# Image Forgery Detection

Sura Sreeja Reddy, Gayam Santhosh Reddy,
Pasupuleti Aashrithapriya, Arigela Rahulkumar and
Pathan Bilalkhan

March 27, 2024

# Image Forgery Detection

SURA SREEJA REDDY
B.TECH - CSE - AI
PARUL UNIVERSITY
VADODARA, INDIA
200303124597@paruluniversity.ac.in

GAYAM SANTHOSH REDDY
B.TECH - CSE -AI
PARUL UNIVERSITY
VADODARA, INDIA
210303124906@paruluniversity.ac.in

PASUPULETI AASRITHAPRIYA
B.TECH - CSE - AI
PARUL UNIVERSITY
VADODARA, INDIA
2203031249005@paruluniversity.ac.in

ARIGELA RAHULKUMAR
B.TECH -CSE - AI
PARUL UNIVERSITY
VADODARA, INDIA
210303124711@paruluniversity.ac.in

PATHAN BILAL KHAN

Asst.Professor

PIET-CSE-Dept

***Abstract*—— Digital image forgery constitutes the deceptive manipulation of digital images to obscure or alter significant data within the image, often making it arduous to discern the manipulated regions from the original content. Preserving the integrity and authenticity of images necessitates the detection of such forgeries. The contemporary lifestyle, coupled with advancements in photography technology, has facilitated the ease of digital image manipulation through readily available image editing software. Consequently, the imperative to detect and mitigate image forgery operations has become paramount.**

**Detection of image forgery encompasses various techniques, including but not limited to identifying object removal, object addition, and anomalous size alterations within the image. Images serve as potent means of communication, underscoring the critical importance of ensuring their veracity. In this project, a comprehensive approach is adopted, employing sophisticated algorithms such as Copy-Move Detection, Canny Edge Detection, Structure Similarity Index, Hierarchical Agglomerative Clustering, and Neural Network algorithms. These methodologies are leveraged to enhance accuracy in the detection and mitigation of digital image forgeries, thereby safeguarding**

**the integrity of visual content in the digital realm.**

***Keywords— Image Forgery, Detection,Deep Image Forgery.***

## I. INTRODUCTION

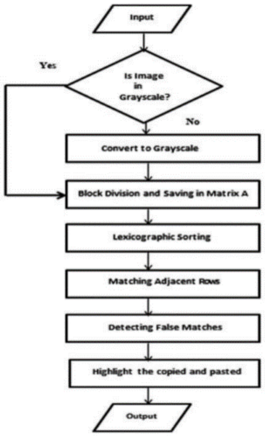
Forgery constitutes the illicit manipulation of images or documents without proper authorization, often motivated by various illicit purposes such as falsifying evidence or illicit financial gain. Visual representations convey concepts more effectively than verbal expressions, and with the advent of digital technology, image processing tools like Adobe Photoshop, GIMP, and Corel Paint Shop have proliferated, posing a significant threat to the integrity of digital imagery.

Image manipulations typically fall into two categories: allowed manipulations and malignant manipulations. Allowed manipulations, also known as incidental manipulations, entail alterations that do not compromise the semantic integrity of the information and are generally acceptable within authentication systems. These alterations are typically minor and subtle, encompassing tasks such as color correction, brightness and contrast adjustments, cropping for layout fitting, and removal of imperfections such as dust, dirt, or scratches. Such edits are permissible as long as they are transparently disclosed or visually indicated, often through delineating different image regions.

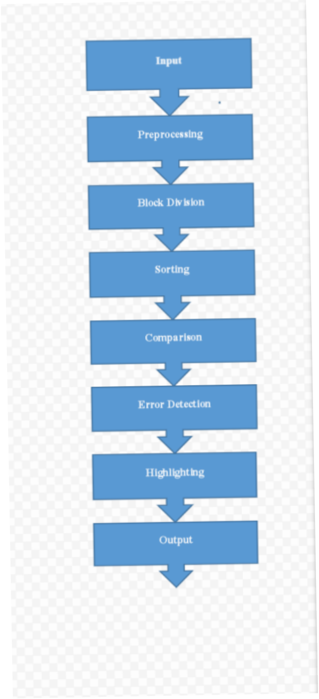
Watermarking serves as a method to imbue digital images with authenticity by embedding an indivisible watermark. In contrast, passive methods, also known as non-intrusive or blind methods, do not require prior information to be included in the digital image. Various attacks can compromise the integrity of digital images, including but not limited to resizing, noise addition, blurring, rotation, scaling, compression, image splicing, and copy-move operations. Understanding and addressing these vulnerabilities are crucial in safeguarding the authenticity and reliability of digital imagery.

