


Figure 4.2: Detection under Plain Copy-move Forgery: Three host images from the dataset (a1)~(c1); the ground truth regions of the corresponding host images (a2)~(c3); detection results of SURF (a3)~(c3); detection results of the proposed method (a4)~(c4).

- Detection under Multiple Cope-Move Forgery: In this part, multiple regions are copied, moved and pasted somewhere else in the same image without any distortion. To detect and plot multiple forgeries in the same image, a new method is proposed where RANSAC method is run iteratively to estimate the different geometric transformations that different cloned regions satisfies. Each time the RANSAC algorithm is run, the number of matched points satisfying one transformation and one pair of copy-move forged regions are excluded from the next iteration. Therefore, different regions satisfying different transformations are plotted in the same image. The visual results of both the proposed and the existing method SURF are presented in Figure 4.3. The number of matched keypoints is also given to compare the methods figuratively. Table 4.2 shows the detection results of 48 images when under multiple copy-move forgery, at the image level.

	Image 1		Image 2		Image 3		Image 4	
	SURF	PROPOSED	SURF	PROPOSED	SURF	PROPOSED	SURF	PROPOSED
TPR	0.753	0.882	0.835	0.873	0.935	1.0	0.809	0.832
FPR	0.044	0.026	0.143	0.137	0.022	0.017	0.013	0.011
Matched points	86	164	106	356	32	134	40	104

Table 4.2 Detection under multiple copy-move forgery

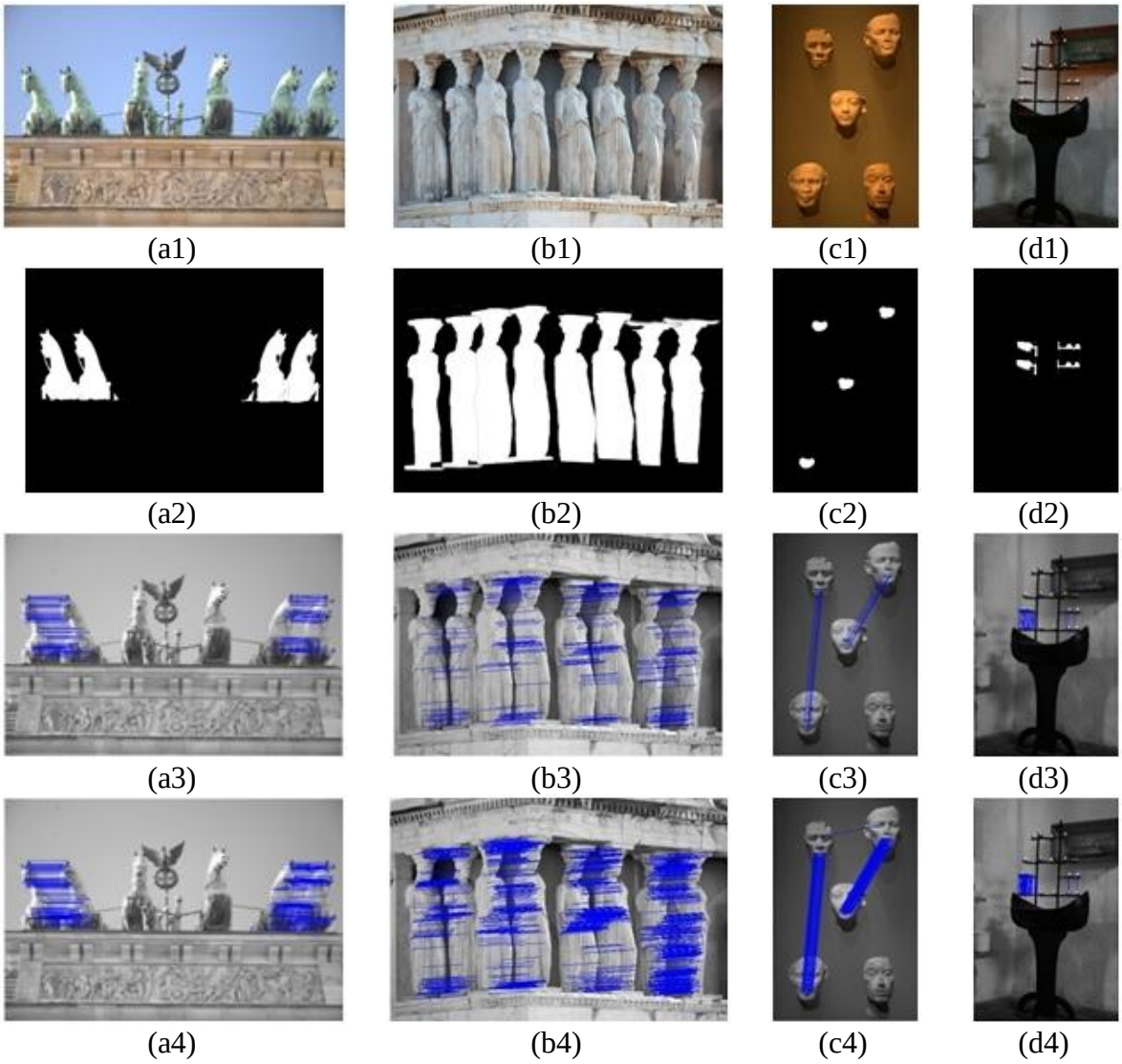


Figure 4.3: Detection under Multiple Copy-move Forgery: Four host images from the dataset (a1)~(d1); the ground truth regions of the corresponding host images (a2)~(d2); detection results of SURF (a3)~(d3); detection results of the proposed method (a4)~(d4).

- Detection under Flat and Smooth Copy-Move Forgery: The main drawbacks of existing keypoint based methods SIFT and SURF is their inability to detect keypoints in the regions with unnoticeable changes or the regions which are comparatively flat and smooth. The proposed algorithm works very well for the regions with inconspicuous changes by providing enough keypoints to perform matching. The results show that SURF is unable to detect any keypoint for some flat images whereas the proposed algorithm detected significant keypoints to mark those regions as forged. The visual results for both the SURF and proposed algorithms are shown in the Figure 4.4. SURF based forgery detection method matches 0, 2 and 4 keypoints respectively for three images as shown in the Table 4.3 whereas the proposed method matched 28, 22 and 34 keypoints respectively.

