M. Tech (Signal Processing & Digital Design) PRINCE SAPRA 2020

STUDY AND IMPLEMENTATION OF COPY-MOVE FORGERY DETECTION METHODS IN IMAGE PROCESSING

A DISSERTATION

SUBMITTED IN PARTIAL FULFILLMENT OF THE REQUIREMENTS
FOR THE AWARD OF THE DEGREE
OF

MASTER OF TECHNOLOGY
IN
SIGNAL PROCESSING AND DIGITAL DESIGN

Submitted by:

PRINCE SAPRA
2K18/SPD/07

Under the supervision of

Mr. Piyush Tewari
Assistant Professor, DTU

DEPARTMENT OF ELECTRONICS AND COMMUNICATION ENGINEERING
DELHI TECHNOLOGICAL UNIVERSITY
(Formerly Delhi College of Engineering)
Bawana Road, Delhi-110042

OCTOBER, 2020

STUDY AND IMPLEMENTATION OF COPY-MOVE FORGERY DETECTION METHODS IN IMAGE PROCESSING

A PROJECT REPORT

SUBMITTED IN PARTIAL FULFILLMENT OF THE REQUIREMENTS
FOR THE AWARD OF THE DEGREE
OF

MASTER OF TECHNOLOGY
IN
SIGNAL PROCESSING AND DIGITAL DESIGN

Submitted by

PRINCE SAPRA
2K18/SPD/07

Under the supervision of

Mr. Piyush Tewari
Assistant Professor, DTU

DEPARTMENT OF ELECTRONICS AND COMMUNICATION ENGINEERING
DELHI TECHNOLOGICAL UNIVERSITY
(Formerly Delhi College of Engineering)
Bawana Road, Delhi-110042

DEPARTMENT OF ELECTRONICS AND COMMUNICATION ENGINEERING

DELHI TECHNOLOGICAL UNIVERSITY

(Formerly Delhi College of Engineering)
Bawana Road, Delhi-110042

CANDIDATE'S DECLARATION

I **Prince Sapra (Roll No. 2K18/SPD/07),** student of M.Tech (Signal Processing and Digital Design), hereby declare that the Project Dissertation titled **"STUDY AND IMPLEMENTATION OF COPY-MOVE FORGERY DETECTION METHODS IN IMAGE PROCESSING"** which is submitted by me to the Department of Electronics and Communication Engineering, Delhi Technological University, Delhi in partial fulfillment of the requirement for the award of the degree of Master of Technology, is original and not copied from any source without proper citation. This work has not previously formed the basis for the award of any Degree, Diploma Associateship, Fellowship or other similar title or recognition.

Place: Delhi **(PRINCE SAPRA)**

Date: 29th October, 2020

DEPARTMENT OF ELECTRONICS AND COMMUNICATION ENGINEERING

DELHI TECHNOLOGICAL UNIVERSITY

(Formerly Delhi College of Engineering)
Bawana Road, Delhi-110042

CERTIFICATE

I hereby certify that the Project Dissertation titled **“STUDY AND IMPLEMENTATION OF COPY-MOVE FORGERY DETECTION METHODS IN IMAGE PROCESSING”** which is submitted by **Mr. Prince Sapra (Roll No. 2K18/SPD/07),** Departmentof Electronics and Communication, Delhi Technological University, Delhi in partial fulfillment of the requirement for the award of the degree of Master of Technology, is a record of the project work carried out by the student under my supervision.To the best of my knowledge, this work has not been submitted in part or full for any Degree or Diploma to this University or elsewhere.

Place: Delhi

Date: 29th October,2020

(Mr. Piyush Tewari)
SUPERVISOR
Professor, ECE Department
Delhi Technological University

ACKNOWLEDGEMENT

I would like to express my gratitude towards all the people who have contributed their precious time and effort to help me without whom it would not have been possible for me to understand and complete the project.

I would like to thank Assistant Prof. Piyush Tewari, Department of Electronics and Communication Engineering, my Project guide, support, motivation and encouragement throughout the period this work was carried out. His readiness for consultation at all times, his educative comments, his concern and assistance even with practical things have been invaluable.

(PRINCE SAPRA)

ABSTRACT

This research work is based on copy-move forgery detection. The copy-move forgery detection technique has various phases which include pre-processing, feature extraction and marking of forgery part on the image. In the previous methodology PCA algorithm was used for the feature reduction in the copy-move forgery detection. The parameters which are taken as input by the PCA algorithm for the feature reduction were defined statically. In this research work, to improve performance of the copy-move forgery detection model, PCA parameters needs to define dynamically.

The GLCM algorithm is used for the feature extraction in this research work. The GLCM algorithm extract 13 textural features and mean of all features will be given as input to the PCA algorithm. The initial parameters of PCA algorithm will be defined dynamically for the copy-move forgery detection. At last Euclidean distance is calculated between the block pixel to define forgery portion in the image. The performance of the proposed algorithm is tested in terms of precision, recall and F-measure. It is found that proposed algorithm performs better as compared to existing method in terms of all three parameters.

CONTENTS

LIST OF FIGURES

Chapter 1

Introduction

1.1 Introduction to Image Processing

The cameras deployed at different locations regularly capture a huge number of images. These images are of no use if they cannot provide useful information. These days, the use of image processing technology has become quite common for the extraction of valuable information from the captured images. With time, numerous approchrshave been designed for the extraction of extremely complicated data from the images. The technological advancement has contributed a lot in this whole process. There are various application fields in which this technology is getting popular day by day. Research, healthcare, pattern recognition, military, etc. are some of the application felids that are using this technology in extensive manner. In addition, there are various businesses that are using image processing to serve different purposes. The use of this technology in business applications helps to automate the several tasks and thereby reduces the manual workload to a large extent.

Image processing plays an important roleinnumerous fieldsand helps to improve the visual presentation of images. In order to generate enhanced images, several computationsandfunctions are performed on the images [1]. Generally, there are two sorts of image processing schemes available. These categories are known as AIP (Analog Image Processing) and DIP (Digital Image Processing). The first category of AIP (Analog Image Processing)makes use of electrical means for the image alteration. TV display is the most popular example of analog image processing. However, the term image processing is typicallyused for digital image processing. The evolution of numerous techniques has made significant improvements in the technology of digital image processing.

In Digital image processing, digital computers are used formanipulation of images. In the last few years, an exponential growth in the use of this technology has been noticed. Its applications cover different fields from medicine to entertainment, passing by environmental processing and remote sensing. A major pillar of contemporary information era known as Multimedia, depend extremely on DIP. The area of digital image processing is immense. This area consists of digital signal processing techniques as well as image-based techniques. An image can be referred as a function f (x, y) that consists two continuous variables x and y. An image should be sampled and converted into a matrix of numbers prior to be processed in digital manner. Generally, a computer uses finite precision for representing the numbers. Therefore, the quantization of these numbers is necessary for representing them in digitized manner. DIP comprises the manipulation of those finite precision numbers.

There are so many ways to process digital images e.g. image enhancement, image restoration, image analysis, and image compression. In the fist method, generally, heuristic methods are used for the image manipulation. This enables a person for the extraction of valuable knowledge from the image. Image restoration methods aimto process the corrupted images [2]. This is done to eliminate the effect of mathematical degradation of the image. Image analysis approaches allow the processing of image for their extraction in automatic manner. Image segmentation, edge extraction and texture & motion analysis are some popular instances of image analysis. Requirement of massive volume of information for image representation is a major feature of images.

1.1.1 Basic Steps in Image Processing

All steps in image processing are summed up as [12]:

- Image acquisition: In this step, a digital image is acquired using a camera.
- Image preprocessing: This step aims to improve the image quality by different means. This increases the possibility for success of the other operations.
- Image segmentation: This step is concerned with partitioning of an input image is carried out into its integral parts or artifacts.
- Image representation: In this step, the conversion of input data is carried out into suitable format for computer processing.
- Image description: This step is implemented for feature extractionand generates some quantifiablerequiredinformation orcharacteristics, essential to differentiate different classes.

- Image recognition: In this step, a label is assigned to an object on the basis of information provided by itsdescriptors [3].
- Image interpretation: This step aims to assign meaning to an ensemble of identified artifacts.

In an image processing framework, the knowledgeregarding any feildissummarizedasa knowledge database.

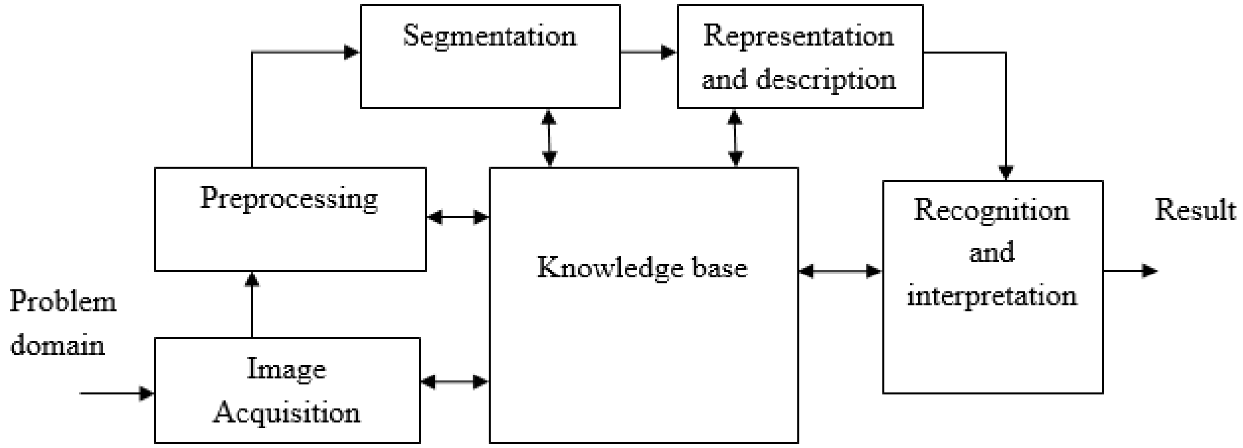


Figure 1.1.1: Fundamental steps in DIP [16]

1.1.2 Applications of Image processing

Following are the popular applications of image processing:

i. Image sharpening and restoration: This application corresponds to the processing of images captured through a digital camera. This approach improves the image quality and manipulate the images for getting desired outcome. This is somewhat similar to Photoshop. Image sharpening and restoration involves, zooming, blurring, sharpening, gray scale to color translation, edge detection etc.

ii. Medical Imaging: This technology can be employed for generating the images of a human body or some part of it. Afterward, the specialists do the processing and analysis of images and provide medical treatmenton the basis of their observations. In everyday life, the use of Ultrasonic, X-ray, CT scan and MRI has been quite common for generating medical images. These techniques make use of different sensory systems in independent manner.

iii. UV imaging: Detection of infrastructure damage caused by a tremor is a crucial application of digital image processing in remote sensing. In case of severe damage, a lot of time is consumed to grasp damage. Sometimes, the damage caused by the earthquake cannot be analyzed with human eye because of the wideness of the region affected by the earthquake [4]. Also, this process takes a lot of time and needs hard work too. This issue can be resolved using digital image processing. In DIP, the acquired image is examinedfor detecting different types of damage caused by the earthquake.

iv. Machine/Robot vision: Increasing the visual ability of a robot or machine is one of the key challenges that a robot undergoes nowadays. The use of digital image processing in this field enables robot to see things, recognizethem, detect the obstaclesetc.

v. Hurdle detection: Image processing also performs a major task of hurdle detection. For this purpose, this technology identifies different sort of image objects and then measures the remoteness between machine and obstacles.

vi. Pattern recognition: This application includesanalysis of images obtained from different domains of machine learning. This application with the help of image processing can detect elements in an image and uses machine learning for training the system with regard to different patterns. The role of this application is quite significant in CAD systems, handwriting recognition, and image recognizing etc.

vii. Video processing: A video refers to the speedy movement of images [5]. The video quality relies on the no. of images per frame in one minute. This applicationincludes noise lessening, detail improvement, motion discovery, frame rate translation, aspect ratio alteration, color space transformation and so on.

viii. Military: This field has been intently studied in current time. The available applications includeobject detection, tracking and 3D (three-dimensional) reconstructions of fields, etc. likewise, it is possible to detect a human body or any subject that generate heat using infrared imaging sensors during night. This approach is generally used in the battlefields. Also, 3D recovery of a target is adopted for finding its equivalent to the template stored in the database prior to its destruction via a missile.