## II. DESIGN

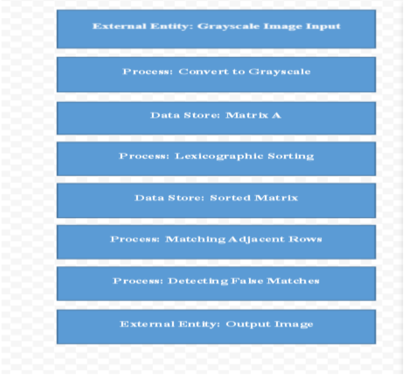
### A. *Project workflow*



### B. *PROJect stages*



### C. *Data flow diagram*


External Entity: Grayscale Image Input
Process: Convert to Grayscale
Data Store: Matrix A
Process: Lexicographic Sorting
Data Store: Sorted Matrix
Process: Matching Adjacent Rows
Process: Detecting False Matches
External Entity: Output Image

## III. IMPLEMENTATION

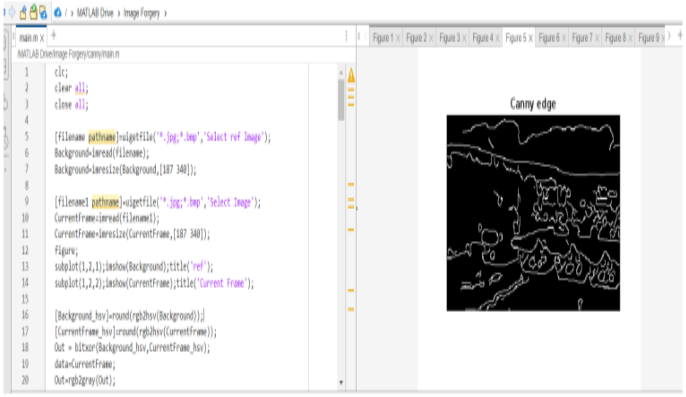
MATLAB stands out as a robust and interactive tool for image analysis and processing, offering a comprehensive suite of operational and enhancement capabilities. Its versatility and widespread applicability make it a preferred choice in various domains. Providing a user-friendly platform, MATLAB enables seamless implementation of algorithms tailored to specific operations. With an array of tools at disposal, MATLAB empowers users to effortlessly enhance images according to their requirements. It finds utility across diverse applications, showcasing its adaptability and effectiveness in addressing image processing challenges. In essence, MATLAB serves as a pivotal tool in both research and practical contexts, facilitating advancements in image analysis and manipulation with unparalleled efficiency and precision.

### A. *tools and technology*

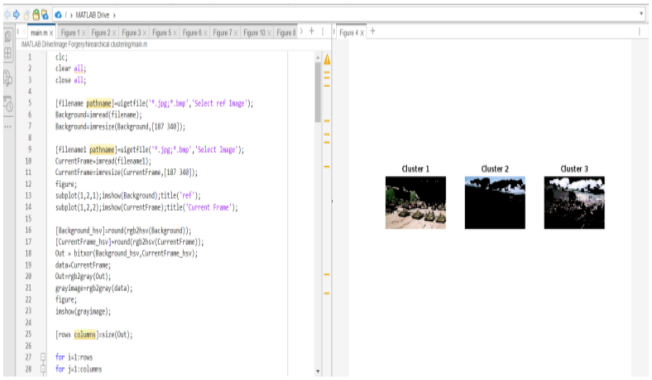
- **Image Acquisition:**
  - Obtain digital images from various sources such as cameras, scanners, or databases.
- **Image Pre-processing:**
  - Enhance image quality by applying operations such as noise reduction, contrast adjustment, and image resizing.
- **Image Segmentation:**
  - Divide the image into meaningful regions or segments to simplify analysis.
- **Feature Extraction:**
  - Identify and extract relevant features from segmented regions, such as edges, textures, or shapes.
- **Matching:**
  - Compare extracted features to determine similarities or correspondences between images.
- **Filtering:**
  - Apply filters to enhance or suppress certain image characteristics, often used for noise reduction or feature enhancement.