	Image1		Image 2		Image 3	
	SURF	PROPOSED	SURF	PROPOSED	SURF	PROPOSED
TPR	NA	0.546	NA	0.839	NA	1
FPR	NA	0.113	NA	0.107	NA	0.014
Matched points	0	28	2	20	4	34

Table 4.3 Detection under flat and smooth copy-move forgery

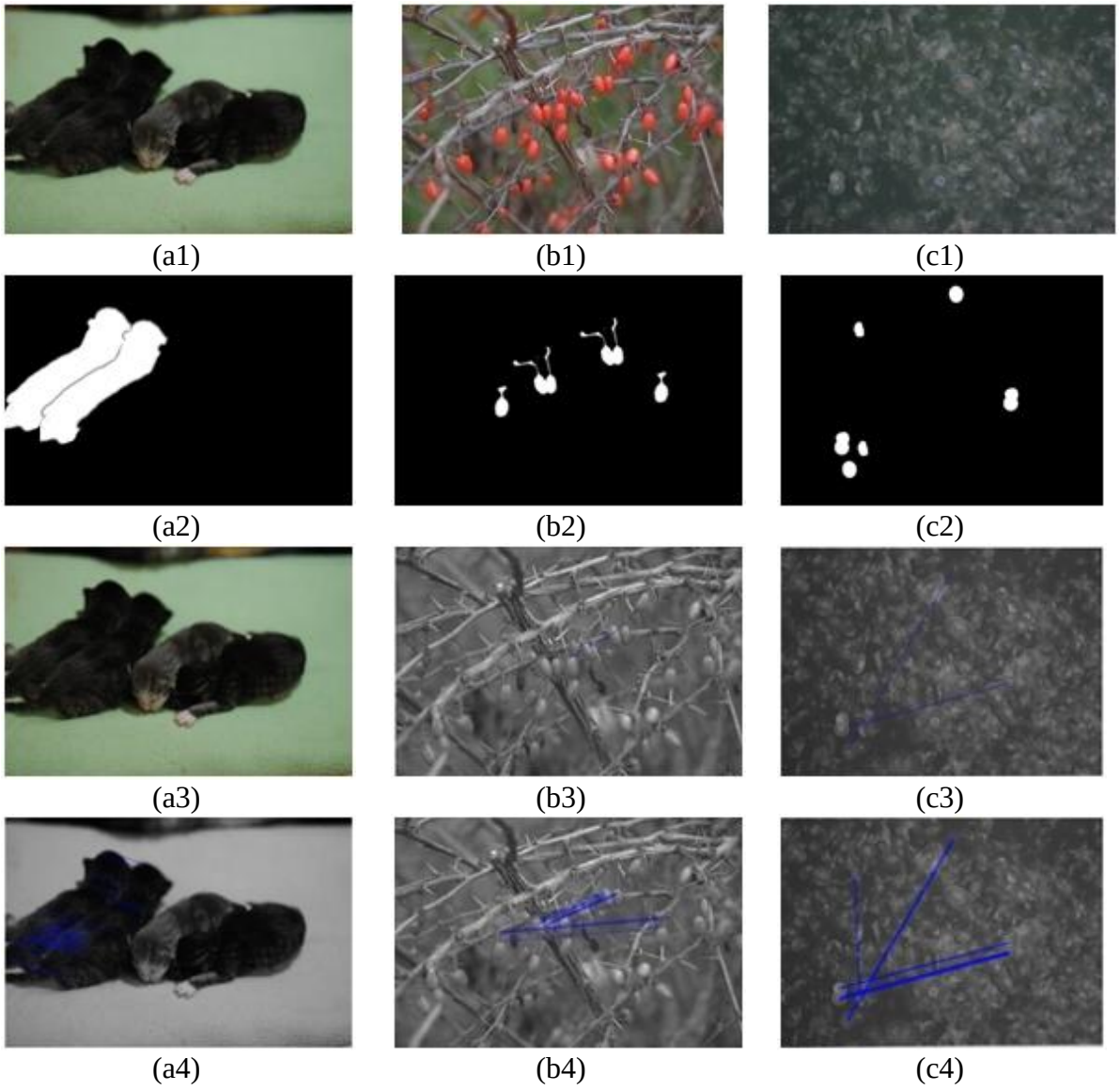


Figure 4.4: Detection under Flat and Smooth Copy-move Forgery: Three host images from the dataset (a1)~(c1); the ground truth regions of the corresponding host images (a2)~(c2); detection results of SURF (a3)~(c3); detection results of the proposed method (a4)~(c4).

- Detection under Rotated Forgeries: Here, the region to be copied is first rotated by some angle and then it is pasted somewhere else in the same image. The degree of rotation that is used to check the rotation invariance of the proposed algorithm is 20, 60 and 180 degrees. However, it is invariant to any type of rotation varying between 0-180 degrees. The results of both the existing and the proposed method in terms of rotation invariance

are comparable and are shown in Figure 4.5 and Table 4.4 but the proposed method still gives more number of matched points than standard SURF technique.

	$\theta = 20°$		$\theta = 60°$		$\theta = 180°$	
	SURF	PROPOSED	SURF	PROPOSED	SURF	PROPOSED
TPR	0.626	0.857	0.805	0.808	0.675	0.815
FPR	0.036	0.032	0.025	0.019	0.039	0.023
Matched points	22	38	20	34	36	56

