

“Image Forgery Detection”

A PROJECT REPORT

Submitted in partial fulfillment for the award of the degree of
BACHELOR OF TECHNOLOGY

Submitted to



Dr. Babasaheb Ambedkar Technological University, Lonere.

Submitted By

- | | |
|-------------------------------|-----------------|
| 1) Muskan Firoj Sayyad | (2167571242035) |
| 2) Sangramsinh Mansing Shinde | (2167571242009) |
| 3) Salman Alamgir Pathan | (2167571242031) |
| 4) Shreyash Vaibhav Nikam | (2167571242037) |

Under the Guidance of

Dr. Vikram S. Patil



Computer Science and Engineering

YSPM's Yashoda Technical Campus

Faculty of Engineering

Wadhe, Satara-415011

2024- 25



Yashoda Shikshan Prasarak Mandal's
Yashoda Technical Campus

Approved by AICTE Delhi/ Govt. of Maharashtra/ Accredited by NAAC
NH-4, Wadhe, Satara 415011

Email : principalengg_ytc@yes.edu.in Call: 02162-271238/39 Mob. 9172220775



Faculty of Engineering

CERTIFICATE

This is to certify that the Project entitled “Image Forgery Detection“ submitted by Miss. Muskan Firoj Sayyad, Mr. Sangramsinh Mansing Shinde, Mr. Salman Alamgir Pathan, Mr. Shreyash Vaibhav Nikam is a record of the bonafide work carried out by them, under my guidance, and it is approved for the partial fulfillment of requirement of Dr. Babasaheb Ambedkar Technological University, Lonere for the award of the degree Bachelor of Technology (Computer Science and Engineering).

Dr. S. V. Balshetwar

HOD

**Computer Science
and Engineering**

Dr. Vikram S. Patil.

Guide &Principal

YSPM's YTC, Satara

(External Examiner)

Place:- Satara

Date:-

Declaration by Student(s)

This is to declare that this report has been written by us. No part of the report is plagiarized from other sources. All information included from other sources has been duly acknowledged. We aver that if any part of the report is found to be plagiarized, we shall take full responsibility for it.

Muskan Firoj Sayyad.
2167571242035

Sangramsinh Mansing Shinde.
2167571242009

Salman Alamgir Pathan.
2167571242031

Shreyash Vaibhav Nikam.
2167571242037

Place:-Satara

Date:-

CONTENTS

			Acknowledgement	i
			Abstract	ii
			List of Figures	iii
Chapter			Contents	Page No.
1			Introduction	1
2			Literature Survey	3
3			System Specification	6
4			Block Diagram	8
5			System Design	10
6			Software Development	14
7			Troubleshooting / Debugging	16
8			Conclusion	19
9			Future Scope	21
10			References	23

ACKNOWLEDGEMENT

This is to acknowledge and thank all the individuals who played defining role in shaping this mini project report. Without their constant support, guidance and assistance this project report would not have been completed alone.

We take this opportunity to express my sincere thanks to my guide **Dr. Vikram S. Patil**. For his guidance, support, encouragement and advice. We will forever remain grateful for the constant support and guidance extended by our Guide, in making this mega project work.

We wish to express my sincere thanks to, **Dr. S. V. Balshetwar** (Head, Department of Computer Science and Engineering at YSPM'S YTC, Satara. We would also like to express my deep gratitude to our Hon'ble **Dr. Vikram S. Patil** who provides good opportunities for all of us.

Last but not the least, We would like to thank all our Friends and Family members who have always been there to support and helped us to complete this mega project work in time.

- 1) Muskan Firoj Sayyad.
- 2) Sangramsinh Mansing Shinde.
- 3) Salman Alamgir Pathan.
- 4) Shreyash Vaibhav Nikam.

ABSTRACT

The increasing sophistication of digital forgery techniques presents significant challenges in maintaining the authenticity of visual content. This project, **Image Forgery Detection System**, addresses these challenges by identifying tampered regions in images through structural analysis. The system utilizes the **Structural Similarity Index Measure (SSIM)** to compare original and potentially forged images, detecting inconsistencies by analysing grayscale features. Preprocessing techniques such as resizing and normalization ensure uniformity across inputs. Differences are highlighted using thresholding and contour detection, providing a visual representation of tampered areas. The approach was tested on datasets containing both original and manipulated images, demonstrating accurate forgery detection. This project serves as a practical tool for digital forensics, content verification, and security, ensuring the integrity of visual data in an era of pervasive manipulation.