1.2 Copy-Move Forgery Detection

In copy-move forgery, a certainareaof anpicture is cut or copied to hide the non essentialparts of an image, and then this part is pasted on some other part. At present, CMF is a leading image tamperingmethod. The use of this image tempering method is quite common due to its simplicity and the generation of high-quality outcomes. Nowadays, this method is used to serve different purposes with the technological advancement. There are various applications in which the use of this image tempering method is quite common. The advantages and disadvantages of this method depend on the purpose for which it is being used [6]. This method hides the original image information and generates the forged images. The implementation of textured areas is carried out as similar color and noise variation features for generating forged image. It is not possible to detect such extreme changes in the statistical properties of an image manually. In order to reduce different types of anomalies amid the real and pasted areas, blurriness is applied on the edges of the altered image [12].

The detection of copy-move forgery is a passive approach [18]. CMF is concerned with copying and pasting of an image area over some other part in the similar image. General reasons of this type of forgery involve hiding a picture constituent (e.g. steganography) or highlighting a specific entity. CMFcan be performed easily and makes a major contribution to manipulate an image, especially when both source and target areas belong to the similarpicture and have similar features [18]. Typically, these features show compatibilityamid the tampered area and the picture. Hence, it is not possible to detect image tempering just seeing by eyes [7]. The generaloperatedregions in the pictureturn out to be grass, foliage or fabric in this type of forgery. These regions can be mixed with the background easily as these regions have similar features such as texture and color [19].

Every copy-move forgery correlates the real image part and the pasted part. This correlation can be used as a base for successfully detecting this sort of forgery. The segments may not match perfectly but just to some extent as the forgery is generally saved in the lossy JPEG format. Therefore, following are the requirements that a copy-move forgery detection algorithm must satisfied [19]:

- The detection schemeshould have the ability to match the majority of small image parts.

- This algorithm should be time efficient by creating few false positives (i.e., detecting inappropriate matching parts) [8].
- The detection algorithm should be based on the assumption that the forged part will possibly be a correlated elementinstead of a gathering of extremely tiny areas or individual pixels.

1.2.1 Framework for forgery detection system

Figure 1.2.1 shows a general framework for forgery detection. All the steps include in this framework for CMFD have been described below:

a. Pre-Processing: This is the primary step in forgery detection. This step implements an image enhancement method for transforming the colored image into gray scale image. In this step, all types of noises are eliminated from the input images.

b. Feature Extraction: This step helps to identify and extract the features of input image for representing image in appropriate manner. Prevention of redundant image data and reducing data size are the two major requirements of feature extraction [9].

c. Matching: This step is implemented for identifying the similarity between the feature descriptors of images when the similarity in an imageconsiders as anindicatorof forgery. There are multiple approaches that can be used to perform this task.

d. Post-Processing: In this task,the classification of image is carried out into fake and original. This step implements transformation on the real and pasted regions.

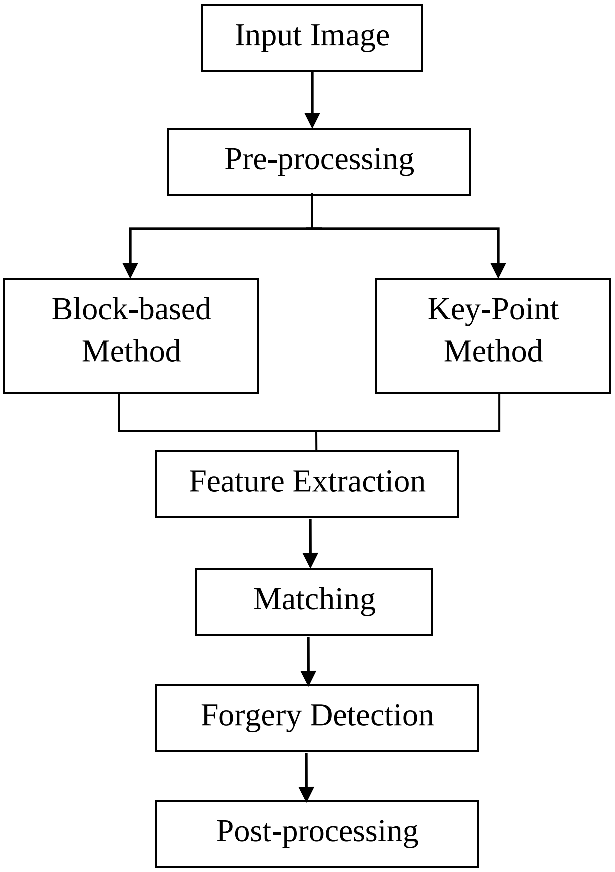


Figure 1.2.1: CMFD (Copy-Move ForgeryDetection) Model [9]

1.3 Copy-Move Forgery Detection Methods:

There are basically two types ofimage forgery methods. The primary category is referred as image tampering while the second category is named as CMF or cloning. In the first category, a specific area of the image is selected [10]. On the other hand, in the second category, a particular area is copied and pasted over some other area of the similar image. This process can hide the valuable image data. The forged picture can be generated by copying and then pasting some image part on the original one. A copy-move forgery method integrates two or more images together for generating the final outcome. 'Foreground' and 'Background' are the two major terms in the context of forgery detection. The term 'Foreground' refers to the object and the RoI (Region of Interest) while terms 'background' represents the rest of the part[10]. Figure 1.3 shows a general classification of CMFD approahes. These techniques are categorized into two approaches of block-based and key-point based.

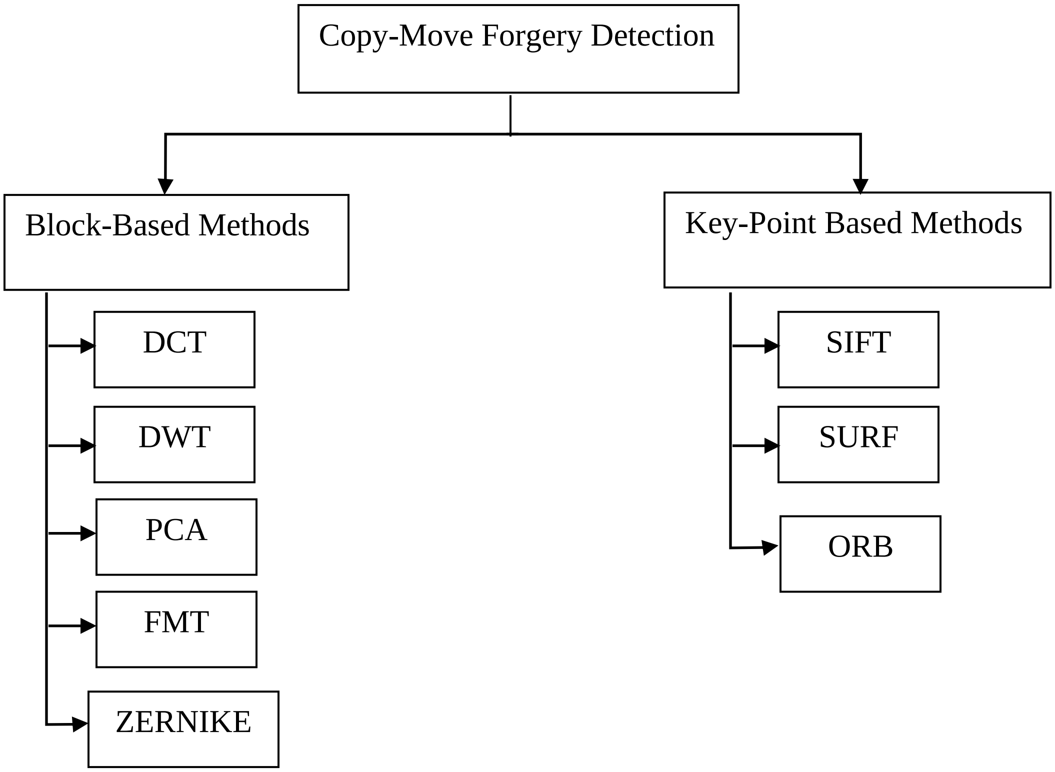


Figure 1.3: Classifications of Copy-Move Forgery detection Techniques [11]

All copy-move image forgery detection techniques have been described below:

A. Block Based Method

In this scheme, the division of an input image is firstlycarried out for generating overlapping blocks. Afterward, the forged area is detected by implementing the feature extraction. After this step, the matching of each block is carried out for identifying similarities [11].

i. Discrete Cosine Transformation (DCT): This algorithm is focused on the conversion of color image from RGB to YC_bC_r color space. In the next step, the division of R, G, and B and Y-component is carried out for generating theoverlapping blocks of a particular size. The neighboring similar image blocks can be generated by extracting the feature vectors and then arranging them in lexicographical manner. In order to identify the copied image blocks, Euclidean distance is adopted as a similarity matrix. The implementation of DCT results in the generation of extremely high-quality results.

ii. Discrete Wavelet Transformation (DWT): DWT approach partitions an input image into four sub-bands rather than partitioning them into overlapping blocks. In this approach, the subdivision of lower frequency band is carried out into overlapping blocks to increase the speed of detection processby minimizing the quantity of blocks. This approach gets the lower sub-band withmoreenergywhichin turn reduces the size [12]. It helpstocapture both frequency as well as the information of the location.

iii. Principal component analysis (PCA): Reduction in image size is the main reason behind implementing this algorithm. It helps to reduce the size of the test image. The main aim of this algorithm is to return the principal component coefficients of a matrix. These coefficients are generally represented as X. The coefficients of single principal component are represented using rows and columns. Some resecahers applied a combination of SURF and SIFT features for getting the benefits of block and key-point based methods. It also assists to modify the parameters related to the assessment and speed. [14]

iv. Fourier Millen transform (FMT): In mathematics, the Mellin transform refers to an integral transform. It is identified as multiplicative version of 2-sided Laplace transform. It helps to obtain invariance against scaling and translation and generates extremely strongoutcomesfor the noisy, lossy JPEG compression and blurry images [13].

v. Zernike moment: Thisscheme helps to localizethe copy-move forgery areas of the digital images. The rotation causes no statisticaleffecton the scale of this approach. Hence, this approach can detect the forged area even in the case of rotated data. This approach also provides support in the detection of the copy-Rotate-Move forgery. This approach also attempts to limit the comprehensive alterations.

B. Key-Point Based Methods

The local feature descriptions of image are applied in the key-point based methods after the division of input image amid isolated points in the first step.At first, these methods identify the high entropy regions, also known as key-points to start the copy-move forgery process.These features are used for extracting the feature descriptors. The matched key-points are detected with forgery by comparing the feature descriptors against each other.Following are the different key-point based copy-move forgery detection methods:

i. Scale Invariant Features Transform (SIFT): This approach aims to detect the duplication of the region. The detection outcomes give an idea regarding the variation in brightness, rotation and invariant with the scale invariant. The invariance of these approaches is not affected by rotation and scaling as the size of all key-points is extremely different from each other. The allocation of descriptors is carried out to the local interest points based on the key-points. Moreover, all descriptorsare compared against each other and the matched descriptors are implemented for the detection of forgedarea. Here, the scaling and rotating techniques are applied for the localization of matched key-points [14].