Table 4.4 Detection under Rotated copy-move forgery

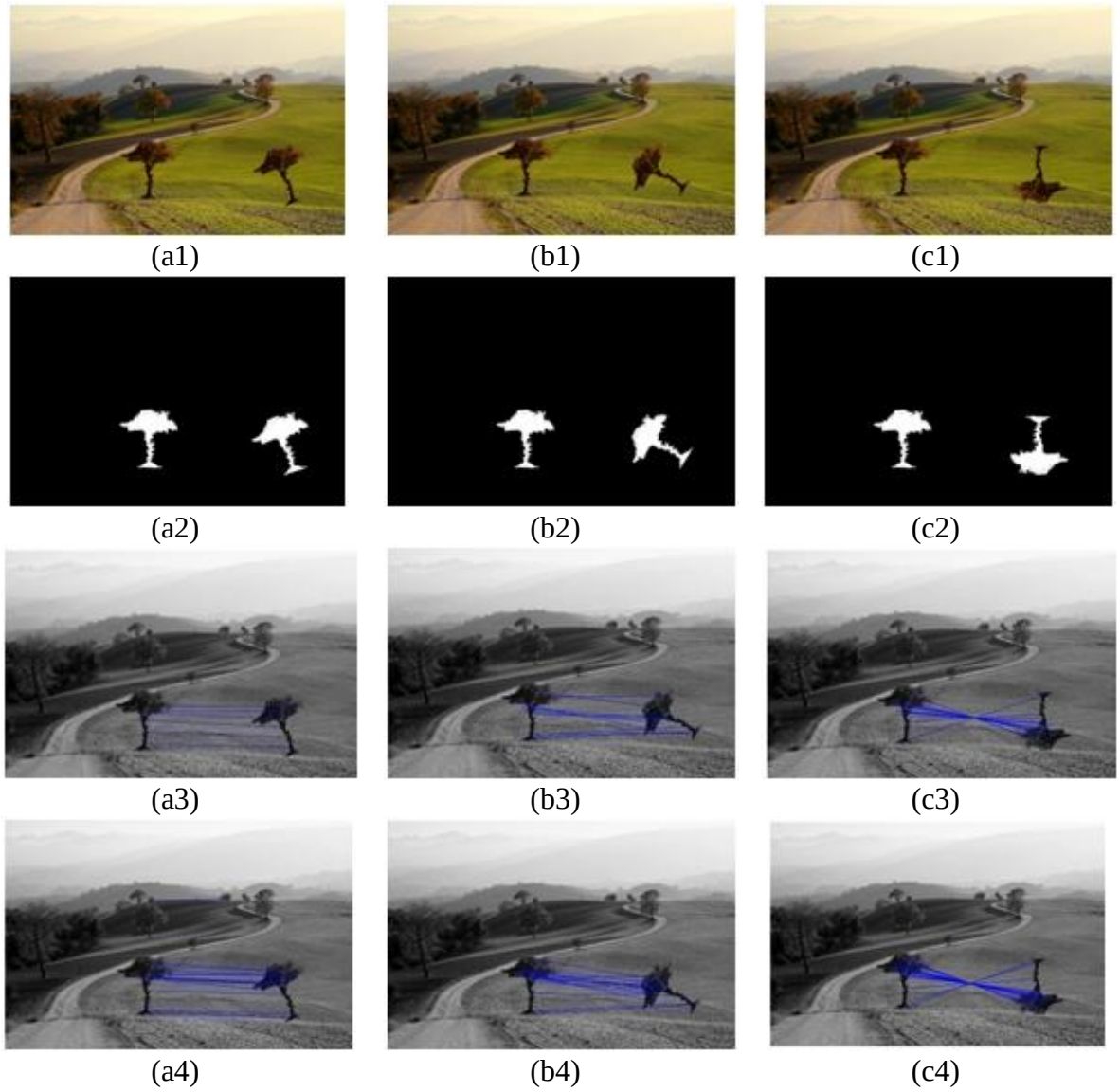


Figure 4.5: Detection under Rotated Copy-move Forgery: Three host images from the dataset (a1)~(c1); the ground truth regions of the corresponding host images (a2)~(c2); detection results of SURF (a3)~(c3); detection results of the proposed method (a4)~(c4).

	SURF[27]	PROPOSED
RECALL	89.58	93.75
PRECISION	91.49	97.87

Table 4.5 Results For Images At Image Level

In the same way, the detection result at image level are presented in Table 4.5. The results are compared with the SURF method presented in [27]. Also, the proposed method has been proved to be robust to Gaussian noise addition, JPEG compression and illumination changes. That is, any pre-processing that is applied to make forgery detection difficult,can be detected by the proposed algorithm effectively and accurately. Also, it can effectively detect forgerd areas in flat and smooth regions where other methods failed to detect any significant keypoints.

4.4 CONTRIBUTION

In this section, an effective hybrid method to detect copy move forgery has been presented. The method uses Shi-Tomasi features and SURF descriptors for detection of copied and pasted regions and also uses RANSAC algorithm for elimination of false matches. To detect multiple forgeries in the same image, a method in which RANSAC method is applied iteratively is also proposed. The proposed algorithm is able to detect significant keypoints in flat and smooth regions to reveal forgery that cannot be noticed by naked eye. Visual results also indicate that the method yields better results compared to other keypoint based existing methods SIFT and SURF even if the image has been rotated, blurred, WGN added or JPEG compressed to hide clues of forgery.

CHAPTER 5
SURF-PSO

The key-points based methods discussed previously incur one another common type of drawback i.e. the detection results of SIFT and SURF are highly dependent on the various predefined parameters values (PPV). These predefined parameters determined with experience provide good results only for a few images. Therefore, their application becomes limited when the keypoints detected in an image are too less to say that the image is forged. Also, sometimes false identification of duplicated regions happens and true forged regions are not detected at all. The technique that detects forged images by using SURF algorithm and the predefined parameters is named as SURF-PPV (SURF using Pre-defined Parameter Values). An example is shown in Figure 5.1 where the points detected are too less to prove that the image is not authentic.

(a) (b) (c)

Figure 5.1 (a) Original Image; (b) Forged Image; (c) Detection result using SURF-PPV

5.1 FORMULATION OF PROBLEMS IN PARAMETER VALUE SELECTION

Any set of predefined parameters is applicable only to a few images. But when it comes to detect large dataset of images, certain limitations occur. Therefore, we need to adjust these parameter values when predefined parameters do not provide satisfactory results or when they are not suitable for a certain image. Since, different researchers get different experiences while using these parameters, therefore there is no unified standard for forgery detection parameters. These problems arises when

1) The duplicated regions are not able to provide enough keypoints for matching criterion or the keypoints detected are mostly unstable that they get filtered out in the process.
2) Some images might contain similar regions and those regions may be erroneously detected as duplicated ones when parameter selection is not done accurately. Hence, it is possible that the native regions of an image are misclassified as forged ones.
3) The number of matched keypoints is too less to prove any image to be forged one. Because in CMF detection techniques, minimum four pairs of matched keypoints are

necessary to prove that the regions are duplicated. Hence, forgery cannot be detected with very few or when no keypoint is detected.

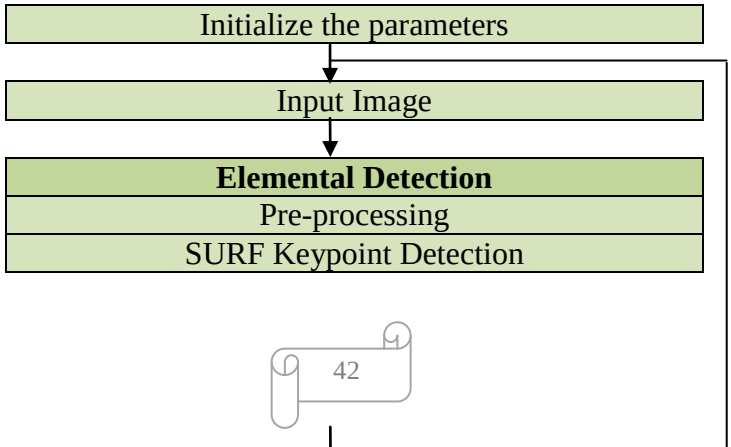
5.2 PROPOSED ALGORITHM (SURF-PSO)

To address this issue of predefined parameter values, a new algorithm is proposed which integrates Particle Swarm Optimization (PSO) with copy-move forgery detection technique in particular SURF algorithm to detect copy-move forgery in more efficient and effective manner. The proposed technique is named as SURF-PSO, which identifies optimized and customized parameters automatically for each image separately. The forged images that are generally missed by SURF-PPV can be easily and effectively detected by SURF-PSO. Hence, SURF-PSO generates more optimized and better results than SURF-PPV.