- **Post-processing:**
  - ○ Perform additional operations to refine results, such as image fusion, morphological operations, or color correction.
- **Key Point Based Method:**
  - ○ Utilize key points or interest points in the image to represent distinct features, enabling robust matching and recognition.
- **Classification:**
  - ○ Assign images or image regions to predefined categories or classes based on extracted features and patterns.

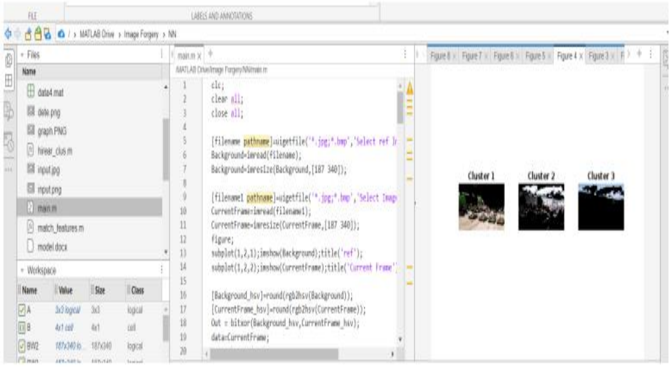
### B. *implemented work*



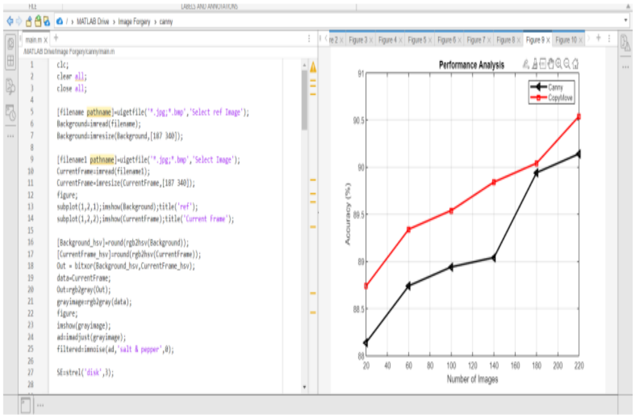
```
clc;
clear all;
close all;

[filename pathname]=uigetfile('*.jpg;*.bmp','Select ref Image');
Background=imread(filename);
Background=imresize(Background,[187 340]);

[filename1 pathname]=uigetfile('*.jpg;*.bmp','Select Image');
CurrentFrame=imread(filename1);
CurrentFrame=imresize(CurrentFrame,[187 340]);
figure;
subplot(1,2,1);imshow(Background);title('ref');
subplot(1,2,2);imshow(CurrentFrame);title('Current Frame');

[Background_hsv]=round(rgb2hsv(Background));
[CurrentFrame_hsv]=round(rgb2hsv(CurrentFrame));
Out = bitxor(Background_hsv,CurrentFrame_hsv);
data=CurrentFrame;
Out=rgb2gray(Out);
```