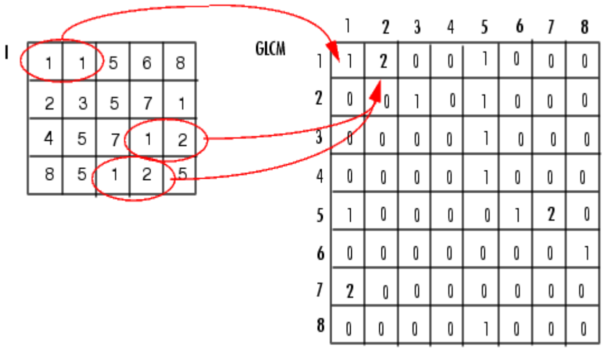
ii. Speeded-up Robust Features (SURF): This approach performs feature extraction on the basis of the sums of 2D Haar Wavelet replies. It competentlymakes use of the vital images and generates speedy and robust outcomes. Moreover, it also makes the detection of displacements and distortions very easy. This geometric alteration causes no effect on this approach. This approach does the detection of multiple cloning and helps to achieve the high computational efficacy. The presence of compressed JPEG image and flat duplicate areas minimizes the appropriateness of SURF detector. The presence of small tempered area reduces the efficiency of outcomes.

iii. Oriented FAST and Rotated Brief (ORB): The fusion of BRIEF descriptor and FAST detector approaches for developing ORB approach generates the extremely high-quality results in terms of cost and efficiency. FAST and its variants are applied in realistic frameworks for the detection of key-points. Block patterns helps to obtain the key-point orientation, histogram and approximation of gradient.

1.4 GLCM (Gray-Level Co-Occurrence Matrix)

GLCM can be described as a statistical method to analyze texture, based on the spatial relationship of pixels. The texture features of second order are extracted using algorithm.The GLCM algorithm calculates the texture of an image based on the number of times pixel’s pair with certain values and a specific spatial relationshipoccur within an image to creat a GLCM. Afterward, statistical featuresare extracted from this matrix.

The GLCM algorithm is implemented for the extraction of second order statistical texture features. It provides information about the location of pixels containing similar gray level values [15]. In this matrix, the equal numbers of rows and columns occur along with the number of gray levels in an image.



1	1	5	6	8
2	3	5	7	1
4	5	7	1	2
8	5	1	2	5

	1	2	3	4	5	6	7	8
1	1	2	0	0	1	0	0	0
2	0	0	1	0	1	0	0	0
3	0	0	0	0	1	0	0	0
4	0	0	0	0	1	0	0	0
5	1	0	0	0	0	1	2	0
6	0	0	0	0	0	0	0	1
7	2	0	0	0	0	0	0	0
8	0	0	0	0	1	0	0	0

Figure 1.4: GLCM Matrix [21]

Figure 1.4 shows the implementation of gray comatrix function for computing the first three values of GLCM. Because of the occurrence of just one situation in the input image, value 1 is included in the component (1,1) specified as output of GLCM. Here, the values 1 and 1 are allotted to two horizontally neighboring pixels correspondingly. GLCM (1,2) comprises value 2 since there are values 1 and 2 for two examples occur in the horizontally adjoiningpixels. The value 0 is allotted to element (1,3) as no adjoining pixels have 1 and 3 values.

Chapter 2

Literature Review

Haipeng Chen, et.al (2020) suggested a well-organized CMFD technique in which SIFT key points were clustered and the similar neighborhoods were searched to place the tampered regions [16]. The clustering of keypoints was done according to the scale and color. They were matched and grouped further into several smaller clusters. The high dimensionality of SIFT caused high time complexity, so this technique helped to reduce that complexity. A new localization algorithm was designed that helped to recognize the forged areas in pixels precisely. This algorithm had used two similarity measures to compare the parallel neighborhoods and to find the manipulated parts of matching pairs. In this suggested approach, three various image data sets were utilized for comparison and verification of efficiency and robustness. With respect to the accuracy of forgery location, matching time complexity and detection consistency, the proposed method provided more efficient results than the existing techniques.

Kunj Bihari Meena, et.al (2020) recommended a novel Tetrolet transform based approach forto detect forged areas in an image [17]. In the beginning, the input picture was separated into overlapped blocks. Tetrolet transform was employed to extract the 4 low and 12 high-pass coefficients. Then feature vectors were sorted in lexicographical order. The extracted Tetrolet features were matched to recognize the similar blocks. The results acquired after the experiment were demonstrated that the recommended technique was appropriate for detectingthe forged parts in a precise way. This technique was effective even in post-processing tasks such as blurriness, rotation, tuning of illumination and contrast and scaling of a copied region. In case of smooth image, the detection of very minor duplicated regions and numerous forgery cases was easily done by this recommended method.

Jun-Liu Zhong, et.al (2020) recommended a highly proficient technique called two-pass hashing feature representation for CMFD [18]. Firstly, the extraction of corresponding blocks from multiple frequency images was done by presenting the normalized moment transformation. The corresponding hashing features were obtained by projecting the multi-dimensional traits of all pixels in equivalent hashing bin. The multiple hashing attribute was concatenated with the presented approach. The two-pass hashing searching algorithm was used efficiently to search and update the adjacent pixel matching. Then the post-processing operations recognized the forgery regions correctly. After the testing it had been observed that the recommended copy-move forgery detection technique acquired the more accurate result than other earlier used techniques. Moreover, the proposed method had efficiently detected the copy-move forgery even under the several attacks without iterations.

Gul Muzaffer, et.al (2019) suggested the architecture based on DL for detecting and localizing the forgeries in copy-move despite conventional schemes of extracting features [19]. The attributes of image sub-blocks were acquired using aPretrained AlexNet CNN in this approach. Thereafter, these sub-blocks were matched. At last, false match elimination was carried out. The outcomes of testing depicted that the suggested approach was better as compared to referenced works. The future work would focus on suggesting more robust technique for providing superior performance in various situations.

Nidhi Anna Kurein, et.al (2019) investigated the issues and proposed a consistent method for the recognition of CMFs. The two major approaches were used to detect the forgery in copy-move [20]. The first was block based and second one was key point based. The Block-based technique was utilized for the partition of overlapped image matrix into blocks and also for the extraction of attributes. The key point feature of every image was extracted for the matching, in the key-point based technique. Two algorithms for detecting the forgery in copy-move were implemented in the presented approach. These were DCT algorithm based on blocks and Scale Invariant Feature Transform based on key points. The efficiency of both the algorithms had been evaluated and GRIP and CoMoFoD databases were utilized for comparison. After the testing, it was observed that the SIFT had provided better and more accurate results than Discrete Cosine Transform method.

Chengyou Wang, et.al (2019) intended an image CMDF technique to detect the forgery images [21]. Two attributes recognized as SURF and PCET were implemented in this technique. First of all, super pixel segmentation had split the image into non-overlapped irregular image blocks. Furthermore, these blocks had included 2 parts – smooth region and texture region. The coefficients of PCET were extracted only when SURF found the key points. Feature matching algorithm had utilized all these coefficients to search same kind of features. After it, false matched points were eliminated and the portions with dense matched points were found by using one tactic. The RANSAC was combined with a filtering scheme. At last, for the refinement of tampered regions, mathematical morphology and an iterative strategy was used. This recommended technique was proved better to detect the forgery of high-brightness smooth region than other CMFD methods. The results after the experiments also verified that the suggested technique had resisted various distortions of diverse attacks.

Aya Hegazi, et.al (2019) suggested a novel technique for CMFD on the basis of SIFT feature [22]. For mitigating the false matches in well-organized manner, two algorithms were introduced. Different datasets that contained various typologies and resolutions of fake as well as original pictures had been investigated in this method. The experimental results demonstrated that the suggested approach attain superior outcome as compare to other latest methods even in the presence of various attacks. This recommended technique had ability to detect the several CMFs with least false matches.

Badal Soni et.al (2019) investigated an improved block-based CMFD technique with the hybrid local features extraction [23]. Initially, an image was split into the blocks that were not overlapped. Then surf features were calculated and matched with each block by using 2Neural Network process. The formation of huge blocks was done and 8 neighbor blocks were considered for every Surf feature match block. The detection of maximally SERs from great regions and then extraction of speeded up robust features descriptors from these regions was done in order to perform matching. The outliers were eliminated by an affine transformation. The experiment of proposed technique had been done by utilizing different standard datasets. The experimental results produced more accurate presentation than other existing techniques.

Priya Mariam Raju, et.al (2018) suggested a new method in order to detect the forgery in copy-move in which the conventional block oriented and key-point oriented schemes had been assimilated [24]. By utilizing the key points of an image, the similar areas within the image were recognized without any difficulty. In this technique, the extraction of key points and detection of matching points had become easy by employing Binary Discriminant features. The effectiveness of this suggested technique to detect the forgery in copy-move had been authenticated by the tested results. This technique had acquired more precise and accurate rates as compared to other accessible approaches. High accuracy and high-quality results had been achieved after the utilization of this approach. The detection of not only single but also the multiple copy-move forgery had been done by this recommended technique. This suggested approach had received better accuracy and F1 Score metrics.

Yong Yew Yeap, et.al (2018) in this work suggested a technique that had been based on the passive forgery identification [25]. Copy move methods were applied to complete the tempering of images. A CMFD approach with oriented fast and rotated brief, for feature extraction was applied in this work. For the feature matching format, Hierarchical Agglomerative Clustering along with the 2NN had been employed. This suggested technique demonstrated the effective results when it was used on the images that were affected by the geometrical interruption. The achieved overall outcome for feature extraction and feature matching was 84.33% and 82.79% respectively. In the conducted experiment, True Positive Rate more than 91% for the multiple levels of rotation, entity conversion and enhancement had been observed for counterfeited images.

Yue Wu, et.al (2018) suggested a novel NN in which copy-move forgery had been utilized to recognize and predict the forged masks [26]. For extracting the block-like feature from the images, this convolutional neural network had been applied in this approach. Self-correlations had been calculated by numerous blocks. In this work, the matching points were positioned by a point-wise feature extractor. In this approach, adeconvolutional network had been used and a forgery mask was renovated. There had been several training and parameter stages employed in this recommended approach. This suggested approach had been completely trained and the failure of forgery mask renewal had been improved. The recommended approach had acquired more efficient outcomes in terms of various attributes as compared to existing methods. This suggested approach had competently protected the information from the anonymous attacks.

Gul Muzaffer, et.al (2018) recommended a block basedmethod for CMFD [27]. This technique had employed the LIOP for the feature extraction from the blocks. LIOP was a novel and more proficient method that detected the copy-move forgeries quickly when applied with Patch Match algorithm. This recommended technique was further compared with latest works. The attack resistance was also investigated. The testing results proved that the recommended technique performed efficiently while detecting the forgery in copy-move even under several cases such as blurring, rotation, scaling etc.

Amanpreet Kaur, et.al (2018) recommended a technique based on block and keypointfor detecting the forgery in copy-move [28]. Keypoints based features were less complex computationally than block-based features. That was why there were selected for this technique. The four feature extractions algorithms were applied such as SURF, KAZE, BRISK and Harris corner point. These all keypoint based algorithms were analyzed and their efficiency was verified for CMFD. In this recommended technique, 4 major phases were used in which image was pre-processed, interest point detector, feature vector description had utilized and feature was matched. The threshold parameter was utilized for the matching algorithm to calculate the accuracy, f1 score and precision. The experimental results were compared on the basis of these three parameters. At last, it was observed that the finest result was provided by KAZE feature in all performance metrics. On the other hand, Harris Corner points were scale invariant and they detected only corners not the edges, so it was not appropriate for copy-move forgery detection.