The proposed algorithm, SURF-PSO, is utilized to optimize the parameter values automatically for each test image. The algorithm of SURF-PSO is depicted in Figure 5.2. It consists of two main steps: One is Elemental detection, which is basically SURF-based framework that is used to detect forgery in images and the other one is Parameters Estimation, which is used to provide satisfactory values of these parameters for each image separately. For estimation of these parameters, Particle Swarm Optimization (PSO) [44, 46] is employed. Initially, the predefined parameter values are given as an input to this algorithm to detect copy-move forged images then the following operations are run N times:

- Elemental Detection detects the forgery in images with the parameter values applied and then the detection result i.e. the no. of matched keypoints is delivered to the next round. The evaluation criterion is built based upon the detection result of 1st round.
- Parameters Estimation estimates the new set of parameter values according to the results obtained by the 1st step. Then the new set of parameters is delivered to step 1 to start the next round. Hence, the process goes on like this.

After completing N rounds of execution, the parameters that give best detection result are chosen for each image. Here, the value of N is decided to be 100.



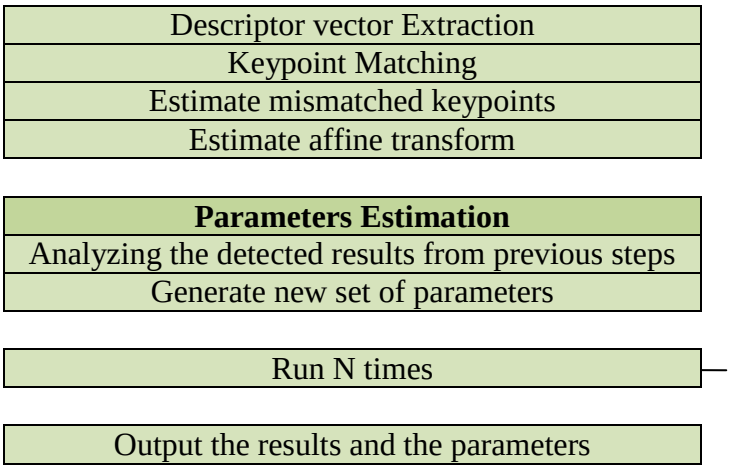


Figure 5.2 Flow diagram of SURF-PSO

5.2.1 The Elemental Detection

After initializing the input parameters for a particular test image, the following five steps of Elemental Detection are preformed.

- Pre-Processing: In this step, the RGB colored image is simply converted to gray scale image.
- Keypoint Detection and Feature Extraction involve detecting points of interest from an image by utilizing the concept of integral images. After detecting keypoints, the feature description method based on Haar wavelet filters is applied to represent each interest point in the form of 64-D feature vector as described in the section 3.2. SURF uses 64-D feature vector instead of 128-D feature vector of SIFT, which makes it computationally much faster than SIFT.
- Keypoint Matching: In matching, a method is suggested that computes the ratio of first and second nearest neighbors of every keypoint and then it is compared with a threshold T (often fixed to 0.6). For every keypoint, a similarity vector $D = \{d_1, d_2, \dots d_3\}$ is defined in which the distance with respect to other keypoints is listed in sorted manner i.e. in ascending order. The condition for keypoints to be matched is listed in Eq. 5.1:

$$\frac{d_1}{d_2} < T \text{ where } T \in (0,1) \tag{5.1}$$

  In this, d_1 and d_2 are first and second elements of the sorted matrix for every keypoint. This procedure is popularly known as 2NN test. Finally, a set of matched points is obtained.
- Estimating Mismatched Keypoints and Affine Transform: Furthermore, the matched points that are lying very close to each other need to be eliminated because they represent the areas that are similar but not copied. This elimination is done by computing the

Euclidean distance between coordinates of matched descriptors. Only those matches are retained for which the computed distance is greater than some particular threshold value denoted by D_{min} and are saved for further processing.

The other mismatched keypoints are removed by estimating the geometric transformations between pair of matched keypoints. The geometric relationship described by H which is a 3×3 matrix, between two points (a,b) and (a',b') is computed as shown in Eq. 5.2:

$$\begin{bmatrix} a' \\ b' \\ 1 \end{bmatrix} = \mathrm{H} \begin{bmatrix} a \\ b \\ 1 \end{bmatrix} \tag{5.2}$$

At least three matched points are needed to compute this matrix. However, the estimated homography can be severely disturbed by the mismatched points (outliers). For this reason, Random Sample Consensus algorithm (RANSAC) [45] is presented to perform the previous estimation. In this, a set (usually three pairs) from the matched points is selected to estimate the homography H, then all the remaining points are transformed according to H and comparison is done with respect to their corresponding matched points in terms of distance. Inliers (TMPs) or outliers (MMPs) are catalogued according to this distance, if it is below or above a certain predefined threshold β respectively. Number of iterations N_{iter} is listed and then the estimated transformation which gives higher number of inliers is chosen. Here, N_{iter} has been set to 1000 and the threshold β to 0.05.

5.2.2 The Parameters Estimation

For parameters estimation, Particle swarm optimization (PSO) is applied, which is used for solving minimization and maximization problems. Before applying PSO, two things are needed to be considered.

- Which parameters are needed to be optimized?
- Formulation of the evaluation function to select the optimized parameters.

1. Parameters for Optimization

   Different values of different parameters make a large impact on detection results. The parameters that are needed to be optimized and their decision boundaries are listed in Table 5.1.

   The parameter values that are used in implementation of SURF are different in different literatures:

O, S, Thresh: These parameters play a useful role in Keypoint Detection stage. *O* specifies no. of octaves, *S* specifies no. of scales per octave and *Thresh* is used to reject unstable keypoints. OpenCV [47] implementation of SURF uses *O*=4, *S*=2 and *Thresh*= 0.05. MATLAB [48] implementation of SURF chose *O*=3, *S*=4 and *Thresh*=0.1000. According to these, the domains of these parameters are chosen as: $O \in [1, 4]$, $S \in [2, 6]$, $Thresh \in [0.0001, 0.1000]$ in this section.

τ: This parameter is utilized in keypoint matching. τ=0.5 is used by Pan et al. [35], IreneAmereni [34] chose τ= 0.6 and Andrea Costanzo [49] set τ=0.8. Hence, the domain is set as $\tau \in [0.5, 0.8]$ in this section.

Dis_{min}: This parameter is used in removing mismatched keypoints in filtering stage. Christlein [16] set the value of this parameter as Dis_{min}=50. Hence, its domain is set as $Dis_{min} \in [10, 60]$ in this section.

