### Seminar Report

On

#### Title of Seminar

By

Name of student Exam No

Under the guidance of

Name of the guide



#### DEPARTMENT OF COMPUTER ENGINEERING Pimpri Chinchwad College of Engineering Nigdi, Pune-411044.

affiliated to Savitribai Phule Pune University (Ac. Yr. 2021-2022)

#### Pimpri Chinchwad Eduacation Trust's Pimpri Chinchwad College of Engineering Nigdi, Pune-411044.



#### **CERTIFICATE**

This is to certify that **name of student** from **Third Year, Computer Engineering** has successfully completed his/her seminar work titled "**Name of Seminar topic**" at Pimpri Chinchwad Eduacation Trust's Pimpri Chinchwad College of Engineering, Nigdi, Pune-411044 in the partial fulfillment of the Bachelors Degree in the Engineering.

Date:		
Place:		
'Name of Guide'	'Name of the HOD'	'Name of the Director'
Guide	Head of the Department	Director

#### Acknowledgment

I take this to express my deep sense of gratitude towards my esteemed guide Prof. ......... for giving me this splendid opportunity to select and present this seminar and also providing facilities for successful completion.

I thank Dr. K. Rajeshwari, Head, Department of Computer Engineering, for opening the doors of the department towards the realization of the seminar, all the staff members, for their indispensable support, priceless suggestion and for most valuable time lent as and when required. With respect and gratitude, I would like to thank all the people, who have helped me directly or indirectly.

Name of the student

Roll no. Class:TECOA199

#### Abstract

Image forgery is nothing but manipulating digital images so as to hide or change some useful information contained in the images. Images are considered as the most effective way to convey information and manipulating this information sometimes creates havoc. The action of tampering images which is done either for fun or to give false evidence can result in a disaster. It is done in such a way that it cannot be determined by the naked human eye so many people have implemented various types of machine learning algorithms which they have implemented with handcrafted features to determine different types of forgery and whether an image is forged or not. These algorithms are used to extract the digital signature of an image and used to differentiate whether an image has tampered or not. In previous works, various techniques have been implemented for either fine or coarse image splicing whereas a technique dealing with both needs to be devised.

## Contents

1	Tec	hnical Keywords	1
	1.1	Problem Definition	2
	1.2	Goals and Objectives	2
	1.3	Motivation	2
	1.4	Scope of the work	2
	1.5	Outcomes	3
2	Intr	roduction	4
	2.1	Domain Description	4
	2.2	Problem Definition	4
	2.3	Motivation	4
3	${ m Lit}\epsilon$	erature Survey	5
	3.1	Existing Methods/Tools/Techniques	5
	3.2	Literature Survey	5
4	Ma	thematical Model	6
5	Pro	posed System Architecture	7
	5.1	System Architecture	7
	5.2	Design with UML Diagrams	7
	5.3	Algorithms	7
	5.4	Implementation/Proof of Concept	7
	5.5	Important Source Code	7
	5.6	Testing Code	7
	5.7	Result screenshot, tables and Analysis	7
6	Adv	vantages / Disadvantages	8

7	App	olications	9
8	Abł	previations	10
9	App	pendix	11
	9.1	Log Report	11
	9.2	Internship letter (if any)	11
	9.3	report of Internship Project (if any)	11
	9.4	hard copy of screenshot of online internship feedback given after internship	11

## List of Tables

1.1	List of students																								,										,												3	,
-----	------------------	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	---	--	--	--	--	--	--	--	--	--	---	--	--	--	--	--	--	--	--	--	--	--	---	---

# List of Symbols, Abbreviations and Nomenclature

Symbol Details

Abs Abstraction

### Chapter 1

#### Technical Keywords

In an advent of social media platforms or digital content sharing platforms the digital data or images can be shared to the world with utmost ease. With an acute rise in social media platforms like messaging applications or photo/post sharing applications, world-wide spread of information takes place within a few minutes. However, it can prove to be a boon or bane for an individual and society. Malefactors tend to use these platforms for their misdeeds, such as spreading fake information in a compelling manner over digital platforms. When it comes to multimedia information images, authenticity check and detection of its forging becomes difficult. Advanced Attempts of splicing images make it very difficult for the human eye to identify whether the image is real or fake. Even a few primitive tools fail to identify the authenticity of images. Digitization is an imperishable characteristic of the 21st century. A digital image is a widespread form of information and is exponentially increasing. Acquisition and alteration of image data are effortlessly accomplished with the help of image editing tools easily available in the public domain. Malicious practices of spreading fake data threaten the security and welfare of the digital world users. The fabricated images are not easily determined with visual inspection and thus require sophisticated technology for detecting forged images. With advancements in image tampering technologies such as GIMP, Pixlr, Photoshop, PhotoScape, etc. it becomes effortless even for an amateur to tamper images flawlessly. Image forgery detection is broadly classified into Active approaches and Passive approaches. Active approaches have predefined information or characteristics of the image. Digital watermarking and digital signature are 2 main active approaches that embed pre-processed information that can be extracted from the image. Passive approaches are comparatively harder to detect and have no predefined information. The images are raw and forgery can be detected solely by various feature extraction techniques. Image splicing is a type of Passive Image forgery wherein the image contains no prior information of its origin. Image splicing is a technique wherein a portion from one image is cropped and pasted onto another image. The cropped part may contain different texture and boundary characteristics than the host image. Thus local and global feature descriptors are extracted from the RGB colour channels of the image. Various machine learning classifiers are implemented for the classification of images into spliced and authentic.