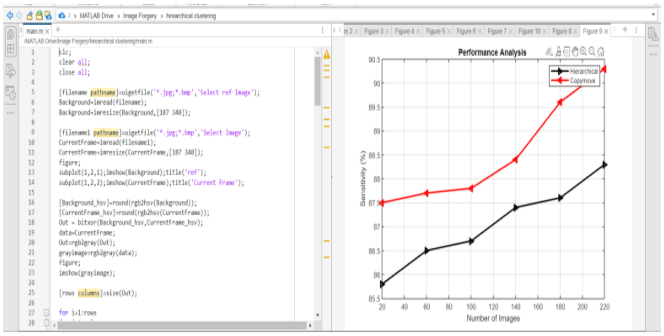
```
clc;
clear all;
close all;

[filename pathname]=uigetfile('*.jpg;*.bmp','Select ref Image');
Background=imread(filename);
Background=imresize(Background,[187 340]);

[filename1 pathname]=uigetfile('*.jpg;*.bmp','Select Image');
CurrentFrame=imread(filename1);
CurrentFrame=imresize(CurrentFrame,[187 340]);
figure;
subplot(1,2,1);imshow(Background);title('ref');
subplot(1,2,2);imshow(CurrentFrame);title('Current Frame');

[Background_hsv]=round(rgb2hsv(Background));
[CurrentFrame_hsv]=round(rgb2hsv(CurrentFrame));
Out = bitxor(Background_hsv,CurrentFrame_hsv);
data=CurrentFrame;
Out=rgb2gray(Out);
grayimage=rgb2gray(data);
figure;
imshow(grayimage);

[rows columns]=size(Out);

for i=1:rows
for j=1:columns
```



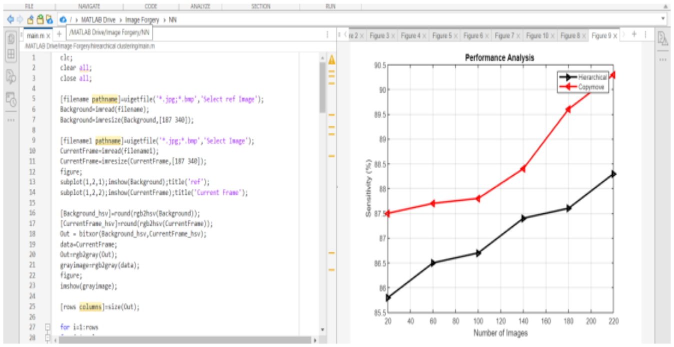
```
clc;
clear all;
close all;

[filename pathname]=uigetfile('*.jpg;*.bmp','Select ref Ir
Background=imread(filename);
Background=imresize(Background,[187 340]);

[filename1 pathname]=uigetfile('*.jpg;*.bmp','Select Imag
CurrentFrame=imread(filename1);
CurrentFrame=imresize(CurrentFrame,[187 340]);
figure;
subplot(1,2,1);imshow(Background);title('ref');
subplot(1,2,2);imshow(CurrentFrame);title('Current Frame'

[Background_hsv]=round(rgb2hsv(Background));
[CurrentFrame_hsv]=round(rgb2hsv(CurrentFrame));
Out = bitxor(Background_hsv,CurrentFrame_hsv);
data=CurrentFrame;
```



```
clc;
clear all;
close all;

[filename pathname]=uigetfile('*.jpg;*.bmp','Select ref Image');
Background=imread(filename);
Background=imresize(Background,[187 340]);

[filename1 pathname]=uigetfile('*.jpg;*.bmp','Select Image');
CurrentFrame=imread(filename1);
CurrentFrame=imresize(CurrentFrame,[187 340]);
figure;
subplot(1,2,1);imshow(Background);title('ref');
subplot(1,2,2);imshow(CurrentFrame);title('Current Frame');

[Background_hsv]=round(rgb2hsv(Background));
[CurrentFrame_hsv]=round(rgb2hsv(CurrentFrame));
Out = bitxor(Background_hsv,CurrentFrame_hsv);
data=CurrentFrame;
Out=rgb2gray(Out);
grayimage=rgb2gray(data);
figure;
imshow(grayimage);
ad=imadjust(grayimage);
filtered=imnoise(ad,'salt & pepper',0);

SE=strel('disk',3);
```



```
clc;
clear all;
close all;

[filename pathname]=uigetfile('*.jpg;*.bmp','Select ref Image');
Background=imread(filename);
Background=imresize(Background,[187 340]);

[filename1 pathname]=uigetfile('*.jpg;*.bmp','Select Image');
CurrentFrame=imread(filename1);
CurrentFrame=imresize(CurrentFrame,[187 340]);
figure;
subplot(1,2,1);imshow(Background);title('ref');
subplot(1,2,2);imshow(CurrentFrame);title('Current Frame');

[Background_hsv]=round(rgb2hsv(Background));
[CurrentFrame_hsv]=round(rgb2hsv(CurrentFrame));
Out = bitxor(Background_hsv,CurrentFrame_hsv);
data=CurrentFrame;
Out=rgb2gray(Out);
grayimage=rgb2gray(data);
figure;
imshow(grayimage);

[rows columns]=size(Out);

for i=1:rows
```



```
clc;
clear all;
close all;

[filename pathname]=uigetfile('*.jpg;*.bmp','Select ref Image');
Background=imread(filename);
Background=imresize(Background,[187 340]);

[filename1 pathname]=uigetfile('*.jpg;*.bmp','Select Image');
CurrentFrame=imread(filename1);
CurrentFrame=imresize(CurrentFrame,[187 340]);
figure;
subplot(1,2,1);imshow(Background);title('ref');
subplot(1,2,2);imshow(CurrentFrame);title('Current Frame');

[Background_hsv]=round(rgb2hsv(Background));
[CurrentFrame_hsv]=round(rgb2hsv(CurrentFrame));
Out = bitxor(Background_hsv,CurrentFrame_hsv);
data=CurrentFrame;
Out=rgb2gray(Out);
grayimage=rgb2gray(data);
figure;
imshow(grayimage);

[rows columns]=size(Out);

for i=1:rows
```