H.M. Shahriar Parvez, et.al (2018) intended a new technique on the basis of region-duplication for forgery detection [29]. This was classified into region duplication technique based on segment. This algorithm was designed on the basis of image segmentation by using Gabor descriptors and K-Means. At first, the Normalized Cut segmentation method was used to segment the image. The image features were extracted by using Gabor Filters. For the clustering of the image features, K Mean clustering algorithm was applied. The clustered regions were compared with the given threshold value to count the authenticity of the image. It had been observed in the testing results that the recommended approach worked efficiently in case of rotation, scale, blurring and all post-processing attacks. The suggested algorithms achieved the better performance results as compared to the existing techniques.

Ali Mumcu, et.al (2018)in this work studied that the manipulation on digital images had been become trouble-free by using the improved image tools frequently [30]. Among all the forgery techniques, copy move forgery due to its simplicity was the most commonly used method. This kind of forgery detection method had included two types. In this work, the forgery detection based on key point was selected. FAST algorithm was utilized to extract the key points and SIFT algorithm to calculate the description vectors. To decrease the run time of the program, parallel programming methods were applied during the implementation of this recommended technique.

Yildiz Aydin, et.al (2018) studied that in essential areas, the digital images played a crucial role, so it was necessary to verify the reliability of images [31]. CMF was a kind of digital image forgeries that had been easily accomplished by using image editing software. A novel key point-based technique was suggested in order to detect the forgery in copy-move. In the literature, the recommended approach had been compared to the Speeded-Up Robust Feature algorithm. The experimental results provided the evidence that the suggested method performed accurately even in post processing operations.

Geetika Gupta, et.al (2017) in this paper investigated a novel technique to detect the copy-move forgery from the images [32]. The information regarding the original image was not required in this mentioned technique. At the starting, the grayscale image had been developed by the overlapping blocks. After it, the extortion of attributes had been done by utilizing the hybrid approaches. This hybrid technique had comprised of the oriented gradient of PCA and histogram. All the attributes had been arranged in the lexicographical way at the end. The straightforward matching of bogus sections had been completed in this observable fact. In this recommended approach, an accurate available method had been applied and compared. After the investigation, it had been observed that the false matches were diminished by the presented offset threshold. This recommended technique had achieved high-quality performance in the assessment of the result and granted two classes of security intrusions. On the account of certain parameters, this suggested approach had provided the better results.

Dhanya R, et.al (2017) recommended the esteem of Image forgery detection approach in the domain of forensic science that had become popular [33]. A brief examination had been conducted on the copy-move forgery in this research. Each and every existing technique with all the appropriate stages to detect the forgery in copy-move had been mentioned in this research work. These existing approaches had some certain constraints due to which these techniques were not exercised in spacious manner. These approaches had required some improvements, so several challenges had been described in technical way in this work. To extract helpful information and accurate values of metrics, numerous tasks were conceded. All the constrictions that were present in existing approaches had been eradicated by the suggested approach. This was the main purpose of this advocated technique. After the investigation it had been found that the suggested approach had provided proficient result of image forensic in less expensive scaffold.

HaniehShabanian, et.al (2017) affirmed that CMF had assisted in tampering the digital images [34]. The replica parts had been carried out from the similar images. In this work, fake sections had been detected by the Forgery detection method. In order to detect the forgery in copy-move from digital images, a new scheme had been introduced in this work that was block-based. The structural similarity index format had been applied as similarity matching step in this approach. Gaussian Pyramid Decomposition technique had been used for the significant enhancement in the run-time speed. The less time had consumed in this technique. The calculation and inspection had become uncomplicated by this technique with some vital measurements. After the testing, its results demonstrated that this recommended method had performed better than the earlier techniques not only in account of effectiveness but also in receptiveness.

Junlin Ouyang, et.al (2017) suggested a new convolutional neutral network based CMFD technique [35]. In the recommended technique, the existing trained model that was taken from the large database ImageNet had been used. The small training copy-move samples were slightly adjusted the net structure. It was observed in the result that the suggested method provided good performance when computer generated the forgery image automatically with the simple image copy-move operation. But the CMF image of real picture was not robust in this method. The reason of this occurrence was carefully evaluated and visualized by using the feature map of CNN. Therefore, some suggestions and methods were mentioned in the conclusion. For the CMFD, the Convolutional Neural Network was applied as this recommended technique had some limitations. The CNN based copy-move forgery detection method required additional research to enhance and acquire the accurate performance in real circumstances.

Tarman, et.al (2017) studied that the CMF was very dangerous. The digital world of images had been affected by it and its detection was also the hardest [36]. In this work, the demonstration of image forgery, types of image forgery, detection techniques and their limitations were described. The new method M-SIFT, an enhanced edition of SIFT that was based on keypoints had been used to detect the forgery also discussed. Furthermore, the implementation and performance evaluation of the proposed algorithm was also described in this paper.

Yuan Wang, et.al (2017) suggested a passive image authentication technique for the CMFD [37]. The picture was divided into overlapping blocks and each block was labeled with LBP. On blocks that were labeled, the extraction of one of the biggest N of Singular Value Decomposition values was performed. The feature vector comprised of SVD value N plus average Y, Cb, Cr values for the block. They were arranged in lexicographical manner. The forged blocks were found out by using element-by-element method. The results of this experiment verified that the presentation of the recommended technique was admirable to detect the forgery in copy-move.

K RemyaRevi, et.al (2017) suggested that the CMF was the prevalent image tampering method [38]. For detecting the CMF, two methods were suggested. These methods were based on block and key point matching. It was observed that the key-point based method had performed more efficiently with respect to computational efficiency and space complexity, as compare to the block-based technique. The key-point based method had proved robust against different geometric transformations. Scale-Invariant Feature Transform method that was key-points based had been reviewed in this work.

Sajjad Dadkhah, et.al (2017) suggested a technique with Ward linkage-based clustering for copy-move detection. SIFT algorithm was utilized for extracting the local image attributes [39]. The Ward-based clustering system consisted of 3 levels of false descriptor elimination. This scheme had been utilized for the detection in this suggested technique. The precision of this technique was enhanced by using Euclidean distance in this proposed elimination system. In the final evaluation, the recommended algorithm performed efficiently against a variety of post-processing attacks. Simulation outcomes demonstrated that the detection accuracy had been enhanced by the suggested algorithm after the elimination of false descriptors.

Mejren Mohammad Al-Hammadi, et.al (2016) intended a CMFD techniqueon the basis of advanced attributes of Speeded up Robust Features to detect the small size forgeries [40]. A SISR approach was used for preprocessing the image that improved the keypoints detection. For the better performance, the recommended approach was compared with original SURF by wide-ranging set of experiments. The dataset in which forgery size was small had been used for the evaluation of this method. The results produced after this experiment confirmed that when small size forgeries were used this proposed method outperformed the SURF.

Hajar Moradi-Gharghani, et.al (2019) recommended a novel block-based CMFD method to detect the tampered region [41]. The DTC transform was used to extract the feature vectors. These feature vectors were organized in lexicographical manner in this method. On the basis of some criteria, the selection of copied blocks was done from the identical vectors. The large flat parts of the picture were eliminated for forgery detection. That was the uniqueness of this work and considered a dispersion threshold. The simulation result demonstrated that the forgery detection of the image with small False- Positive had done more efficiently concerning FPR and DAR in comparison with the conventional methods.

Ahmet Boz, et.al (2016) investigated a novel technique to detect the forgery in copy-move [42]. In this method, LBP and DCT were applied. First of all, the partition of an image was done into the overlapping blocks. Every block of image then converted to LBP domain. Then Discrete Cosine Transform was carried out on these converted blocks for obtaining the feature matrix of the image. This feature matrix was sorted lexicographically and then the similar blocks of the image were arranged in sequence. To diminish the false positives and to derive the local features that was not much sensitive to varying lighting conditions, was the main objective of this technique. It was possible only when DTC was used on blocks of the image that were converted to LBP domain. The outcome of this testing had provided the fewer false positives result, when LBP and DCT were applied together to individual usage to detect theimage forgery in copy-move.

Shi Wenchang, et.al (2016) recommended a new technique that was known as CMFD-PSO [43]. The PSO was integrated into Scale Invariant Feature Transform-based framework by it. The customized parameter values that were implemented to detect the forgery in copy-move in Scale Invariant Feature Transform framework had been generated by applying PSO algorithm. After the testing, the results demonstrated that the customized values for images had been generated automatically by the CMFD-PSO and these values were not independent of experiences and experiments. It was also evaluated that CMFD-PSO had provided more efficient results as compared to EPV-SIFT. The detection of region duplication became more accurate and more suitable with the CMFD-PSO as it had increased the number of true matched key points significantly.

Atefeh Shahroudnejad, et.al (2016) suggested a new CMFD technique on the basis of Affine SIFT [44]. That suggested technique was fully affine invariant. The transformation and deformation of copy-move regions had been efficiently done by this method. First of all, the matched key points of ASIFT were searched. Then super pixel segmentation and morphological operations were utilized so that all the pixels were estimated within the duplicated regions. After the experiment, it was evaluated that the recommended approach was well-organized and influential for the detection of copy-move regions. This technique had worked with accuracy even when the copied region had passed from the post-processing and transformations.

Xiuli Bi, et.al (2016) presented a novel adaptive polar based filtering approach to detect forgery in copy-move in images [45]. This work paid attention to the post-processing of the matching outcomes for improving the efficiency of the presented approach. In this work, the extraction of two-pixel sets had been carried out for filtering out the unnecessary pixels from the pixels which were matched at first. The extracted pixel sets were identified as matched pixels set in symmetrical and unsymmetrical way. Moreover, the computation of the polar distribution of the two sets had been carried out correspondingly. Afterward, it was possible to compute the filtering thresholds based on the polar distribution in adaptive manner. Also, the unnecessary pixels could be filtered in the same way. At last, the identified forged areas were generated by implementing some morphological operations to the other pixels. The tested outcomes revealed that the presented approach provided much improved outcomes in terms of CMFD in comparison with the other traditional approaches.

Rahul Dixit, et.al (2016) intended a new CMFD approach. The new approach was designed according to the Undecimated DyWTfor its working [46]. The presented scheme did the division of a picture into sub-blocks of pixels with the purpose to find the image blocks similar to each other. This was done to identify the forged image parts. This work applied the Canberra distance formula for computing the similarity among blocks regarding the features extracted by the presented approach. Afterward, the reduction in the number of fake block matches contributed for enhancing the detection precision of the presented approach. A lot of tests were conducted in this work for evaluating and comparing the presented approach. The tested results demonstrated that the superiority of the presented approach against the other techniques in terms of detection accuracy.

Haoqing Luan, et.al (2016) studied a very popular image forgery method was identified as CMF (Copy Move Forgery) [47]. This image tempering method had hided the redundant artifacts and generated the duplicate version of the required artifacts for changing the sense of images. A novel CMFD method was recommended on the basis of SIFT. It was possible to identify the various copied and moved images parts using the double thresholds. The tested outcomes revealed that the presented approach showed robustness against obstructions and different levels of geometric image treatments.

Guangcheng Cao, et.al (2015) suggested a technique of copy-move tampering in the same image. It was Locality Preserving Projection (LPP) based passive forensic method [48]. The detected image was put into various small blocks firstly and then continued to their coordinates. It was assured by the similarity matrix that before and after the transformation, there was not any change noticed in neighboring relation. The LPP algorithm was applied to lessen the dimension of block. At the end, the reduced dimensions of the small blocks were matched to complete the forgery detection. After the experiment it had been evaluated that the proposed technique located the tamper on the exact position accurately and also detected the copy-move forgery effectively. After the comparison with PCA, it was observed that the proposed technique had improved the detection precision. This method also reduced the complexity of algorithm and time of testing.