Parameters	Definition	Lower Bound	Upper Bound
O	No. of Octaves	1	4
S	No. of Scale Levels per Octave	2	6
Thresh	Threshold for rejecting unstable keypoints	0.0001	0.1000
τ	Threshold for keypoint matching	0.5	0.8
Dis_{min}	The minimum distance	10	60

Table 5.1 Optimization Parameters (Parameters in SURF based algorithm)

2. Evaluation Function

Although different literatures use different metrics to evaluate the performance of detection techniques, the key idea is similar. The more the number of truly matched points (TMPs) and the less the number of mismatched points (MMPs), the more effective is the detection result. Therefore, while building the evaluation function, these factors are considered to be most important.

When the number of truly matched keypoints (TMPs) is large, the duplicated regions are not only estimated accurately but also the detection results become more convincing. Hence, the evaluation function used is represented as shown in Eq. 5.3:

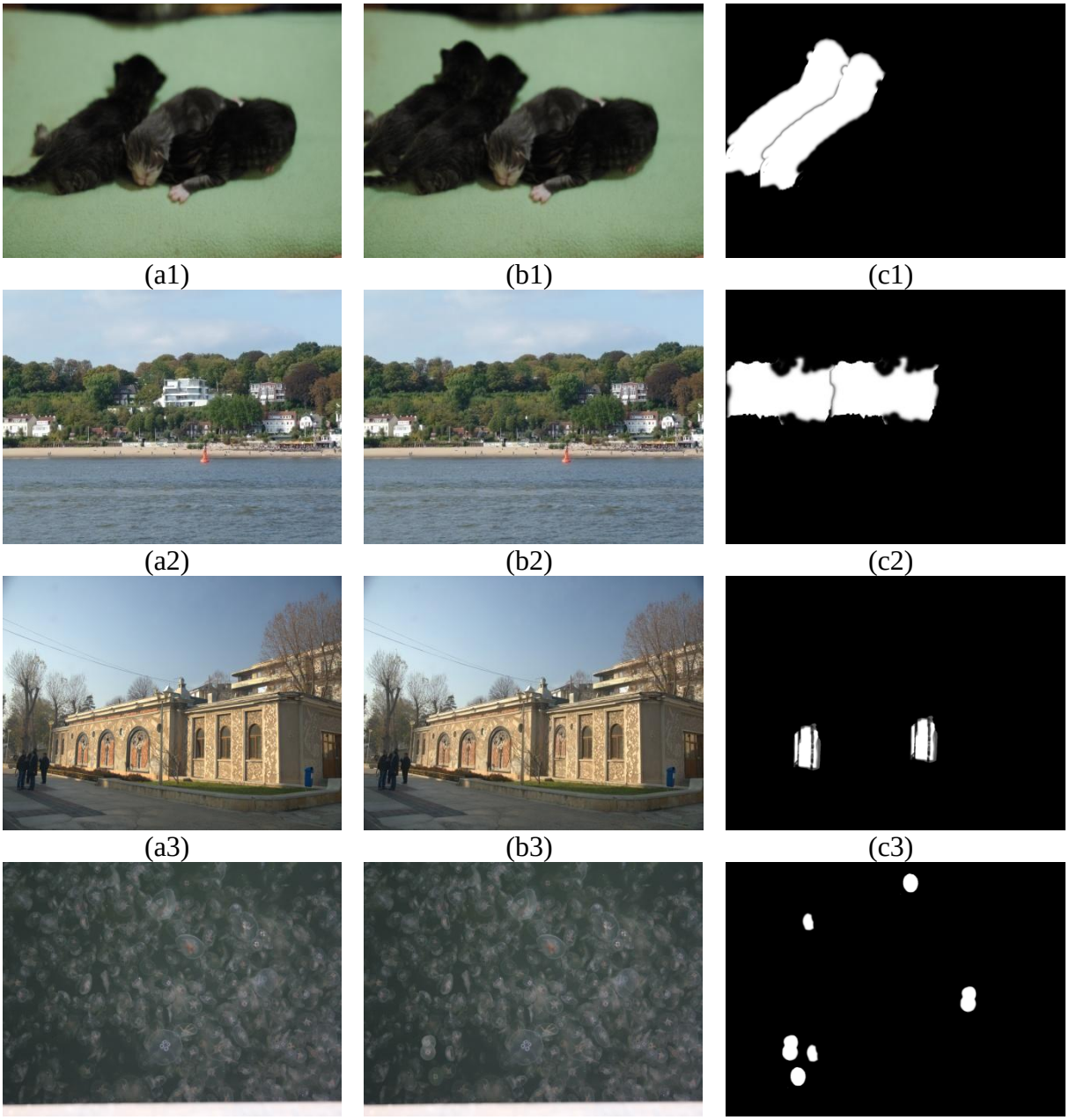
$$P_m = \frac{TMPt}{(TMPt + \delta)}, \qquad \delta = \begin{cases} MMPt, & MMPt > 10 \\ 10, & MMPt \leq 10 \end{cases} \tag{5.3}$$

Where TMPt and MMPt are truly matched and mismatched keypoints respectively. TMPt are the true matched keypoints that satisfy the affine transform described in section 4.1. The other pairs that do not satisfy this transformation are regarded as mismatched keypoints MMPt. δ is a mismatch coefficient and it provides a value i.e. a default minimum value to MMPt in order to reflect real matching. P_m is the probability of

matching. The parameters yielding highest value of P_m are chosen. Hence, the criterion for evaluation of SURF-PSO is P_m.

5.3 RESULTS AND DISCUSSION

The SURF-PSO is implemented in Matlab 2015a and the results are compared with standard SURF-PPV. Christlein et al. [16] database is utilized here to check the performance of SURF PSO. This database consists of 48 forged images with average size of images equal to 3000*2300 pixels. Five examples that are used in this experiment are shown in Figure 5.3.



(a1) (b1) (c1)

(a2) (b2) (c2)

(a3) (b3) (c3)

(a4) (b4) (c4)

(a5) (b5) (c5)

Figure 5.3 Examples utilized for Performance Evaluation (a1)-(a5) Original Images; (b1)-(b5) Forged Images; (c1)-(c5) Ground truth Images

Some settings for PSO algorithm that are made at Parameters Estimation step are as follows: The maximum numbers of iterations is 80 and the size of population is 20. The inertia range is set to 1.1. The self and social adjustment weights are set to 1.49. The fitness function of PSO is given as

$$P_f = \frac{1}{P_m} \tag{5.4}$$

The main difference between SURF-PPV and SURF-PSO lie among the parameters values only. Choosing different parameters yield different results. Hence, parameter selection is the main criterion for improving the detection of copy-move forged images. Therefore, the results of both the methods are compared on the basis of TMPs and the precision between them which is calculated as:

$$Precision = \frac{TMPs}{(TMPs + MMPs)} \tag{5.5}$$

Where TMPs are truly matched keypoints and MMPs are the mismatched keypoints as determined by RANSAC in the filtering section.

The visual results of five images are shown in Figure 5.4. The detection results of these images typically demonstrate the futility of detection of copy move forgery using SURF-PPV.