Keywords: Structural Similarity Index Measure (SSIM), Image manipulation, Tampered images, Digital forensics, Image comparison, Grayscale analysis, Security, Forgery identification, Visual data integrity, Image authentication.

LIST OF FIGURES

Sr. No.	Title	Page No.
1	Control Flow Diagram	09
2	Level 0 Data flow diagram	11
3	Level 1 Data flow diagram	12
4	Flow Diagram	13
5	UML Diagram	14

CHAPTER 1

INTRODUCTION

Chapter 1

Introduction

Image Forgery Detection System addresses the growing challenges of detecting manipulated images in today's digital world. As image editing tools become more advanced, distinguishing between authentic and altered images has become increasingly difficult. This is particularly problematic in areas like journalism, law enforcement, and digital forensics, where the accuracy of visual content is vital. With the rise of sophisticated forgery techniques, there is a pressing need for automated systems that can reliably detect tampered images and maintain the authenticity of digital media.

The system uses the **Structural Similarity Index Measure (SSIM)** to compare original and forged images by analyzing their structural features. Unlike pixel-based methods, SSIM detects differences in image patterns such as edges and textures, making it more effective at identifying subtle manipulations that traditional methods might miss.

Preprocessing steps such as resizing and normalization ensure consistency across images before comparison. Differences between the images are then highlighted using thresholding and contour detection, making tampered areas easily visible. This workflow ensures efficient forgery detection while providing an intuitive interface for users.

The **Image Forgery Detection System** plays a crucial role in **digital forensics, security, and media authentication**. In an age of widespread image manipulation, this system offers a reliable solution to ensure the authenticity and integrity of visual content, helping to maintain trust in digital media.

CHAPTER 2

Literature Survey

Chapter 2

Literature Survey

1. Image Forgery Detection using Deep Learning: A Survey, April 2020

Authors:- Zankhana J. Barad, Mukesh M. Goswami

The paper provides a comprehensive review of deep learning techniques for image forgery detection. It contrasts traditional methods that rely on handcrafted features with newer deep learning approaches, which can automatically extract complex patterns from images. The paper also surveys publicly available datasets for training and testing deep learning models, comparing their effectiveness in detecting manipulated images. It highlights the improved accuracy of deep learning methods over traditional ones and presents insights into the application of these techniques in real-world scenarios.

2. Image Forgery Detection, June 2023

Authors: Dipanshu Narayan, Himanshu, Rishabh Kamal

The paper discusses a method for detecting copy-move image forgeries, where a part of an image is duplicated and placed elsewhere in the same image. This type of forgery is difficult to detect because the copied parts share similar attributes with the original image. The proposed solution uses Convolutional Neural Networks (CNNs) to extract features from image blocks and classify images as either original or forged. The model achieves an accuracy of 97.7% using the CASIA2 dataset, which contains both authentic and forged images. The approach effectively addresses challenges like image compression and resizing, which can mask alterations. The method offers real-time processing, making it suitable for applications in social media, legal, and academic contexts, where image forgery detection is critical.

3. Image Forgery Detection using CNN, August 2023

Authors: Meet Patel, Kartikay Rane, Niyati Jain, Praneel Mhatre, Shree Jaswal

The paper proposes a novel image forgery detection system using Convolutional Neural Networks (CNNs) to identify various types of image manipulations, including copy-move, splicing, and retouching. The system integrates Error Level Analysis (ELA) with deep learning to enhance detection accuracy. Tested on real-world images, it achieved a 93% detection accuracy, outperforming existing methods. This CNN-based system offers a robust solution for detecting image forgery in applications like forensics, security, and digital media analysis, addressing the growing concern of manipulated images in today's digital landscape.

4. Image Forgery detection using Deep Learning Model, November 2022

Authors: Praveen Gupta, Chour Singh Rajpoot, T.S.Shanthi, Dvsssv Prasad, Ashok Kumar, S Sandeep Kumar.