Neetu Yadav, et.al (2015) studied that the copy-move forgery was a simple method that consisted of image improvement software with numerous well-built tools [49]. The similarity between the copied and pasted area of similar original image was created on the same region frequently by the CMFD techniques. For the verification of CMF, methods based on key-points and block had been applied. Forgery was localized correctly when various techniques and SIFT key-points were joint together. In the SIFT examination it was observed that the high dimensionality of feature vector was acted as a bottle neck. In this paper, a method to detect the forgery in copy-move by using SIFT descriptors was suggested. GMM was used to cluster the SIFT descriptors and analysis was speeded-up by the obtained suspect region.

Surbhi Sharma, et.al (2015) studied that the forgery occurred easily with the development of image processing methods. The other main factor was the usage of multimedia communication rapidly [50]. In the digital images the most common problem was copy-move forgery. There were many techniques to detect the forgery in copy-move. A well-organized was described for detecting CMF. The Center Symmetric LBP was utilized to detect a copy-move forgery from the medical images that had size up to 12*12. The testing results proved that the recommended block-based technique was robust to deal with several attacks including Gaussian blurring and geometric distortion. It had been evaluated that the proposed approach performed more accurately as compared to other existing methods.

Davide Cozzolino, et.al (2015) suggested a novel approach in order to detect and localize the forgeries in copy-move [51]. This algorithm was planned on the basis of RIFs. In the literature, dense-field methods ensured the better-quality performance with reference to the key-point based counterparts. But this technique provided a performance at the rate of higher processing time, just because of feature matching phase. Then a fast approximate NSS algorithm named Patch Match was applied to overcome the drawbacks of earlier used algorithm. This was an appropriate method to evaluate the dense regions of the pictures. This matching algorithm had dealt efficiently with the invariants and proved robust while dealing post processing. A simplified and trustworthy post processing procedure was implemented in this technique. This investigation of this proposed technique was done by using databases that were available online. It had been observed that the recommended technique acquired the accurate, faster and more robust performance as compared to other dense-field methods.

Salih Türk, et.al (2015) presented DoG Coding approach to detect the forgery in copy-move [52]. The variations in image illumination caused no effect to the new approach. This approach helped to generate the coded new image. The use of this approach was quite common in the palmprint recognition frameworks. The image was divided into sub-blocks for determining the features. The block-based region growing segmentation algorithm had been designed for determining the magnitude of the duplicate area. This work used CoMoFod dataset that included images, captured under different conditions for the testing of the presented approach.

Elham Mohebbian, et.al (2015) stated that a very popular image tempering method was identified as copy-move forgery [53]. This image tempering method was quite popular among image falsifiers. This work presented an approach planned on the basis of DCT for the detection of image forgery by taking into account the complexness of the acquired image. The classification of images had been carried out into two classes for the detection of forged area. These classes were identified as smooth and complex. The implementation of DCT approach had been carried out to every block for the feature extraction. The tested outcomes revealed that the presented approach could accurately identify the forged areas even in the case when various image manipulation methods had been applied on the images.

EdoardoArdizzone, et.al (2015) presented an extremely new hybrid methodology to detect the forgery in copy-move [54]. The presented methodology performed comparison among triangles instead of blocks (or single points). In this work, the extraction of interest points had been carried out from the image while the artifacts were demonstrated in the form of a set of linked triangles which were constructed on these points. The matching of triangles had been carried out based on their shapes, content and the local feature vectors against the triangles' vertices. The developed techniques showed robustness against geometric variations. The outcomes generated by the presented approaches were compared against different existing CMFD approaches. In addition, the researchers in educational institutions could use the dataset adopted in this work.

DijanaTralic, et.al (2014) proposed that the copy-move forgery was achieved in the video sequences. In the same sequence, the copying and pasting of a set of frames was done at a new location, to accomplish the forgery. As a result, the altered video content was obtained [55]. For the identification of CMF video, the development of robust descriptor was required. This descriptor helped to examine the duplicated video frames. The LA and LBP were applied as texture descriptors in this technique. Every frame was divided into overlapping blocks. The Cellular Automata had been applied in a frame to learn the set of rules that described the intensity changes of every block. The duplication of frames was detected by using the histogram feature. After the experiments, the recommended technique provided the accurate and high efficiency results for the detection of CMF videos.

TakwaChihaoui, et.al (2015) suggested an automatic hybrid technique in order to detect the forged image areas [56]. This work made the utilization of SIFT for identifying the local image attributes. This work also used SVD approach to match the similar features of the images. The tested outcomes revealed that the presented approach showed robust against geometrical alterations. This approach could successfully identify the forged parts in the image.

Le Zhong, et.al (2013) presented a novel mixed moment based blind detection technique for making the existing image region CMFD (Copy Move Forgery Detection) approach more robust for the post processing [57]. Initially, this approach made use of GPT (Gaussian Pyramid Transform) for the extraction of low-frequency information from the picture and the division of low frequency region into overlapping blocks. Then, the eigenvector of block, made up of exponenti-fourier moments and histogram moments had been organized in lexicographical manner. Next, Euclidean distance and space distance were considered to place the tampered area in precise and speedy way. The tested outcomes revealed that presented approach could identify the tempered image area in efficient manner with the help of different methods (e.g. translation, rotation, scaling and mixed operation tamper) even when the image was captured in different lighting conditions and had different contrast levels.

Sunil Kumar, et.al (2013) studied that the use of BM (Block matching) algorithm or block tiling algorithm was quite common for the detection of image forgery [58]. These algorithms faced a major challenge related to the time. The increase in the image size increased the number of overlapping blocks in speedy way which in turn increased the time of feature collection and matching. The presented approach eliminated this issue without degrading the quality of the technique. This work applied DCT (Discrete Cosine Transform) for representing the characteristics of overlying blocks. This work also tried to computerize the threshold to differentiate the lost matches from the real matches.

Chapter 3

Proposed Work

3.1 Problem Formulation

In general, an image represents the real-time event. Digital images have turned out to be an important part of everyone’s life in the recent times. These days, an image can be tampered easily using the available digital processing tools.The art of image tampering is itself a subject of study. Nowadays, generating reliable forged images is no more difficult due to the availability of digital and common image manipulation techniques. In recent times, it is possible to generate manipulated images using some news items, technical tests and lawful evidences. Hence, no one can guarantee the authenticity of images. All these factors generate the need for the effective tools and technologies for the recognition of image forgery. The techniques used to detect the image tampering evaluate the authenticity and uniqueness of a picture. Digital image processing software and editing tools, make the task of image manipulation and image enhancement very simple. It is not possible to distinguish the real image and forged image by naked eye. Now-a-days, massive amount of digitally forged images is available online. This is a serious threat and decreases the reliability of digital images. Hence, different techniques are developed for validating the genuineness of the acquired image. Hence, the image forensics aims to detect the image forgery. Here are the different research gaps:

1. The CMFD intrusion can manipulate the real information. Over the time, different approaches have been developed for the detection of the copy-move forgery. However, most of the approaches are based on the idea of template matching. The matching of each and every pixel increases the execution time to a large extent. In order to overcome this issue, this work makes use of PCA and GLCM algorithm for CMFD.

2. The approach developed to detect the digital image forgery is based on the notion of morphological operation. The extreme complexity of morphological operation also reducesthe detection accurateness. This gap is also fulfilled by the new approach.

3.2 Objectives

This segment includes the objectives of this researchwork. The key objectives of this work are:

1. To design a robust algorithm for detecting copy-move forgery in images.

2. To detect the copy-move parts in forged images.

3. To make comparison between the introduced and existing techniques in terms ofprecision,recall and F1-measure.

3.3 Research Methodology

Following are the various steps which are applied for the copy-move forgery detection:-

1. Keypoints/Feature extraction

The attributes are extracted from the image in the first stage. These features are used for detecting the forgery. The procedure in which abstractions of image information is acquired is known as feature detection. The key points are implemented as the attributes in this technique for the recognition of forgery's position. The comparison of attributes is performed in the image for detecting the copy-move forgery. The forged portions are represented by the same points in an image.

2. Apply GLCM Algorithm

The grayco-matrix function is applied for developing a GLCM. This function computes the value of occurrence of pixel using the intensityvalue *i* in a specific spatial association to a pixel having the value *j*. The pixel of interest and the pixel to its immediate right are used to describe the spatial association by default. However, the spatial relationships can be identified within two pixels. In the resultant GLCM, every element (*i*,*j*) is the addition of the number of times that the pixel that has value *i* which is occurred in the specified spatial association with value *j* within the input image.The input image is scaled using thegrayco-matrixas the processing is prohibitive for computing a Gray-Level Co-occurrence Matrixof an image. The scaling is carried out in thegrayco-matrix for alleviating intensity values that comprised in grayscale image. The size of thegray-level co-occurrence matrix is determined through the number of gray levels. The NumLevels as well as the GrayLimits parameters included in the grayco-matrix function are implemented so that the number of gray levels in the Gray-Level Co-occurrence Matrix and the scaling of intensity values are controlled. There are some properties of the spatial distribution of the gray levels which are contained in the GLCM within the texture image. To illustrate, the texture becomes coarse in terms of the specified offset in case of contemplation of various entries in the GLCM with the diagonal. The gray-level co-occurrence matrix has provided a number of statistical measures.

For instance, the computation offirst three values usinggrayco-matrixin a GLCM is represented in the Fig 1.4.The value 1 is comprised in the element (1,1) in the output GLCM as the input image has only one example in which the values 1 and 1 is assigned to two horizontally adjacent pixels. The value 2 is comprised in element (1,2) of GLCM as there two examples in which the values 1 and 2 is defined for two horizontally adjacent pixels. The value 0 is comprised in the element (1,3) in the GLCM since, the values 1 and 3 is assigned for two horizontally adjacent pixels as they have not any instance. The input image is processed, the image for other pixel pairs (*i*,*j*) is scanned and the sums in the corresponding elements of the gray-level co-occurrence matrix are recorded with the help of grayco-matrix. The GLCM algorithm considers theaverage of the features. This average will further utilize asinput to PCA algorithm in order to reduce the feature. PCA algorithm is a widely used method for the image formation, for example, data, as the identification of similarities and differences between them can be done effectively. By maintaining a strategic distance from redundant information, dimensions of an image can be reduced without suffering much loss which is another advantage of the PCA algorithm. With the help of statistics and mathematical schemes including PCA etc. can be easily understood. In the field of image recognition and compression, various applications have been provided by this valuable statistical PCA method. The mean taken of the features extracted by the GLCM is further used for determiningthe block's size as the image is further divided in blocks for easy feature extraction with maximum number of features in a block.

3. Apply PCA Algorithm [23]

Thevaluable information from each image block is extrcated using PCA algorithm. It is a multivariate method which is adopted for the analysis of data table [24]. This data table characterizes various correlated variables based on their quantity. This algorithm aims to extract the valuable information from the table so that new orthogonal variables can be represented. These variables are referred as principal components.

