<Project Title>

<Name>
Index No : <index no>

Supervisor: <supervisor name>

<January 2022>

Submitted in partial fulfillment of the requirements of the
B.Sc in Computer Science Final Year Project (SCS4224)

<Project Title (Font Size 28)>

<Name with Initials (Font Size 20)>

Declaration

I certify that this dissertation does not incorporate, without acknowledgement, any material previously submitted for a degree or diploma in any university and to the best of my knowledge and belief, it does not contain any material previously published or written by another person or myself except where due reference is made in the text. I also hereby give consent for my dissertation, if accepted, be made available for photocopying and for interlibrary loans, and for the title and abstract to be made available to outside organizations.

Candidate Name:

……

Signature of Candidate Date:

This is to certify that this dissertation is based on the work of

<Name with Initials>

under my supervision. The thesis has been prepared according to the format stipulated and is of acceptable standard.

Principle/Co- Supervisor's Name:

……

Signature of Supervisor Date:

Abstract

A summary of your dissertation, with emphasis on the conclusions. This should fit in about ¾ of this page. Do not cite references or put lists here. It can be 2-3 paragraphs.

Preface

The purpose of this is for you to state explicitly the extent to which your dissertation relies on the work of others, and highlight the portion that you claim to be your own original work. For example: you might say: “The results of chapter 3 rely upon a simulation provided by the research group. The analysis of the data is entirely my own work. I carried out the analytical calculation of chapter 4 in conjunction with my supervisor…” and so on. Without this statement, it will be assumed that no work is original and that your thesis is a review article. If you merely claim that the thesis is all your own work, you should be aware that any evidence to the contrary may leave you susceptible to charges of plagiarism.

Acknowledgement

General thanks that you may want to give.

Table of Contents

List of Figures

List of Tables

Chapter 1 - Introduction

Nam dui ligula, fringilla a, euismod sodales, sollicitudin vel, wisi. Morbi auctor lorem non justo. Nam lacus libero, pretium at, lobortis vitae, ultricies et, tellus. Donec aliquet, tortor sed accumsan bibendum, erat ligula aliquet magna, vitae ornare odio metus a mi. Morbi ac orci et nisl hendrerit mollis. Suspendisse ut massa. Cras nec ante. Pellentesque a nulla. Cum sociis natoque penatibus et magnis dis parturient montes, nascetur ridiculus mus. Aliquam tincidunt urna. Nulla ullamcorper vestibulum turpis. Pellentesque cursus luctus mauris.

Nulla malesuada porttitor diam. Donec felis erat, congue non, volutpat at, tincidunt tristique, libero. Vivamus viverra fermentum felis. Donec nonummy pellentesque ante. Phasellus adipiscing semper elit. Proin fermentum massa ac quam. Sed diam turpis, molestie vitae, placerat a, molestie nec, leo. Maecenas lacinia. Nam ipsum ligula, eleifend at, accumsan nec, suscipit a, ipsum. Morbi blandit ligula feugiat magna. Nunc eleifend consequat lorem. Sed lacinia nulla vitae enim. Pellentesque tincidunt purus vel magna. Integer non enim. Praesent euismod nunc eu purus. Donec bibendum quam in tellus. Nullam cursus pulvinar lectus. Donec et mi. Nam vulputate metus eu enim. Vestibulum pellentesque felis eu massa.

Quisque ullamcorper placerat ipsum. Cras nibh. Morbi vel justo vitae lacus tincidunt ultrices. Lorem ipsum dolor sit amet, consectetuer adipiscing elit. In hac habitasse platea dictumst. Integer tempus convallis augue. Etiam facilisis. Nunc elementum fermentum wisi. Aenean placerat. Ut imperdiet, enim sed gravida sollicitudin, felis odio placerat quam, ac pulvinar elit purus eget enim. Nunc vitae tortor. Proin tempus nibh sit amet nisl. Vivamus quis tortor vitae risus porta vehicula.

Chapter 2 - Literature Review

2.1 Adversarial Attacks

Recent study Goodfellow, Shlens, and Szegedy [1] exposed that deep neural networks, are vulnerable to adversarial examples. Figure 2.1 shows an example.

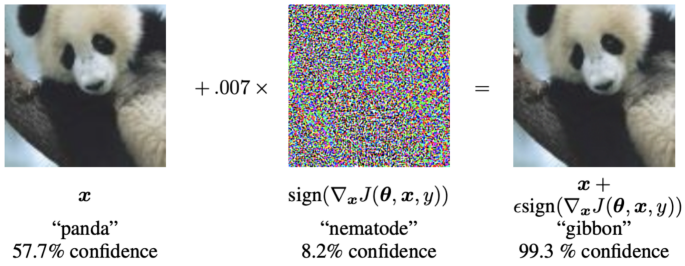

Figure 2.1: Model miss-classifying an adversarial example in vision field

Chapter 3 - Design

Chapter 4 - Implementation

Chapter 5 - Results and Evaluation

Nam dui ligula, fringilla a, euismod sodales, sollicitudin vel, wisi. Morbi auctor lorem non justo. Nam lacus libero, pretium at, lobortis vitae, ultricies et, tellus. Donec aliquet, tortor sed accumsan bibendum, erat ligula aliquet magna, vitae ornare odio metus a mi. Morbi ac orci et nisl hendrerit mollis. Suspendisse ut massa. Cras nec ante. Pellentesque a nulla. Cum sociis natoque penatibus et magnis dis parturient montes, nascetur ridiculus mus. Aliquam tincidunt urna. Nulla ullamcorper vestibulum turpis. Pellentesque cursus luctus mauris.

Table 5.1: Example table

Method	Acc.	AUC	F1
Model	0.9	0.8	0.1

Chapter 6 - Conclusions

Bibliography

[1] Ian J Goodfellow, Jonathon Shlens, and Christian Szegedy. “Explaining and harnessing adversarial examples”. In: *arXiv preprint arXiv:1412.6572* (2014).