#### 1.1 Problem Definition

Image forgery detection using machine learning with a fusion of global and local thepade's sbtc features.

#### 1.2 Goals and Objectives

- To study and implement the combination of the existing algorithms like the random forest, random tree, etc.
- Identifying whether image tampers or not.
- To do a Feature combination of global and local TSBTC nary.

#### 1.3 Motivation

Digital images become a significant resource of information in the digital world as they are the fastest means of information and medium of communication with the advent of digital

technology, image tampering has become very common. Image Forgery is used mainly for fake news, election and religious polarization, increasing the political power and influence, defaming someone, etc. The adverse effects of such forgery can be long-lasting thus it becomes necessary to deal with such situations so as to reduce the damage caused by such agendas. The use of Machine learning algorithms instead of manual detection can help in better detection of forged and non forged images.

#### 1.4 Scope of the work

- 1. The scope of the project is to categorize images as forged or original using global and local feature vectors to train machine learning classifiers.
- 2. The scope of the project is to improve the existing methodologies present in image forgery detection and increase the prediction accuracy.

#### 1.5 Outcomes

- Finding Accuracies for local TSBTC nary.
- Finding Accuracies for global TSBTC nary.
- Doing Feature fusion of local and global TSBTC feature vectors which gives better accuracy for 2,3,4 nary.

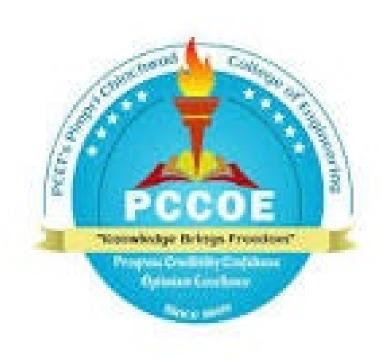


Figure 1.1: Logo for Pimpri Chinchwad College of Engineering

Table 1.1: Comp Branch

Sr. No.	Name of the student	Roll No.	Branch
1.	Apoorva	TECOB299	COMPUTER
2.	Shivam	TECOD499	COMPUTER

$$\int_{x=0}^{2} x^2 + y^2 dx \tag{1.1}$$

## Chapter 2

#### Introduction

- 2.1 Domain Description
- 2.2 Problem Definition
- 2.3 Motivation

## Chapter 3

## Literature Survey

- 3.1 Existing Methods/Tools/Techniques
- 3.2 Literature Survey

## Chapter 4

### Mathematical Model

### Chapter 5

### Proposed System Architecture

- 5.1 System Architecture
- 5.2 Design with UML Diagrams
- 5.3 Algorithms
- 5.4 Implementation/Proof of Concept
- 5.5 Important Source Code
- 5.6 Testing Code
- 5.7 Result screenshot, tables and Analysis

## Chapter 6

Advantages / Disadvantages

# Chapter 7

## **Applications**

## Chapter 8

### Abbreviations

### Chapter 9

### Appendix

- 9.1 Log Report
- 9.2 Internship letter(if any)
- 9.3 report of Internship Project(if any)
- 9.4 hard copy of screenshot of online internship feedback given after internship

### **Bibliography**

- [1] Jean-Marie Bonnin, P. Rawat "Designing a Header Compression Mechanism for Efficient Use of IP Tunneling in Wireless Networks" *IEEE CCNC Aug 2010*.
- [2] B. Storer and et al, "Softwire Hub and Spoke Deployment Framework with L2TPv2," RFC5571, *IETF*, June 2009.
- [3] P.Rawat and et al, "Tunneling Header Compression TuCP for Tunneling over IP," Internet Draft, IETF, Work in Progress, Mar. 2009. "Java AWT Reference" by John Zukowski.
- [4] "Java Software Solutions" by Lewis and Loftus.