The approach displays instances based on the similarity of observations while the variables as points within maps. The data is placedmainlycorresponding to every variable if a specified data matrix includes p variables and n samples. The data occurs in the middle after the generation of principal components. This, however, does not affect the spatial relations of data or the variances occurring along the variables. The first principal component (Y_1) is given by the linear combination of variables X_1, X_2, ..., Xp. The first principal component can be represented as [59]:

$$Y_1 = a_{11}X_1 + a_{12}X_2 + \cdots + a_{1p}X_p \qquad \dots (1)$$

As matrix, it can be represented as:

$$Y_1 = a_1^T X \qquad \dots (2)$$

The first principal component is measured to discover the highest possible variance within the data set. The variance of Y_1 can be generated by the selection of big values for weights, represented as $a_{11}, a_{12}, \dots a_{1p},$. The weights are measured with the limitation such that the sum of squares is 1, to avoid such condition.

$$a_{11}^2 + a_{12}^2 + \cdots + a_{1p}^2 = 1 \qquad \dots (3)$$

The second principal component is measured in the similar manner to prevent the occurrence of correlation in the direction of the first principal component. The next maximum variance makes use of this second principal component.

$$Y_2 = a_{21}X_1 + a_{22}X_2 + \cdots + a_{2p}X_p \qquad \dots (4)$$

This process continues till the measurement of p principal components. These components correspond to the original number of variables. Corresponding values are achieved for the sum of variances of all principal components and the sum of variances of all variables in this point.

Hence, the changesin all real variables with respect to the principal components can be represented as:

$$Y = XA$$

4. Keypoint matching

The matching of keypoints which are extracted from the input image is done with each other for the recognition of same points in the similar image. The identical regions are discovered in an image using the value of threshold in the presented forgery detection techniques. The value of threshold for keypoint matching is not calculated with any mathematical model due to which it may be inaccurate for certain images.The value of threshold is chosen heuristically.But the blocks made with the help of GLCM output are known to be the most appropriate features of the image so we can say the value we achieved of the threshold must have the best value above which we can say that the pixel doesn’t have any kind of informatic value of the feature of the image so we can discard that pixel. Similarity matching is performed within the pixels, once the required pixels are obtained.So, the Euclidean Distance is employed as the similarity measure because of its accuracy. If the Euclidean Distance between the keypoints is above the desired chosen threshold value, such keypoints are regarded as similar. The labels are assigned to these keypoints and taken as matching feature points.

5. Suspected region identification

The only position of forgery areas is the matching attribute points. The extraction of these areas is performed in more accurate manner.Anapproach based on block related to region localization has been implemented when every matching keypoint is replaced with unmatched keypoints. These keypoints are achieved from the earlier stage. The keypoints will be compared with the other blocks to evaluate forgery pixels from the image. Further the morphological operation is applied to which mark the forgery part on the image.

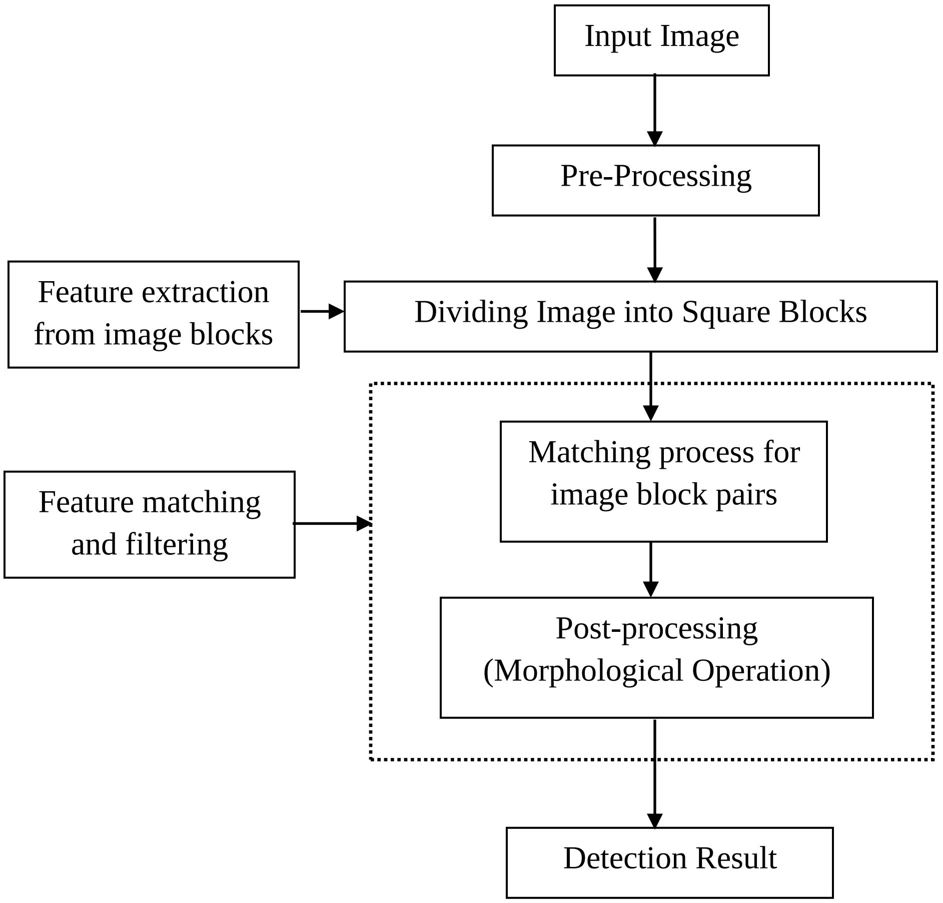

Input Image
Pre-Processing
Feature extraction from image blocks
Dividing Image into Square Blocks
Matching process for image block pairs
Feature matching and filtering
Post-processing (Morphological Operation)
Detection Result

Figure 3.1: Proposed Architecture

As shown in figure 3.1, the architecture is designed for the image copy-move forgery detection. In the proposed architecture, the input image will be pre-processed for the forgery detection. The GLCM algorithm is applied which extract textural features of the image and output of the GLCM algorithm to define the size of blocks size dynamically. The features or keypointsare further sorted out with the help of PCA.The forged areas are marked with the help of extracted features. At last, morphological operation will be applied which mark forgery part on the image. Morphological opening and closing operations are applied at a scale defined by the size of the structural element to represents the final detection result of the algorithm.

Chapter 4

Result and Discussion

In this research, the MATLAB software is employed to solve the complex mathematical problem. This tool uses C programming language. This software includes manifold built-in toolboxes. These toolboxes can easily perform many functions. Algorithm implementation, graph plotting and the designing of many user interfaces are some of the task, performed by this software. The network simulation is possible using this tool as it contains high graphics. This tool generates MATRIXs for the processing of components. And for calculating the result parameters, like Precision, Recall and F1 Score, the fitcknn() and fitctree() functions of MATLAB are used for better results.

Data set used: This research work uses CoMoFoD dataset for computation purpose. This dataset comprises1200 forged and processed images.

RGB Images

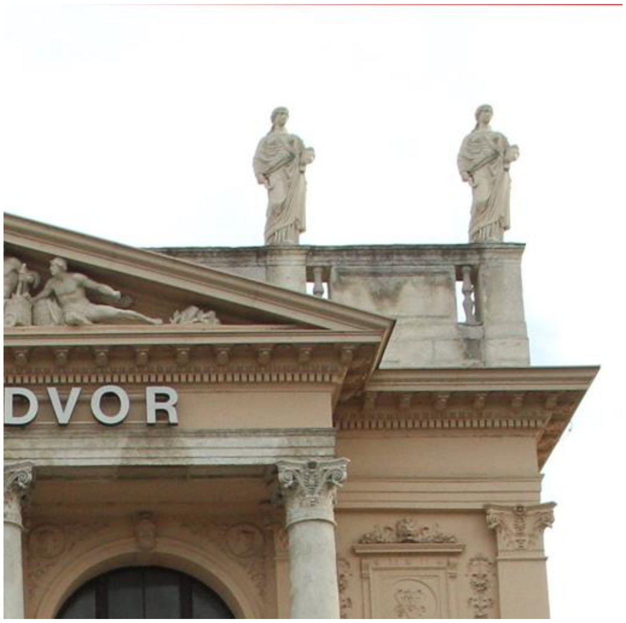


Figure 4.1: Input image

Figure 4.1, represents a cut-copy image as an input image.Theinput image is a colored (RGB) image. Then, the transformation of input image is converted into the gray scale image so that the more image processing operations can be applied on this image.

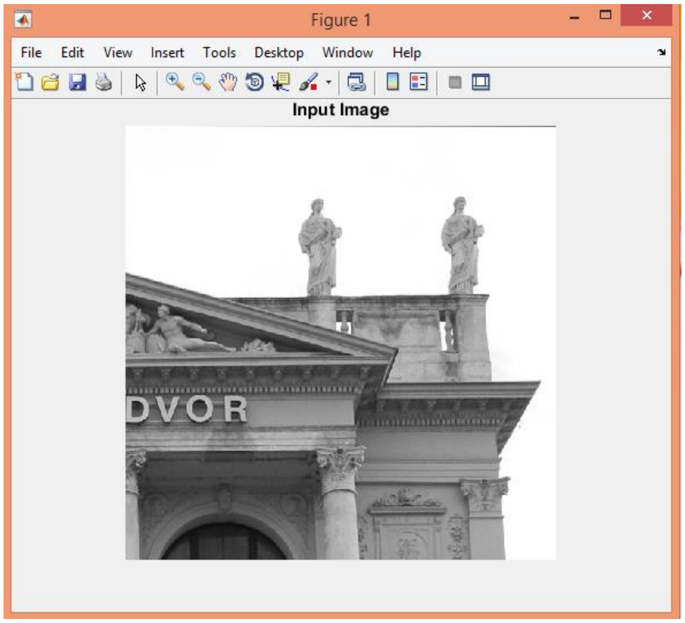


Figure 4.2: Grayscale image

Figure 4.2 shows the input image after processing. This is a grayscale image.

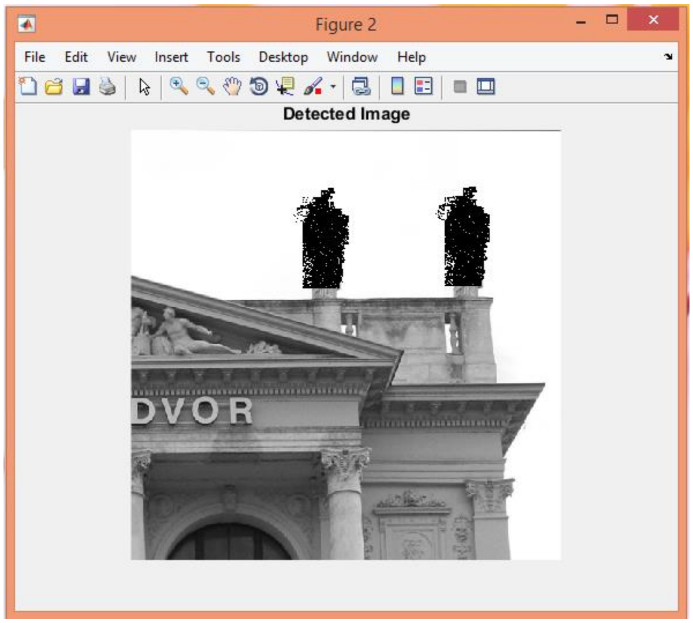


Figure 4.3: Output image with detected forged areas

Figure 4.3 demonstrates an image with detected forged areas. In this image, the marking of mismatchedimagecomponentsis carried out with the black color.