The paper Image Forgery Detection using Deep Learning Model addresses the challenge of detecting image tampering, which can compromise the integrity of visual evidence, particularly in legal and forensic settings. The study proposes a deep learning solution using the VGG-19 architecture to identify forged images. The authors utilize a dataset from CASIA, containing both authentic and manipulated images. Preprocessing steps, including image resizing and denoising, are applied to prepare the dataset for training. The model is evaluated based on accuracy and loss, achieving more than 95% accuracy and a minimal loss value, which makes it highly efficient compared to other existing models. The authors suggest that, in the future, the model could be deployed as a tool on a website, allowing the general public to easily detect image forgeries.

5. Image Forgery detection using Deep Learning Model, December 2022.

Authors: K. Latha, D.Kavitha, S. Hemavathi, K. Jayasakhti Velmurugan, Neathi. R.

The paper *Image Forgery Detection Using Machine Learning* explores the increasing concern over the authenticity of digital images due to advancements in imaging technology and the widespread use of photo-editing software. With the rise of social media and the ease of altering images, the integrity of digital images has been compromised, creating a need for effective detection methods. The study employs a machine learning algorithm, specifically Support Vector Machine (SVM), to identify whether an image has been manipulated. The model also includes a feature to block users who attempt to upload altered images. This approach helps maintain the credibility of digital images, especially in fields that rely on them for decision-making, such as medicine and warfare.

CHAPTER 3

System Specification

Chapter 3

System Specification

Software Requirements:

- Operating system : Windows, macOS, or Linux (any OS that supports Python and the required libraries).
- Front End : Python, Matplotlib, GUI.
- Back End : Python

Libraries:- OpenCV, NumPy, scikit-image, OS module.

- Tool :IDE/Code Editor, Python

Hardware Requirements:

- Process : Intel Core i5
- SSD : 512 GB
- Monitor : 15.6-inch or larger screen with Full HD (1920x1080)
- Ram : 8 GB
- Graphics Card : nVIDIA 4GB

CHAPTER 4

Block Diagram

Chapter 4

Block Diagram

Control Flow Diagram:

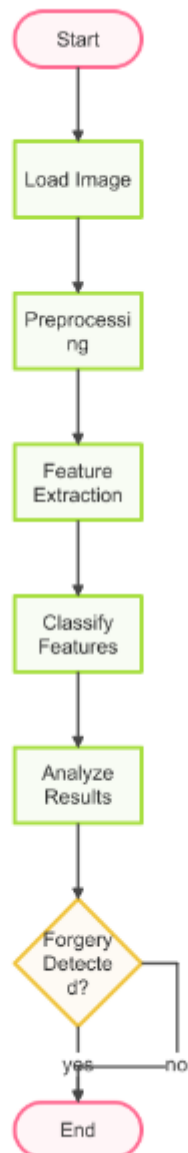


Figure 4.1: Control Flow Diagram

CHAPTER 5

System Design

Chapter 5

System Design

DFD:

