8-June-21

Deep-Fake

Report

By:

Arpajit Adhikary (ECE, Delhi Technological University)

Contents

[IR Transmission and Receiving for Room Security 1](#_Toc65436719)

[Introduction 1](#_Toc65436720)

[Methodology 1](#_Toc65436721)

[Implementation 1](#_Toc65436722)

[Expected Outcomes 1](#_Toc65436723)

[Timeline 1](#_Toc65436724)

# Deep-Fake

## Introduction

The fact that authentication techniques exist, there also exists methods to tamper the security. In this project, we are focusing on a particular process of tampering with fingerprints. The addition of noise to fingerprint images causes the authenticator to confuse and consider fake fingerprints to be the original ones. With this project, we shall be able to detect these attacks, also termed Adversarial Attack.

## Methodology

The implementation should be in the form of the following performance:

The samples of fingerprints will be used for detection and rejection.

We will have a target classifier for the comparison.

A loop will be implied to get accurate results on every subject.

The looping condition shall be to reach a similar image as compared to our target classifier.

The

## Implementation

We will be designing a hardware circuit to implement the idea and develop a door mechanism for serving our purpose.

## Expected Outcomes

We expect that this implementation should help us bring out a circuit and a mechanical door design, which will keep us updated on our room activities and alert us about intruders.

## Timeline

We expect to complete our projects in the following order:

* We hope to achieve our circuit implementation by mid-semester.
* We shall be completing the door mechanism by the end of the semester.