In Figure 5.4 (b1), it is clearly shown that the SURF-PPV is not able to reveal the duplicated regions at all, while SURF-PSO can reveal the same accurately and effectively.

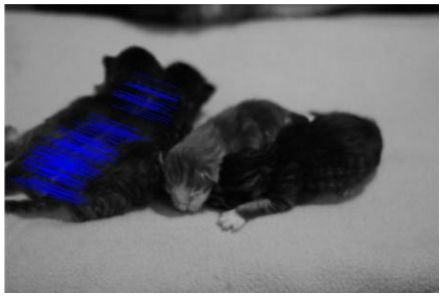
Figure 5.4(b2) shows that the matched points detected by SURF-PPV are too less to accurately mark the forged regions. Using particle swarm optimization (PSO), the number of truly matched keypoints increases significantly and hence the detection results are improved.

In Figure 5.4(b3), although SURF-PPV can detect some true forged areas, but it also detects enough false matched key-points to misinterpret the authentic regions as forged ones.

SURF-PSO is also applied to detect multiple copy-move forgery as shown in Figure 5.4(a4). The results show that the SURF-PPV method is not able to detect enough matched points to

mark the regions as forged ones. Hence, with only 10 matched points detected in different regions of multiple forgeries, one cannot infer that those regions are not authentic. Therefore, we can say that no forgery is detected in this case. However, SURF-PSO detects enough matched points in each region separately and hence provides efficient detection results.

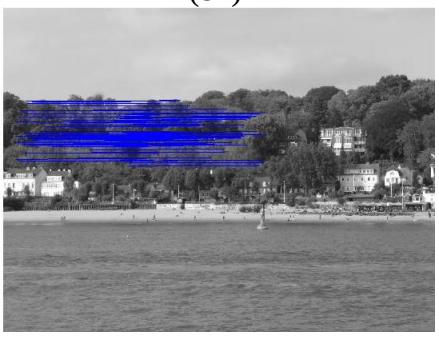
Similarly, in Figure 5.4(b5), it is shown that no forgery is detected in case of SURF-PPV whereas the results obtained by SURF-PSO are correct and accurate because it improves the detection by increasing the flexibility in choosing parameter values.



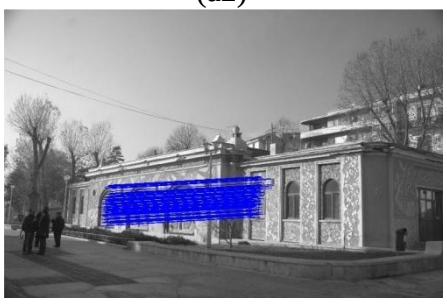
(a1)

(b1)

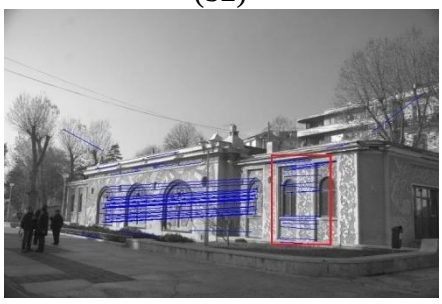
(a2)



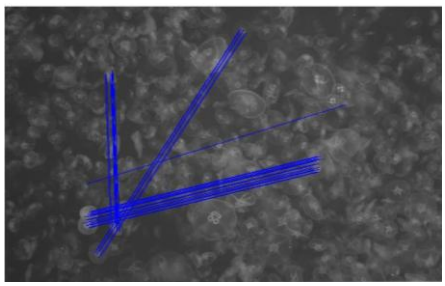
(b2)



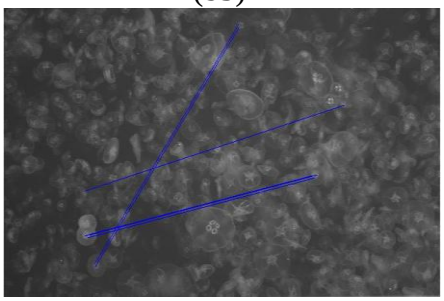
(a3)



(b3)



(a4)

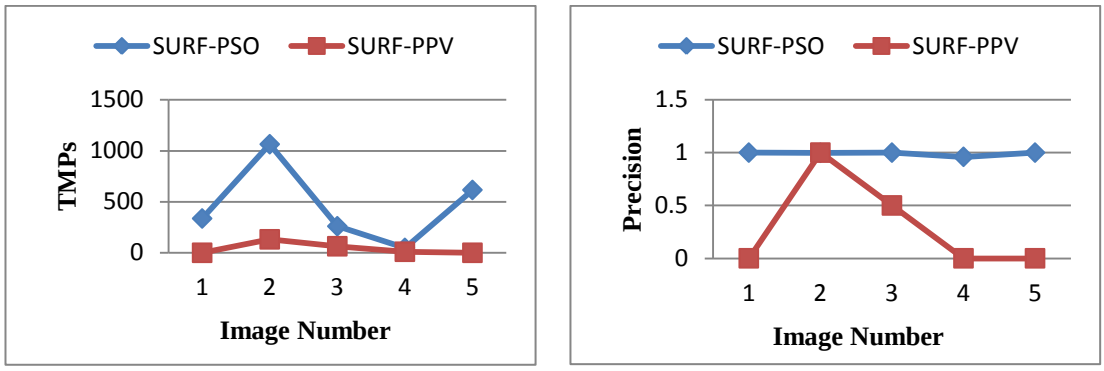


(b4)

(a5) (b5)

Figure 5.4 Comparison between detection results of SURF-PSO (a1-a5) and SURF-PPV (b1-b5)

The comparison results of five images based on truly matched keypoints (TMPs) and precision between SURF-PSO and SURF-PPV are shown in Figure 5.5. Also, the mathematical results of these five images are listed in Table 5.2 which indicates the name and size of different images used, TMPs, MMPs and the precision of SURF-PPV, SURF-PSO and CMFD-PSO [41].



(a) (b)

Figure 5.5 Comparison between TMPs detected by SURF-PSO and SURF-PPV (a); Comparison of Precision between SURF-PSO and SURF-PPV (b)

Based on the results, it can be said that the detection results of SURF-PSO are better than SURF-PPV. Using PSO algorithm, SURF-PSO can choose different suitable and optimized parameters for each image separately. Hence, SURF-PSO not only detects more images than SURF-PPV, but also increases the number of truly matched keypoints and hence improves the precision.