## IV. LITERATURE SURVEY

Yun et al. (2022) propose a novel method for detecting digital forgeries in images manipulated with Adobe Photoshop filters. Their approach utilizes image interpolation and the EM algorithm to compute interpolated coefficients, effectively identifying manipulated regions. This research significantly advances techniques for enhancing the authenticity and integrity of digital content, addressing critical needs across various domains.

[1] Authors: Yong-In Yun, Jung-Beom Lee, Da-un Jung, Dong-Hwan Har, Jong-Soo Choi Year of Publication: 2022

Charpe and Bhattacharya (2020) address the challenge of detecting image forgery, crucial in fields like medical imaging and journalism. Their method employs lexicographic sorting and Phase Correlation to detect duplicated blocks, aiding in the identification of tampering. Techniques for detecting contrast enhancement and copy-paste forgery are presented, showcasing robustness against JPEG compression. This research significantly contributes to image forensics, offering practical tools for verifying the authenticity of digital images in critical applications.

[2] Author: Jayshri Charpe; Antara Bhattacharya Year of Publication: 2020.

Parvez et al. (2022) address the increasing issue of image forgery by proposing an efficient technique for detecting region-duplication forgery. Their method utilizes image segmentation with normalized cut, Gabor descriptors, and K-Means clustering to identify duplicated regions. Experimental results demonstrate the robustness of the approach against various post-processing attacks such as rotation, scaling, blurring, and JPEG compression. This research contributes significantly to the field of image forensics, offering a practical solution to validate the integrity of digital images in the face of sophisticated manipulation techniques.

[3] Author: H.M. Shahriar Parvez; Hamid A. Jalab; Ala'a R. AlShamasneh; Somayeh Sadeghi; Diaa M. Uliyan Year of Publication: 2022.

Khan and Kulkarni (2020) propose a blind image forensics approach for detecting copy-move forgery, a prevalent type of image manipulation. The method utilizes Discrete Wavelet Transform (DWT) to reduce image dimensionality. Employing lexicographic sorting and Phase Correlation, duplicated blocks are identified, significantly reducing detection time. The technique demonstrates resilience against post-processing attacks, highlighting its potential for practical application in ensuring the authenticity and integrity of digital images, crucial in today's technologically driven world.

[4] Author: Saiqa Khan; Arun Kulkarni Year of Publication: 2020.