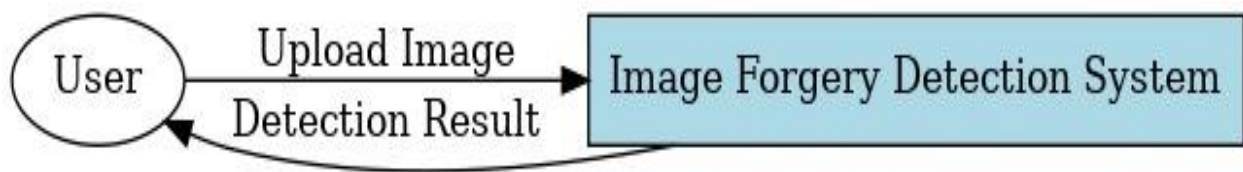


Figure 5.1: Level 0 Data Flow Diagram

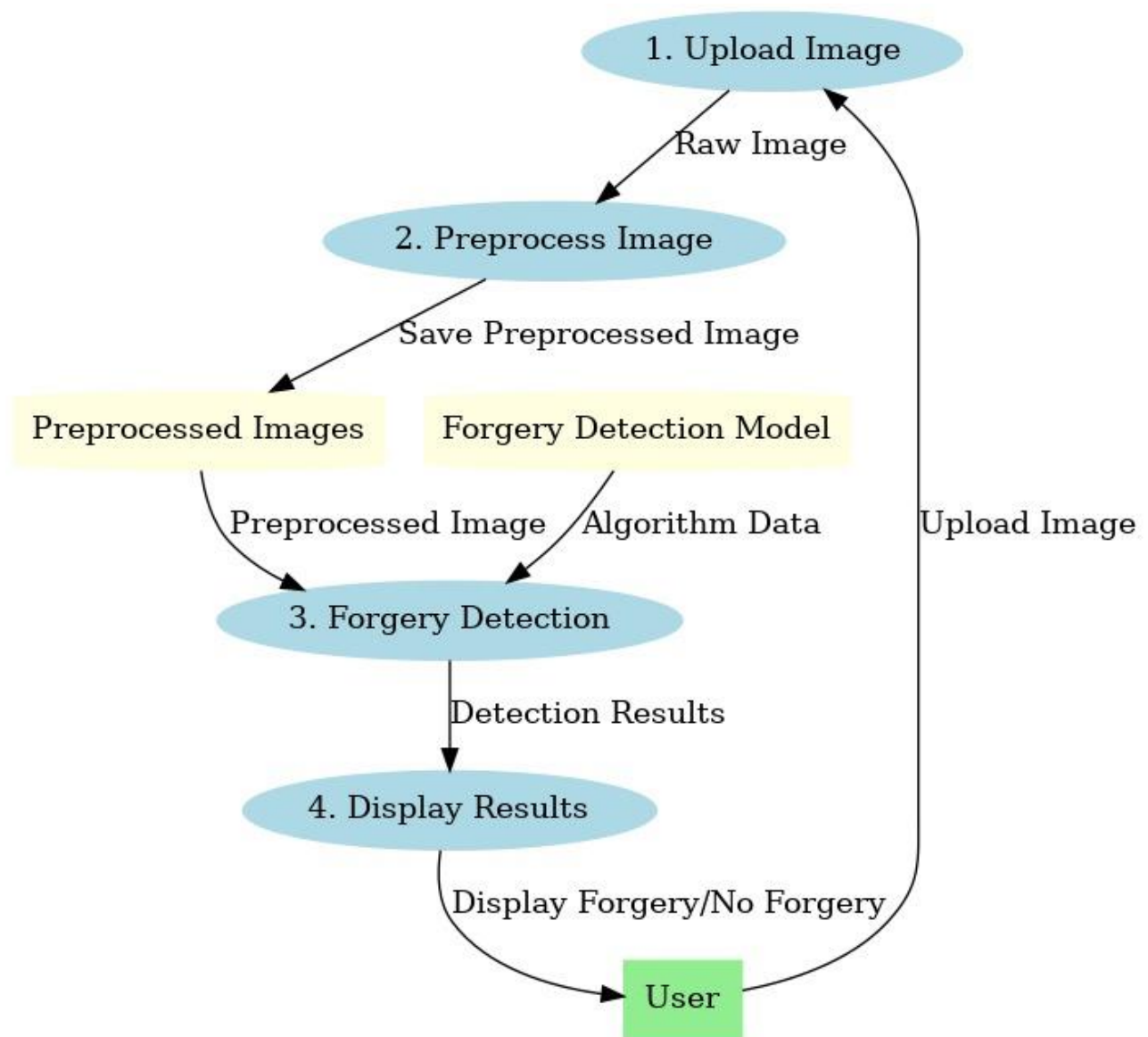


Figure 5.2: Level 1 Data Flow Diagram

UML diagram:

