HMR INSTITUTE OF TECHNOLOGY & MANAGEMENT

Hamidpur, Delhi-110036

(An ISO 9001: 2008 certified, AICTE approved & GGSIP University affiliated institute)

E-mail: hmritmdirector@gmail.com, Phone: - 8130643674, 8130643690, 8287461931, 8287453693

Department of Computer Science and Engineering

Synopsis of Minor Project

Date: 15/09/2023

Minor Project Title: MI-MAP: Misclassification of Images by Masquerading using Adversarial Patterns

Name of Supervisor(s):

Program: - B.Tech(CSE)		**Year/Semester: - 7th Semester**	
S. No.	**Enrolment No.**	**Name**	**Signature**
1	03513302720	Kanishk Vikram Singh	
2	05513302720	Peeyush Kumar Singh	
3	50413302720	Tushar Bhatia	

Minor Project Summary:

In MI-MAP, the aim is to analyze and generate adversarial patterns to intentionally manipulate the classification and detection models to either misclassify or completely refuse to detect the subject at all by adding imperceptible changes to images. We will be considering the Mini-ImageNet dataset for training and testing purposes. The results are then used to study the vulnerability of such systems, exploring methods to generate effective adversarial patterns, evaluating the impact of such attacks on model performance and reliability and designing robust and secure models.

Objectives:

1) Exploring various techniques to generate adversarial patterns.
2) Understanding the weakness of machine learning models against adversarial attacks.
3) Designing robust and secure deep learning models by understanding their vulnerabilities.

Research Paper Topic: MI-MAP: Misclassification of Images by Masquerading using Adversarial Patterns

Base Paper Link: https://arxiv.org/pdf/1412.6572.pdf

Resource Requirement:

Hardware

1. Processor: Intel® Core™ i5-13500 (14 cores, 20 threads) Processor 24M Cache, up to 4.80 GHz
2. Graphics Processing Unit: Intel® Arc A770 with 32 X^e-cores and 512 tensor cores
3. RAM: 32 GB DDR4 3200 MHz
4. Disk Space: 250 GB
5. Camera: HP w300 1080p

Software

1. Language: Python 3.11
2. Editor: Jupyter Notebook
3. Deep Learning Library: TensorFlow 2.13
4. OS: Windows, Linux

Schedule of Minor Project Work Along with Research Paper:

- September
- October
- November
- December

Signature of Student: **Signature of Supervisor(s):**

Signature of Minor Project Co-ordinator:

Co-ordinator Name:

Approval by Project Committee

Member	Signature	Remark (Approved/Not Approved)

Member	Signature	Remark (Approved/Not Approved)