Mookdarsanit et al. (2021) propose a novel method for detecting image forgery using XOR comparisons and determinant calculations for improved performance compared to pixel-by-pixel comparison. Their approach leverages lexicographic sorting and Phase Correlation for identifying duplicated blocks, reducing detection time significantly. Experimental results demonstrate a notable speed improvement, emphasizing the method's potential for enhancing image forensics applications, particularly in case investigations and image validity assessments where timely and accurate detection of forgery is crucial.

[5] Author: Pakpoom Mookdarsanit; Lawankorn Soimart; Mahasak Ketcham Year of Publication: 2021.

Zeng et al. (2020) propose a novel method for detecting blurred image splicing through blind image restoration. Their approach utilizes blur parameters estimation based on spectrum characteristics to restore spliced regions and the rest of the image. By employing lexicographic sorting and Phase Correlation, duplicated blocks are identified, significantly reducing detection time. Additionally, a new measure is developed to assist in inconsistent region segmentation in restored images, even under noise or low-quality compression. This research contributes to the advancement of forgery detection techniques, particularly in identifying image splicing, crucial for ensuring the integrity of digital content.

[6] Author: Feng Zeng; Wei Wang; Min Tang; Zhanghua Cao Year of Publication: 2020.

Murali et al. (2021) propose a method for detecting copy-create image forgeries by analyzing luminance levels. They utilize discrepancies in perceived brightness to identify areas in forged images that may have been copied and pasted. Through lexicographic sorting and Phase Correlation, duplicated blocks are identified, reducing detection time significantly. The approach contributes to the field of image forensics by offering a technique that considers variations in lighting conditions and reduces the time required for forgery detection. This research emphasizes the importance of scrutinizing luminance levels to authenticate digital images, particularly in cases involving manipulation with image processing software.

[7] Author: S. Murali; Basavaraj S. Anami; Govindraj B. Chittapur Year of Publication: 2021.

Su and Kaizhen (2021) propose a robust method for detecting copy forgery in digital images using LPP-SIFT (Locality Preserving Projection- Scale Invariant Feature Transform) features. The algorithm combines SIFT key point extraction with LPP to obtain low-dimensional feature descriptors, followed by key point matching. By utilizing lexicographic sorting and Phase Correlation, duplicated blocks are identified, significantly reducing detection time. The approach efficiently detects copy operations and other post-processing forgeries like rotation and scaling. Experimental results validate the efficacy of the method, making it a valuable contribution to the field of image forensics.

[8] Author: Baina Su; Zhu Kaizhen Year of Publication: 2021.

Bhartiya and Jalal (2022) propose an innovative method for detecting image forgery in JPEG images by leveraging JPEG compression properties. The method utilizes feature-based clustering to classify image blocks as forged or non-forged, exploiting traces of re-compression to detect manipulation. Through lexicographic sorting and Phase Correlation, duplicated blocks are identified, significantly reducing detection time. The approach produces better results compared to probability-based techniques, contributing to the advancement of image forensics methods and ensuring the integrity of digital images in various applications.

[9] Author: Gunjan Bhartiya; Anand Singh Jalal Year of Publication: 2022.

Zhang et al. (2022) present a survey on passive-blind image forgery detection methods, acknowledging the increasing use of digital photography and the availability of low-cost image editing software. Their paper focuses on detecting common forgery methods such as copy-move, blur, and re-sample forgery. Through lexicographic sorting and Phase Correlation, duplicated blocks are identified, reducing detection time significantly. The survey emphasizes the importance of continually advancing image forensics techniques to ensure the authenticity of digital images in an environment where image manipulation tools are readily accessible and frequently utilized.

[10] Author: Zhen Zhang; Yuan Ren; Xi-Jian Ping; Zhi-Yong He; Shan-Zhong Zhang Year of Publication: 2022.

The proposed methodology for detecting image forgery harnesses feature point extraction and morphological operations, demonstrating commendable performance across diverse challenges like geometric transformations and JPEG compression. This system furnishes precise outcomes in identifying copy-move forgeries sans reliance on pre-existing datasets, underscoring its autonomy and effectiveness in forensic analysis.