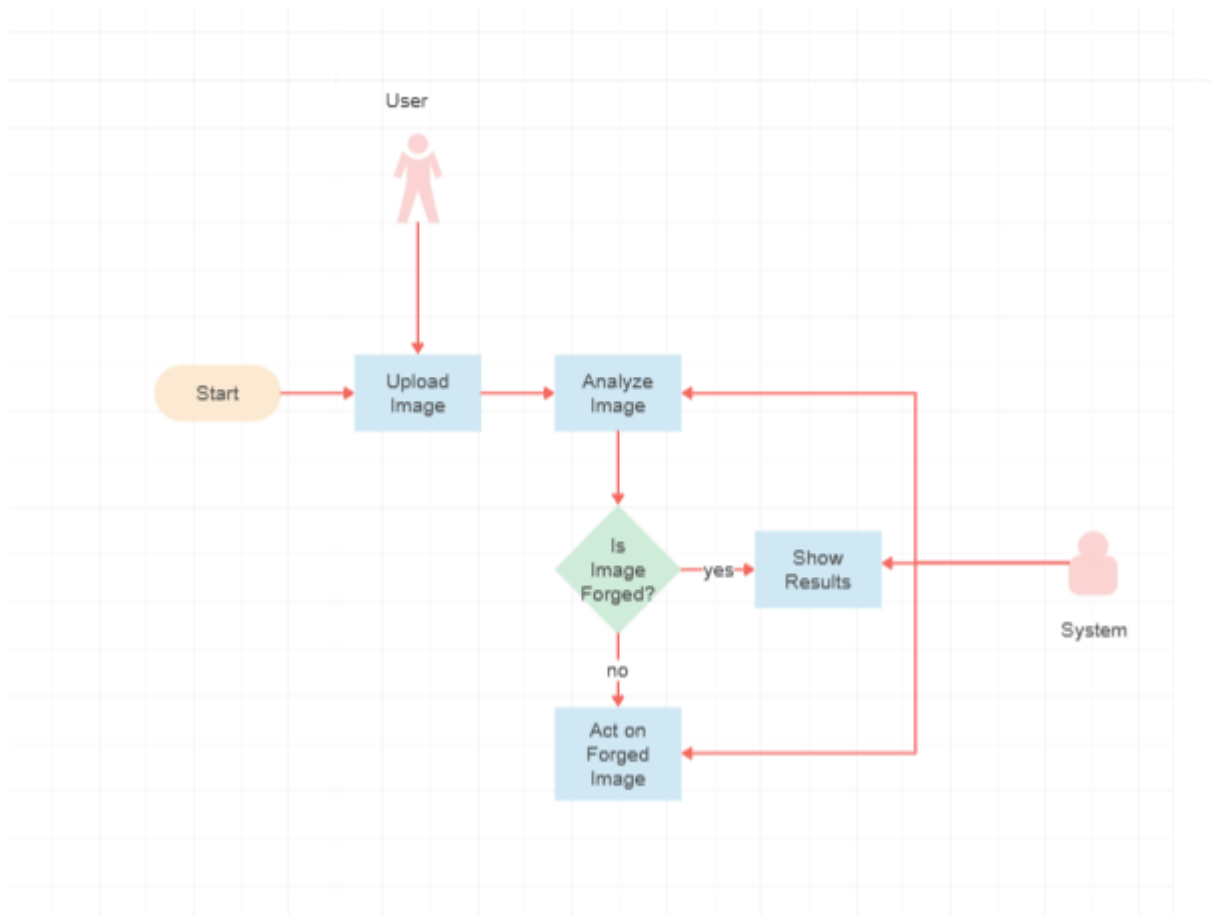


Figure 5.4: UML Diagram

CHAPTER 6

Software Development

Chapter 6

Software Development

Problem statement:

The rise of advanced image manipulation techniques has led to an increase in deceptive practices like misinformation, fraud, and evidence tampering. Verifying image authenticity manually is time-consuming and unreliable, creating a need for an automated system to detect forgeries and ensure the credibility of visual content.

Proposed work:

The Image Forgery Detection System uses machine learning and forensic algorithms to detect image tampering by analysing key features and identifying inconsistencies. It provides clear results, such as forged areas and forgery probability scores, through a user-friendly interface. This tool helps combat misinformation, verify digital evidence, and maintain content credibility, benefiting industries like media, law enforcement, and research.

CHAPTER 7

Troubleshooting / Debugging

Chapter 7

Troubleshooting / Debugging

1. Low Model Accuracy:

Issue: The system's accuracy in detecting forgeries is lower than expected.