Image (Size)	PPV (O,S,Thresh,ϒ, Dis_{min})	SURF-PPV			SURF-PSO			CMFD-PSO [41]		
		TMPs	MMPs	Prec.	TMPs	MMPs	Prec.	TMPs	MMPs	Prec.
four_babies (1024×681)	4,6,0.005,0.57,50	0	0	0	336	0	1	1500	3	0.998
beach_wood (1024×768)	4,5,0.012,0.59,55	132	0	1	1064	2	0.998	5112	2	0.999
window (1024×768)	4,6,0.020,0.62,40	64	64	0.5	260	0	1	190	0	1
Jellyfish (1296×1944)	4,5,0.045,0.60,50	10	2	0	48	2	0.96	-	-	-
hedge (1224×1632)	4,6,0.015,0.56,60	0	8	0	616	0	1	-	-	-

Table 5.2 Comparison among SURF-PPV, SURF-PSO and CMFD-PSO

The results are also compared with CMFD-PSO technique presented in [41] where the multiple copy-move forgery is not taken into account. The CMFD technique that is utilized in CMFD-PSO for Elemental Detection is SIFT. Also, the matched keypoints detected in that case are more which clearly means that the computational complexity is more due to increased length of descriptor vector. But the method proposed in this section is computationally less complex and also deals with multiple copy-move forgery.

5.4 CONTRIBUTION

The use of SURF-PSO has been presented in this section. Experimental results shows that the SURF-PSO can automatically generate optimized parameters for each image separately and the results obtained by SURF-PSO are more accurate than SURF-PPV. Five images are utilized to conduct the experiment in which SURF-PSO detected 1064 matched key-points for one image whereas SURF-PPV detected only 132. Also, the precision rate of SURF-PSO is 1 for most images unlike SURF-PPV, where precision is almost 0. Hence, the concept of integrating PSO with SURF to improve the detection results of copy move forgery has been effectively presented.

CHAPTER 6
CONCLUSION AND FUTURE SCOPE

6.1 CONCLUSION

This thesis examines the analysis of Copy-move Forgery Detection Techniques to detect forgeries in digital images. The concept of forgery detection is based on extracting interest points and their descriptor vectors from the test images and using them to reveal the forged areas by using matching criterion. The advantages that an efficient forgery algorithm must possess are low computational complexity, high detection accuracy, less false positives and high robustness to various post-processing operations such as rotation, scaling, JPEG compression, blurring, Gaussian noise addition etc.

This thesis work has proposed a novel approach for detecting copy-move forgery in digital images based on Shi-Tomasi detector and SURF descriptor. The standard SURF technique that is computationally less complex and robust to different post-processing operations possess one common drawback i.e. it is unable to detect reliable keypoints when copied regions are too small or when the image contains forgery in flat and smooth regions of the image. This is because the key-points detected by SURF descriptor are scattered unevenly throughout the image. Therefore, the SURF detector in standard SURF algorithm is simply replaced by Shi-Tomasi detector. The Shi-Tomasi detector detects enough key-points in these regions for matching process to happen. Each interest point is then given a unique identity by using a region description method based on SURF descriptor. After that, matching of these vectors is performed to reveal duplicated regions. An algorithm to detect multiple forgeries in same image has also been proposed. The proposed algorithm has improved the precision and recall from 91.49% and 89.59% to 97.87% and 93.75% respectively as compared to conventional SURF based detection.

Also, their exists another drawback of key-point based methods like SURF i.e. their detection accuracy highly depends upon number of pre-defined parameters which are usually determined with human experience. The pre-defined parameters do not perform well equally for all images. They are applicable to a few images only. Therefore, this limits the application of detection process. To deal with this, an algorithm integrating SURF detection scheme with Particle Swarm Optimization has been proposed to generate optimized parameters for each image separately and independently. In this thesis, the proposed SURF-PSO is applied on five images separately and the results prove that SURF-PSO performs much better than the conventional SURF technique. The precision of the SURF-PSO is 1 for three images while it

is 0 or 0.5 for conventional SURF and for a particular image, SURF-PSO detected 1064 matched points while conventional SURF detected only 132.

6.2 FUTURE SCOPE OF WORK

The detection of copy-move forgery in digital images is a topic without boundaries. Further, studies can be extended in the areas like:

- Generally, existing strategies are less effective in homogenous and smooth regions because they also have to maintain robustness to various post-processing operations (e.g. rotation, noise addition, scaling, lossy compression, and blurring). Keeping in mind the end goal to cover such regions, computational time and complexity will increase and result in slower handling time and require a high computational cost. Also, the threshold values to determine the manipulated region are changed for each image size and content; consequently, influencing the accuracy of the strategy even when a training has been done. Therefore, work should be expanded further for detection of homogeneous and smooth areas.
- Studying salient feature selection and enhancing the matching or coordinating techniques for decreasing the complexity while keeping up the accuracy is another subject of interest in Copy-move forgery detection field.
- Big data is likewise another famous research patterns, and the implications of big data is the failure to handle and analyze large datasets. There remains a requirement for further research with an intention on real world applicability of a strategy or techniques to address the digital forensic data volume challenge. This is not surprising because of the significant increase in data shared on the web (e.g. transferring and sharing of pictures via web-based networking media destinations, for example, Facebook, Instagram, Flickr and Whatsapp), which exceeds the processing and analytical capabilities of current devices. In this manner, confirming the genuineness of such pictures remains an operational challenge.

REFERENCES

[1] Kumar S and Das PK (2011). Copy-move forgery detection in digital images: progress and challenge, *International Journal on Computer Science and Engineering*, 3(2), 652-663.

[2] Wu L *et al*. (2013). Image tampering localization via estimating the non-aligned double JPEG compression, *Proceedings of IS&T/SPIE Electronic Imaging*, 86650R1–86650R7.

[3] Al-Hammadi MHA. Copy Move Forgery Detection In Digital Images Based On Multiresolution Techniques. Ph.D Thesis, King Saud University, 2013.

[4] Krawetz N and Solutions HF (2007). A pictures worth digital image analysis and forensics, *Black Hat Briefings*, 1-31.

[5] Li Y (2013). Image copy-move forgery detection based on polar cosine transform and approximate nearest neighbor searching, *Forensic science international*, 224(1), 59-67.

[6] Cao G *et al.* (2014). Contrast enhancement-based forensics in digital image, *IEEE transactions on information forensics and security*, 9(3), 515-525.

[7] Caoduro E (2014). Photo filter apps: Understanding analogue nostalgia in the new media ecology, *Networking Knowledge: Journal of the MeCCSA Postgraduate Network*, 7(2).

[8] Hsu YF *et al.* (2007). Image splicing detection using camera response function consistency and automatic segmentation, *2007 IEEE International Conference on Multimedia and Expo*. 2007, pp. 28-31

[9] Qureshi MA *et al*. (2014). A review on copy move image forgery detection techniques, *IEEE International Multi-Conference* in *Systems, Signals & Devices (SSD)* [11th: Barcelona, Spain: 2014], pp. 1-5.

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

[11] Elwin JGR *et al.* (2010). Survey on passive methods of image tampering detection, *IEEE international conference on Communication and computational intelligence (INCOCCI)* [Erode, India: 2010], pp. 431-436.