## Conclusion

The strategic fusion of feature point extraction and morphological operations marks a pivotal advancement in digital forensics, endowing the algorithm with the capacity to discern intricate image characteristics resiliently amidst varied manipulations. Whether subjected to geometric alterations or compressed via JPEG, the system upholds its resilience, ensuring steadfast reliability even in the face of adversities. Its independent performance, devoid of reliance on pre-established datasets, epitomizes versatility and utility in forensic endeavors.

In the realm of image forgery detection, this system emerges as a beacon of promise, offering robust solutions to enduring challenges. Its unwavering resilience to transformations and compression not only bolsters its trustworthiness but and the broadens its applicability across practical scenarios. By furnishing accurate identifications of copy-move forgeries, it equips law enforcement, media professionals, and forensic the specialists with a formidable instrument to uncover fraudulent manipulations. Furthermore, its independence from predefined datasets signifies adaptability across diverse investigative landscapes, underlining its significance in digital image forensics and the pursuit of authenticity in the digital milieu.

Additionally, our commitment to enhanced security, exemplified by Firebase Authentication and stringent encryption protocols, safeguards user data from unauthorized access, ensuring utmost confidentiality. Moreover, our dedication to incorporating user feedback underscores our continuous endeavor towards refinement and evolution to meet evolving user needs, cementing our commitment to excellence.

## Acknowledgment

I am deeply grateful to express my sincere appreciation to Mr. Pathan Bilalkhan R., Assistant Professor, for his unwavering support, invaluable guidance, and relentless encouragement throughout my endeavors. His expertise, mentorship, and unwavering commitment have been instrumental in navigating the challenges and achieving the goals of this project. Under his tutelage, complexities were simplified, and obstacles were overcome with ease.

I am truly privileged to have benefitted from Mr. Pathan Bilalkhan R.'s wisdom, prompt advice, and steadfast leadership, which have significantly contributed to the success of this endeavor. I am indebted to him for his invaluable contributions, and I am proud to have had the opportunity to work under his guidance.

Furthermore, I extend my gratitude to the Almighty for granting me the strength and perseverance to embark on this journey.

## References

1. A.C. Popscu, and H.Farid, “Statistical Tools for Digital Forensics” ,in Proc.The 6th international workshop on information hiding ,Toronto, Canada 2019.

2. Shivani Thakur, RamanpreetKaur, Dr. Raman Chadha,JasmeetKaur, “A Review Paper on Image Forgery Detection In Image Processing”, IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278- 0661,p-ISSN: 2278-8727, Volume 18, Issue 4,Ver. I (Jul.-Aug. 2019), PP 86-89.

3. DevanshiChauhan, DipaliKasat, SanjeevJain, VilasThakare, “Survery on KeyPoint based Copymove Forgery Detection Methods on Images”, science direct volume 85, 2019.

4. ]Ali Qureshi, M., and M. Deriche. “A review on copy move image forgery detection techniques.” IEEE, 2019.

5. ]Qazi, Tanzeela. “Survey on blind image forgery detection.”IET, 2019.

6. ]M. Qiao,Sung, Q. Liu and B. Ribeiro, ”A novel approach for detection of copy- move forgery,” Fifth International Conferenceon ADVCOMP (Advanced Engineering Computing and Applications Sciences, 2019.

7. ]Gajanan K. Birajdar, Vijay H. Mankar, “Digital image forgery detection using passive techniques: A survey,” Digital Investigation, vol. 10, no.3, 2019, pp. 226-245.

8. ]GagandeepKaur, Manoj Kumar, “Study Of Various Copy Move Forgery Attack Detection In Digital Images”, International Journal Of Research In Computer Applications And Robotics, Vol.3 Issue 9, Pg.: 30-34 September 2019.

9. Rohini.A.Maind, AlkaKhade, D.K.Chitre, “Image Copy Move Forgery Detection Using Block Representing Method”, International Journal Of Soft Computing And Engineering (Ijsce) Issn: 2231- 2307,Volume-4, Issue-2, May 2019.

10. ]R.C. Gonzalez, R.E. Woods, “Digital Image Processing”, 2nd edition, Addison- Wesley, 2019.