Debugging Steps:

- Check the quality and quantity of the training dataset; add more diverse images, including different types of forgeries.
- Verify the feature extraction methods and ensure they capture the relevant image characteristics.
- Review the model's training parameters and adjust them to prevent overfitting or underfitting.

2. Performance Lag:

Issue: The system is slow or unresponsive when processing large images.

Debugging Steps:

- Optimize image processing by resizing or compressing images before analysis.
- Check for resource bottlenecks, and consider using GPU acceleration for faster processing.
- Implement asynchronous or batch processing to handle large datasets more efficiently.

3. Incorrect Detection Results:

Issue: The system provides incorrect results in detecting manipulated images.

Debugging Steps:

- Review the feature extraction process to ensure it's capturing the correct details in images.
- Retrain the model with a more comprehensive and varied dataset.
- Test the system with different image types and adjust the model based on the results.

4. UI Malfunctions:

Issue: The user interface does not display correctly or fails to respond as expected.

Debugging Steps:

- Check the responsiveness of UI elements, ensuring they work on various devices and screen sizes.
- Inspect the front-end code for alignment issues and ensure smooth communication with the backend via APIs.
- Test the app across different browsers to identify platform-specific UI issues.

5. Image Upload Failures:

Issue: The system fails to upload images or encounters errors during the upload process.

Debugging Steps:

- Verify that the supported image formats (JPEG, PNG, TIFF) are being used.
- Check the image file size to ensure it does not exceed the upload limit.
- Ensure proper error handling for unsupported files and provide appropriate user feedback.

6. False Positive/Negative Detection:

Issue: The system misidentifies forged or original images (false positives or false negatives).

Debugging Steps:

- Refine the training dataset to include a broader range of image manipulations and editing types.
- Fine-tune the model's detection capabilities by experimenting with different algorithms.
- Conduct more testing with diverse real-world images to reduce false results.

CHAPTER 8

Conclusion

Chapter 9

Conclusion

The **Image Forgery Detection System** successfully addresses the growing need to verify the authenticity of digital images in an era of widespread manipulation. By using machine learning and forensic techniques, the system provides an effective and user-friendly solution for detecting image tampering. Through ongoing improvements in model accuracy, system performance, and user interface design, this tool has proven valuable for industries like media, law enforcement, and research. With potential future expansions, such as video analysis and real-time monitoring, the system will continue to enhance the credibility and security of digital content.

CHAPTER 9

Future Scope

FUTURE SCOPE

1. **Support for Video Analysis:** Expanding the system to detect manipulation in video files to address the growing issue of deep fake technology.
2. **Integration with Cloud Services:** Providing cloud-based processing for scalability and accessibility, enabling faster analysis for large datasets.
3. **Real-time Social Media Monitoring:** Implementing APIs to monitor social media platforms for forged images and alert users to potentially manipulated content.
4. **Enhanced Accuracy Through AI:** Continuous improvement of detection algorithms using user feedback and the inclusion of advanced AI techniques for higher accuracy.

CHAPTER 10

References

REFERENCES

A] Papers & Websites:

1. Image Forgery Detection using Deep Learning: A Survey, April 2020
Authors:- Zankhana J. Barad, Mukesh M. Goswami
<https://ieeexplore.ieee.org/abstract/document/9074408>
2. Image Forgery Detection, June 2023
Authors: Dipanshu Narayan, Himanshu, Rishabh Kamal
<https://ieeexplore.ieee.org/document/10151341>
3. Image Forgery Detection using CNN, August 2023
Authors: Meet Patel, Kartikay Rane, Niyati Jain, Praneel Mhatre, Shree Jaswal
<https://ieeexplore.ieee.org/document/10205377>
4. Image Forgery detection using Deep Learning Model, November 2022
Authors: Praveen Gupta, Chour Singh Rajpoot, T.S.Shanthi, Dvsssv Prasad, Ashok Kumar, S Sandeep Kumar.
<https://ieeexplore.ieee.org/document/10205377>
5. Image Forgery detection using Deep Learning Model, December 2022.
Authors: K. Latha, D.Kavitha, S. Hemavathi, K. Jayasakhti Velmurugan, Neathi. R.
<https://ieeexplore.ieee.org/document/10046422>