[12] Celik MU *et al.* (2006). Lossless watermarking for image authentication: a new framework and an implementation, *IEEE Transactions on Image Processing*, 15(4), 1042-1049.

[13] Stamm MC and Liu KR (2010). Forensic detection of image manipulation using statistical intrinsic fingerprints, *IEEE Transactions on Information Forensics and Security*, 5(3), 492-506.

[14] Kaur H and Kaur K (2015). A Brief Survey of Different Techniques for Detecting Copy-Move Forgery, *International Journal of Advanced Research in Computer Science and Software Engineering*, 5(4), 875-882.

[15] Mahmood T *et al.* (2015). A survey on block based copy move image forgery detection techniques, *IEEE International Conference on Emerging Technologies (ICET)* [Peshawar, Pakistan: 2015], pp. 1-6.

[16] Christlein V *et al*. (2012). An evaluation of popular copy-move forgery detection approaches, *IEEE Transactions on information forensics and security*, 7(6), 1841-1854.

[17] Warif NBA *et al.* (2016). Copy-move forgery detection: Survey, challenges and future directions, *Journal of Network and Computer Applications*, 75, 259-278.

[18] Saha S, Bhattacharyya D, and Bandyopadhyay SK (2010). Security on fragile and semifragile watermarks authentication, *Int. J. Comput. Applicat*, 3(4), 23-27.

[19] Fridrich AJ, Soukal BD, and Lukáš AJ. Detection of copy-move forgery in digital images. *in Proceedings of Digital Forensic Research Workshop*. 2003.

[20] Huang Y *et al.* (2011). Improved DCT-based detection of copy-move forgery in images, *Forensic science international*, 206(1), 178-184.

[21] Zhao J and 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.

[22] Popescu A and Farid H. Exposing digital forgeries by detecting duplicated image region Technical Report: Hanover, Department of Computer Science, Dartmouth College, USA, 2004, pp. 32.

[23] AlSawadi M *et al.* (2013). Copy-Move Image Forgery Detection Using Local Binary Pattern and Neighborhood Clustering, *IEEE European in Modelling Symposium (EMS)* [Manchester, UK: 2013], pp. 249-254.

[24] Davarzani R *et al.* (2013). Copy-move forgery detection using multiresolution local binary patterns, *Forensic science international*, 231(1), 61-72.

[25] Bayram S, Sencar HT and Memon N (2009). An efficient and robust method for detecting copy-move forgery, *IEEE International Conference on Acoustics, Speech and Signal Processing, ICASSP* [Taipei, Taiwan: 2009], pp. 1053-1056.

[26] Grgic S, Grgic M and Zovko-Cihlar B (2001). Performance analysis of image compression using wavelets, *IEEE Transactions on industrial electronics*, 48(3), 682-695.

[27] Muhammad G, Hussain M and Bebis G (2012). Passive copy move image forgery detection using undecimated dyadic wavelet transform, *Digital Investigation*, 9(1), 49-57.

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

[29] Hussain M *et al.* (2012). Copy-move image forgery detection using multi-resolution Weber descriptors, *IEEE International Conference on Signal Image Technology and Internet Based Systems (SITIS)* [8th: Naples, Italy: 2012], pp. 395-401.

[30] Quan X and Zhang H (2012). Copy-move forgery detection in digital images based on local dimension estimation. in Cyber Security, *International Conference on Cyber Warfare and Digital Forensic (CyberSec)*[Kuala Lumpur, Malaysia: 2012], pp. 180-185.

[31] Muhammad G *et al.* (2013). Multi-scale local texture descriptor for image forgery detection, *IEEE International Conference on Industrial Technology (ICIT)* [Cape Town, South Africa: 2013], pp. 1146-1151.

[32] Lowe DG (2004). Distinctive image features from scale-invariant keypoints, *International journal of computer vision*, 60(2), 91-110.

[33] Bay H *et al.* (2008). Speeded-up robust features (SURF), *Computer vision and image understanding*, 110(3), 346-359.

[34] Amerini I *et al.* (2010). Geometric tampering estimation by means of a SIFT-based forensic analysis, *IEEE International Conference on Acoustics Speech and Signal Processing (ICASSP)*, [Dallas, TX, USA: 2010], pp. 1702-1705.

[35] Pan X and Lyu S (2010). Region duplication detection using image feature matching, *IEEE Transactions on Information Forensics and Security*, 5(4), 857-867.

[36] Pun CM, Yuan XC and Bi XL (2015). Image forgery detection using adaptive oversegmentation and feature point matching, *IEEE Transactions on Information Forensics and Security*, 10(8), 1705-1716.

[37] Chen L *et al.* (2013). Region duplication detection based on Harris corner points and step sector statistics, *Journal of Visual Communication and Image Representation*, 24(3), 244-254.

[38] Harris C and Stephens M. A (1988). Combined corner and edge detector, in *Alvey vision conference*, [4th: Manchester,UK: 1988].

[39] Mishra P *et al.* (2013). Region duplication forgery detection technique based on SURF and HAC, *The Scientific World Journal*.

[40] Amerini I *et al.* (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.

[41] Wenchang S *et al.* (2016). Improving image copy-move forgery detection with particle swarm optimization techniques, *China Communications*, 13(1), 139-149.

[42] Shi J (1994). Good features to track, *IEEE Computer Society Conference on Computer Vision and Pattern Recognition,Proceedings CVPR'94* [Seattle, WA, USA: 1994], pp. 593-600.

[43] Kennedy J. *Particle swarm optimization*, in *Encyclopedia of machine learning*, 2011, pp. 760-766.

[44] Eberhart R and Kennedy J (1995). A new optimizer using particle swarm theory, *Proceedings of the International Symposium on Micro Machine and Human Science, MHS'95.* [6th: Nagoya, Japan: 1995], pp. 39-43.

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

[46] Kennedy J and Eberhart R (1995). Particle swarm optimization, *IEEE International of Conference on Neural Networks* [1st: Perth, Australia: 1995].

[47] Bradski G and Kaehler A. *Learning OpenCV: Computer vision with the OpenCV library*." O'Reilly Media, Inc.", 2008.

[48] Documentation M. *The MathWorks Inc*, 2005.

[49] Costanzo A *et al.* (2014). Forensic analysis of SIFT keypoint removal and injection, *IEEE Transactions on Information Forensics and Security*, 9(9), 1450-1464.

LIST OF PUBLICATIONS

[1] Gupta A and Kansal A. Performance Enhancement of SURF-based Copy-move Forgery Detection by using Particle Swarm Optimization (PSO), *Signal, Image and Video Processing.* (Communicated).

[2] Gupta A and Kansal A. A novel approach for improving Copy-move Forgery detection by combining Shi-Tomasi detector and SURF descriptor, *Turkish Journal of Electrical Engineering and Computer Sciences.* (Communicated).