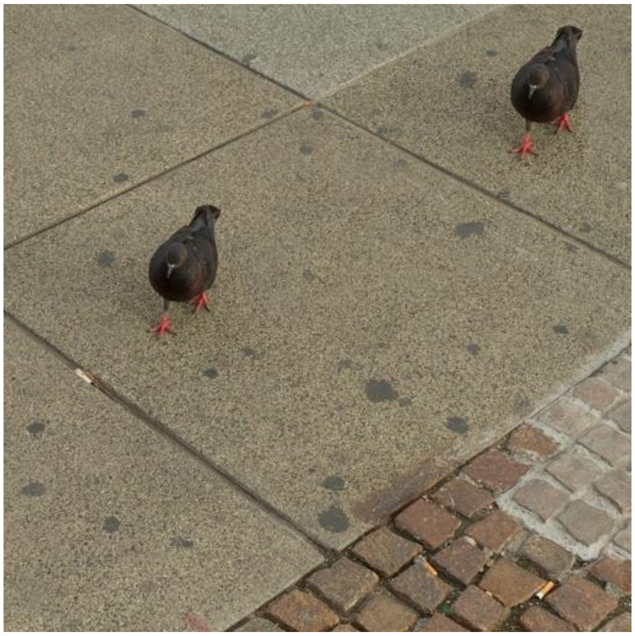


Figure4.4: Input image

Figure 4.4, represents a cut-copy image as an input image. The input image is a colored (RGB) image which will be converted to gray scale image,so that the more image processing operations can be applied on this image.

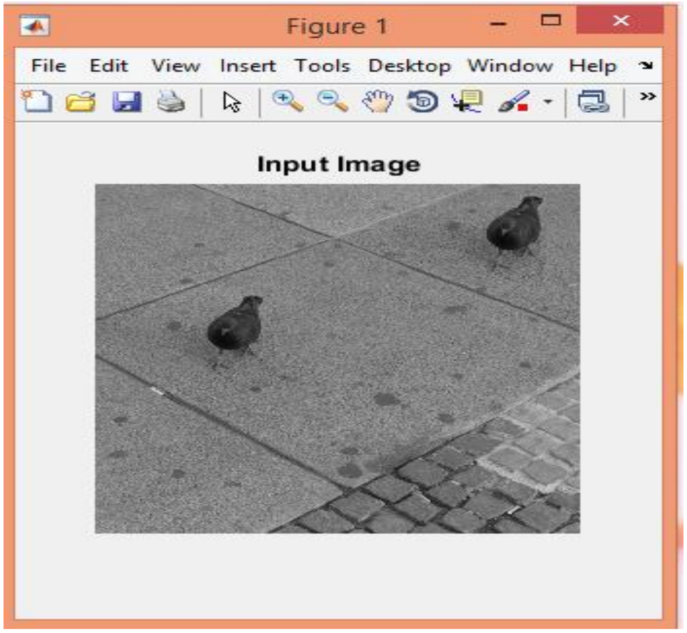


Figure 4.5: Grayscale image

Figure 4.5 shows the input image after processing. This is a grayscale image.

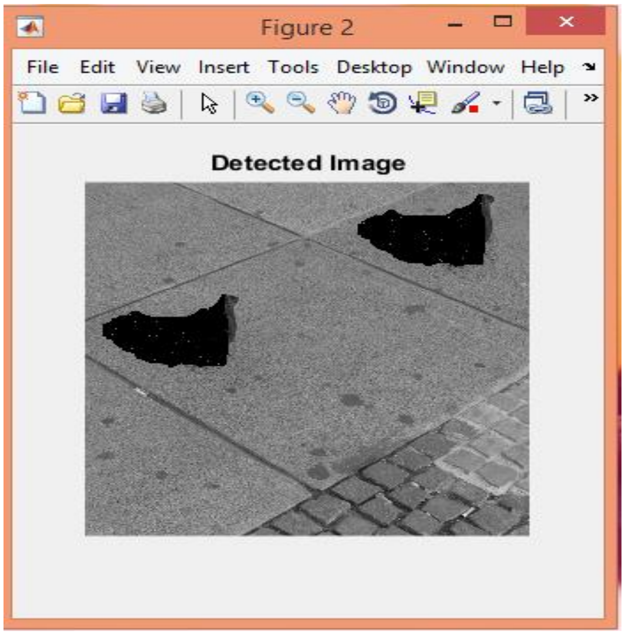


Figure 4.6: Output image with detected forged areas

Figure 4.6 demonstrates an image in which forged areas are detected using proposed algorithm. In this image, the mismatched image will be marked with the black color.

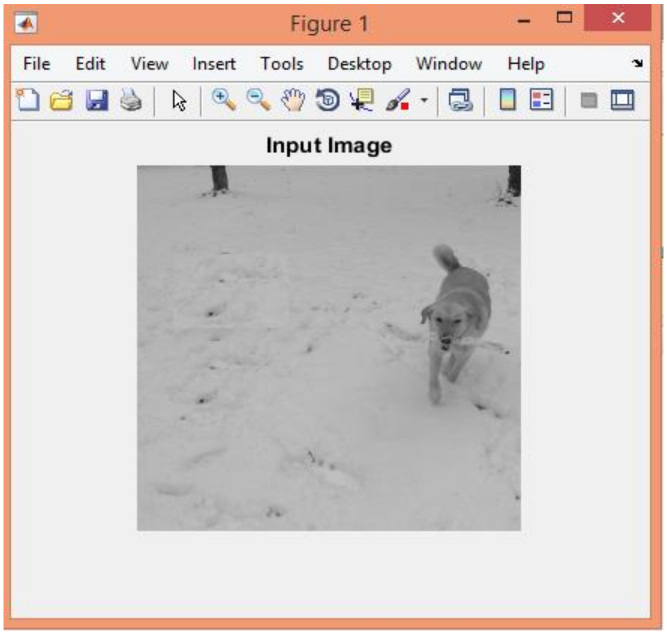


Figure 4.7: Input Image

Figure 4.7 represents a cut-copy image as an input image. Here, the proposed algorithm is applied to detect the tampered image area.

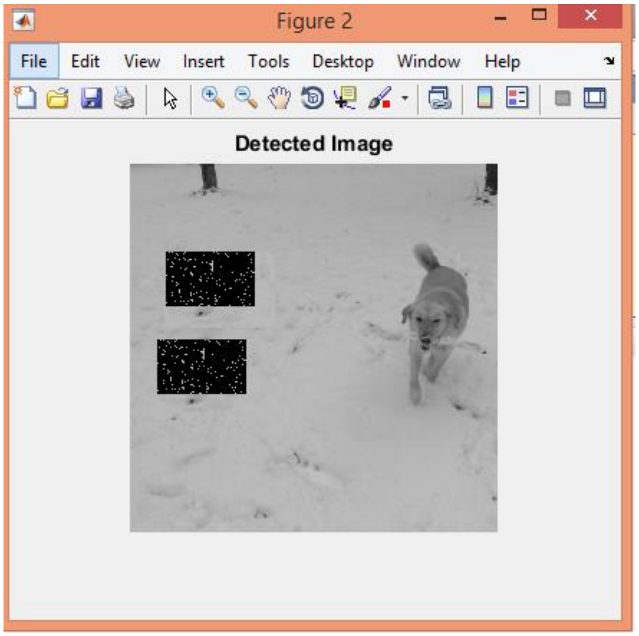


Figure 4.8Output image with detected forged areas

Figure 4.8 represents the detected regions by marking them with black color.

Table 1: Image Level and Pixel Level Analysis of Existing Method [26]

Level	Precision	Recall	F-Measure
Image Level	0.92	0.93	62.90
Pixel Level	0.92	0.92	72.58

Table 2: Image Level and Pixel Level Analysis of Proposed Method

Level	Precision	Recall	F-Measure
Image Level	0.98	0.98	93.54
Pixel Level	0.98	0.98	95.16

Table 3: Quantitative analysis on brightness changes over images.

Parameters	Existing Technique	Proposed Techniques
Precision	0.92	0.98
Recall	0.92	0.98
F1Measure	72.58	91.93

Table 4: Quantitative analysis on contrast adjusted over images.

Parameters	Existing Technique [26]	Proposed Technique
Precision	0.92	0.98
Recall	0.92	0.98
F1Measure	69.35	95.16

Table 5: Quantitative analysis on color changesover images.

Parameters	Existing Technique [26]	Proposed Technique
Precision	0.92	0.98
Recall	0.92	0.98

F1Measure	70.96	93.54

Conclusion

The copy-move forgery detection is the technique which is applied to detect forgery portion from the image. The various schemes are already proposed for the cop-move forgery detection which is broadly classified into block based and key point based techniques. This research based on the copy-move forgery detection using block based technique. In the proposed technique, the GLCM algorithm is used for the textual feature analysis and mean value of the features will be given as input to the PCA algorithm for the feature reduction. In the last pixel values are compared with the Euclidean distance to find the forgery pixels from the image. The proposed model is implemented in MATLAB and results are analyzed in terms of precision, recall and F-measure. The proposed model performed well in terms of all three parameters as compared to existing model.

References

[1] X. Kang, and S. Wei, “Identifying tampered regions using singular value decomposition in digital image forensics”, 2008, in International Conference on Computer Science and Software Engineering, volume 3, issue 10, pp. 92630.

[2] H. Huang, W. Guo, and Y. Zhang, “Detection of copy-move forgery in digital images using SIFT algorithm,” 2008, in Pacific-Asia Workshop on Computational Intelligence and Industrial Application, volume 2, issue 15, pp. 2726.

[3] G. H. Li, Q. Wu, D. Tu, and S. J. Sun, “A sorted neighborhood approach for detecting duplicated regions in image forgeries based on DWTand SVD,” 2007, in Proceedings of IEEE International Conference on Multimedia and Expo, Beijing, volume 23, issue 15, pp. 17503.

[4] M. Ghorbani, M. Firouzmand, and A. Faraahi, “DWT-DCT (QCD) based copy-move image forgery detection,” 2011, in 18th IEEE International Conference on Systems, Signals and Image Processing (IWSSIP), volume 12, issue 4, pp. 14.

[5] I. Amerini et al., “A SIFT-based forensic method for copymove attack detection and transformation recovery”, 2011, IEEE Trans. Inf. Foren. Sec., volume 6, issue 3, pp. 1099111

[6] J. Fridrich, D. Soukal, and J. Lukas, “Detection of copy move forgery in digital images,” 2003, in Proceedings of the Digital Forensic Research Workshop, volume 17, issue 3, pp. 58.

[7] A. C. Popescu, and H. Farid, “Exposing digital forgeries by detecting duplicated image regions,” 2004, Dept. Comput. Sci., Dartmouth College, Tech. Rep. TR2004-515, volume 5, issue 2, pp.34-40

[8] Parulsharma, Harpreet Kaur, “Copy-Move Forgery Detection with GLCM and Euclidian Distance Technique in Image Processing”, 2019, International Journal of Recent Technology and Engineering (IJRTE), volume-8, issue- 1C2, pp. 43-47

[9] M. AlSawadi, G. Muhammad, M. Hussain and G. Bebis, “Copy-Move Image Forgery Detection Using Local Binary Pattern and Neighborhood Clustering”,2013, Modelling Symposium (EMS), volume 5. issue 13, pp. 249-254

[10] H. Yao, T. Qiao, Z. Tang, Y. Zhao and H. Mao, “Detecting CopyMove Forgery Using Non-Negative Matrix Factorization,” 2011, Third International Conference on Multimedia Information Networking and Security, volume 8, issue 18, pp. 591-594.

[11] Yanjun Cao, T. Gao, and Qunting Yang, “A robust detection algorithm for copy-move forgery in digital images”, 2012, Forensic Int., volume 214, issue 7, pp. 33-43

[12] Salam A.Thajeel, Ghazali Sulong, “A Survey of Copy-Move Forgery Detection Techniques”, 2014, Journal of Theoretical and Applied Information Technology, volume 70 issue 1, pp. 25-35

[13] Saba Mushtaq and Ajaz Hussain Mir, “Image Copy Move Forgery Detection: A Review”, 2018, International Journal of Future Generation Communication and Networking, volume 11, issue 2, pp.11-22

[14] Chengyou Wang, Zhi Zhang and Xiao Zhou, “An Image Copy-Move Forgery Detection Scheme Based on A-KAZE and SURF Features”, 2018, Symmetry, volume10, issue 706, pp. 1-20

[15] Younis E. Abdalla1, M. Tariq Iqbal and M. Shehata, “Copy-Move Forgery Detection Based on Enhanced Patch Match”, 2017, International Journal of Computer Science, volume 14, issue 6, pp. 1-7

[16] Haipeng Chen, Xiwen Yang, YingdaLyu, “Copy-Move Forgery Detection Based on Keypoint Clustering and Similar Neighborhood Search Algorithm”, 2020, IEEE Access, vol. 8, issue 12, pp 45-50

[17] Kunj Bihari Meena, Vipin Tyagi, “A copy-move image forgery detection technique based on tetrolet transform”, Journal of Information Security and Applications, volume 52, issue 34, June 2020, article 102481

[18] Jun-Liu Zhong, Chi-Man Pun, “Two-pass hashing feature representation and searching method for copy-move forgery detection”, Information Sciences, volume 512, issue 15, February 2020, pages 675-692

[19] Gul Muzaffer, GuzinUlutas, “A new deep learning-based method to detection of copy-move forgery in digital images”, 2019, Scientific Meeting on Electrical-Electronics & Biomedical Engineering and Computer Science (EBBT), volume 6, issue 23, pp. 50-65

[20] Nidhi Anna Kurien, S Danya, Diya Ninan, C Heera Raju, Jisa David, “Accurate And Efficient Copy-Move Forgery Detection”, 2019, 9th International Conference on Advances in Computing and Communication (ICACC), volume 4, issue 14, pp 345-355

[21] Chengyou Wang, Zhi Zhang, Qianwen Li, Xiao Zhou, " An Image Copy-Move Forgery Detection Method Based on SURF and PCET”, 2019, IEEE Access, volume 7, issue 12, pp. 170032 - 170047

[22] Aya Hegazi, Ahmed Taha, Mazen M. Selim, “An improved copy-move forgery detection based on density-based clustering and guaranteed outlier removal”, Journal of King Saud University - Computer and Information Sciences, In press, corrected proof Available online 24 July 2019, volume 34, issue 19, pp 65-73

[23] Badal Soni, Pradip K. Das, Dalton Meitei Thounaojam, "Geometric transformation invariant block-based copy-move forgery detection using fast and efficient hybrid local features", Journal of Information Security and Applications, volume 45, issue 18, April 2019, Pages 44-51

[24] Priya Mariam Raju, Madhu S. Nair, "Copy-move forgery detection using binary discriminant features", 2018, Journal of King Saud University – Computer and Information Sciences, volume 65, issue 13, pp 195–207

[25] Yong Yew Yeap, U. U. Sheikh, Ab Al-Hadi Ab Rahman, "Image Forensic for Digital Image Copy Move Forgery Detection", 2018 IEEE 14th International Colloquium on Signal Processing & its Applications (CSPA 2018), volume 35, issue 21, pp. 1-6

[26] Yue Wu, Wael Abd-Almageed, and Prem Natarajan, "Image Copy-Move Forgery Detection via an End-to-End Deep Neural Network", 2018 IEEE Winter Conference on Applications of Computer Vision, volume 53, issue 12, pp. 72-80

[27] Gül Muzaffer, Eda SenaErdöl, GüzinUlutaş, "A copy-move forgery detection approach based on local intensity order pattern and patch match", 2018, 26th Signal Processing and Communications Applications Conference (SIU), volume 67, issue 11, pp. 725-730

[28] Amanpreet Kaur, Savita Walia, Krishan Kumar, "Comparative Analysis of Different Keypoint Based Copy-Move Forgery Detection Methods", 2018 Eleventh International Conference on Contemporary Computing (IC3), volume 38, issue 15, pp. 234-240

[29] H.M. Shahriar Parvez, Hamid A. Jalab, Ala'a R. Al-Shamasneh, Somayeh Sadeghi, Diaa M. Uliyan, "Copy-move Image Forgery Detection Based on Gabor Descriptors and K-Means Clustering", 2018, International Conference on Smart Computing and Electronic Enterprise (ICSCEE), volume 52, issue 17, pp. 432-439

[30] Ali Mumcu, Ibrahim Savran, "Copy move forgery detection with using FAST key points and SIFT description vectors", 2018, 26th Signal Processing and Communications Applications Conference (SIU), volume 52, issue 17, pp. 432-439

[31] Yildiz Aydin, GülMuzaffer, GüzinUlutaş, “Detection of copy move forgery technique based on SIFT and SURF”, 2018, 26th Signal Processing and Communications Applications Conference (SIU), volume 45, issue 24, pp. 564-469

[32] Geetika Gupta, Akshay Girdhar, “A Robust Passive Method for Detection of Copy-Move Forgery in Images”, 2017, IEEE, volume 68, issue 32, pp. 674-679

[33] Dhanya R, R KalaiSelvi, “A State-of-the-Art Review on Copy Move Forgery Detection Techniques”, Proceedings of 2017 IEEE International Conference on Circuits and Systems (ICCS 2017), volume 56, issue 20, pp. 563-570

[34] HaniehShabanian, Farshad Mashhadi, “A New Approach for Detecting Copy-Move Forgery in Digital Images”, 2017, IEEE, volume 45, issue 21, pp.753-760

[35] Junlin Ouyang, Yizhi Liu, Miao Liao, “Copy-move forgery detection based on deep learning”, 2017, 10th International Congress on Image and Signal Processing, BioMedical Engineering and Informatics (CISP-BMEI), volume 18, issue 7, pp. 391-400

[36] Tarman, Hardeep Saini, “M-SIFT: A detection algorithm for copy move image forgery”, 2017, 4th International Conference on Signal Processing, Computing and Control (ISPCC), volume 28, issue 2, pp. 864-870

[37] Yuan Wang, Lihua Tian, Chen Li, “LBP-SVD Based Copy Move Forgery Detection Algorithm”, 2017, IEEE International Symposium on Multimedia (ISM), volume 50, issue 4, pp. 954-960

[38] K RemyaRevi, M Wilscy, “Scale invariant feature transform based copy-move forgery detection techniques on electronic images — A survey”, 2017, IEEE International Conference on Power, Control, Signals and Instrumentation Engineering (ICPCSI), volume 22, issue 8, pp. 563-569

[39] Sajjad Dadkhah, Mario Koppen, Somayeh Sadeghi, Kaori Yoshida, H. A. Jalab, Azizah Abdul Manaf, “An efficient ward-based copy-move forgery detection method for digital image

forensic", 2017, International Conference on Image and Vision Computing New Zealand (IVCNZ), volume 23, issue 10, pp. 863-869

[40] Mejren Mohammad Al-Hammadi, Sabu Emmanuel, "Improving SURF Based Copy-Move Forgery Detection Using Super Resolution", 2016, IEEE International Symposium on Multimedia (ISM), volume 18, issue 3, pp. 985-993

[41] Hajar Moradi-Gharghani, Mehdi Nasri, "A new block-based copy-move forgery detection method in digital images", 2016, International Conference on Communication and Signal Processing (ICCSP), volume 25, issue 8, pp. 285-291

[42] Ahmet Boz, Hasan Şakir Bilge, "Copy-move image forgery detection based on LBP and DCT", 2016, 24th Signal Processing and Communication Application Conference (SIU), volume 13, issue 26, pp. 435-442

[43] Shi Wenchang, Zhao Fei, Qin Bo, Liang Bin, "Improving image copy-move forgery detection with particle swarm optimization techniques", 2016, China Communications, volume 13, issue 1, pp.753-760

[44] Atefeh Shahroudnejad, Mohammad Rahmati, "Copy-move forgery detection in digital images using affine-SIFT", 2016, 2nd International Conference of Signal Processing and Intelligent Systems (ICSPIS), volume 21, issue 6, pp. 267- 273

[45] Xiuli Bi, Chi-Man Pun, Xiao-Chen Yuan, "Adaptive Polar Based Filtering Method for Image Copy-Move Forgery Detection", 2016, IEEE Trustcom/BigDataSE/ISPA, volume 45, issue 7, pp. 542-550

[46] Rahul Dixit, Ruchira Naskar, "DyWT based copy-move forgery detection with improved detection accuracy", 2016, 3rd International Conference on Signal Processing and Integrated Networks (SPIN), volume 34, issue 9, pp. 334-343

[47] Haoqing Luan, N.F. Law, "A novel dual-threshold SIFT-based copy-move forgery detection", 2016, Asia-Pacific Signal and Information Processing Association Annual Summit and Conference (APSIPA), volume 2, issue 5, pp. 544-552

[48] Guangcheng Cao, Ying Chen, Gaigai Zong, Ying Chen, “Detection of copy-move forgery in digital image using locality preserving projections”, 2015, 8th International Congress on Image and Signal Processing (CISP), volume 30, issue 19, pp. 837-844

[49] Neetu Yadav, Rupal Kapdi, “Copy move forgery detection using SIFT and GMM”, 2015, 5th Nirma University International Conference on Engineering (NUiCONE), volume 28, issue 14, pp. 364-370

[50] Surbhi Sharma, Umesh Ghanekar, “A Rotationally Invariant Texture Descriptor to Detect Copy Move Forgery in Medical Images”, 2015, IEEE International Conference on Computational Intelligence & Communication Technology, volume 65, issue 39, pp. 877-883

[51] Davide Cozzolino, Giovanni Poggi, Luisa Verdoliva, “Efficient Dense-Field Copy–Move Forgery Detection”, 2015, IEEE Transactions on Information Forensics and Security, volume 10, issue 11, pp. 435-438

[52] Salih Türk, Özkan Bingöl, Güzin Ulutaş, “Detection of copy-move forgery using DoGCode”, 2015, 23nd Signal Processing and Communications Applications Conference (SIU), volume 29, issue 4, pp. 556-563

[53] Elham Mohebbian, Mahdi Hariri, “Increase the efficiency of DCT method for detection of copy-move forgery in complex and smooth images”, 2015, 2nd International Conference on Knowledge-Based Engineering and Innovation (KBEI), volume 20, issue 8, pp. 452-460

[54] EdoardoArdizzone, Alessandro Bruno, Giuseppe Mazzola, “Copy–Move Forgery Detection by Matching Triangles of Keypoints”, 2015, IEEE Transactions on Information Forensics and Security, volume 10, issue 10, pp. 975-982

[55] DijanaTralic, Sonja Grgic, Branka Zovko-Cihlar, “Video frame copy-move forgery detection based on Cellular Automata and Local Binary Patterns”, 2014, X International Symposium on Telecommunications (BIHTEL), volume 16, issue 7, pp. 256-262

[56] TakwaChihaoui, Sami Bourouis, Kamel Hamrouni, “Copy-move image forgery detection based on SIFT descriptors and SVD-matching”, 2014, 1st International Conference on Advanced Technologies for Signal and Image Processing (ATSIP), volume 49, issue 23, pp. 765-772

[57] Le Zhong, Weihong Xu, “A robust image copy-move forgery detection based on mixed moments”, 2013, IEEE 4th International Conference on Software Engineering and Service Science, volume 32, issue 6, pp. 864-871

[58] Sunil Kumar, Jagannath Desai, Shaktidev Mukherjee, “A fast DCT based method for copy move forgery detection”, 2013, IEEE Second International Conference on Image Information Processing (ICIIP-2013), volume 12, issue 5, pp. 532-540

[59] Yanfen GAN, Jing CANG, “A Detection Algorithm for Image Copy-move Forgery Based on Improved Circular Projection Matching and PCA”, 2013, Sensors & Transducers, Vol. 159, Issue 11, pp. 19-25