Enhanced Pattern Unlocking in Smartphones

Ayush Gupta, Harsh Jain, Wrik Bhadra

IIIT Delhi

Problem Statement

As per a 2018 report, there are about 2.4 billion smartphone users across the globe, and half of them use a pattern to unlock their phone.

However, this unlocking method is prone to smudge attack and over-the-shoulder snooping. A study conducted by researchers of US Naval Academy and the University of Maryland, Baltimore County claims that 2 out of 3 people can easily recreate a pattern just after viewing it once from 5-6 ft. away.

In our current project, we propose to address the attacks mentioned above by examining and incorporating additional factors that can significantly improve the unlocking mechanism.

Motivation

Improving this system allows us to reach a large base of people who use a pattern as their unlocking mechanism. Our motivation behind developing this system so to enhance the security of smartphones. Our research suggests that this is a relatively unexplored topic and hence working on this might open up new avenues.

In regards to this, we recount an experience our friend had when a small girl was able to unlock his phone just by looking at the trace created on the screen; essentially a smudge attack.

Objective

We will develop a system that will take into account the actual haptic gesture, speed, and pressure on the screen while drawing the pattern.

This combined data along with a Convolutional Neural Network and Binary Classification Model will predict the authenticity of the user.

Model and Architecture

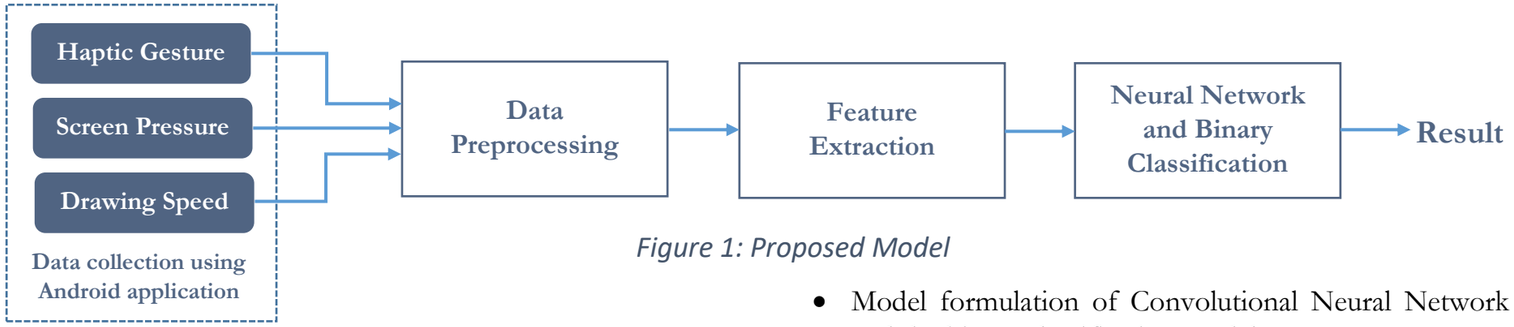
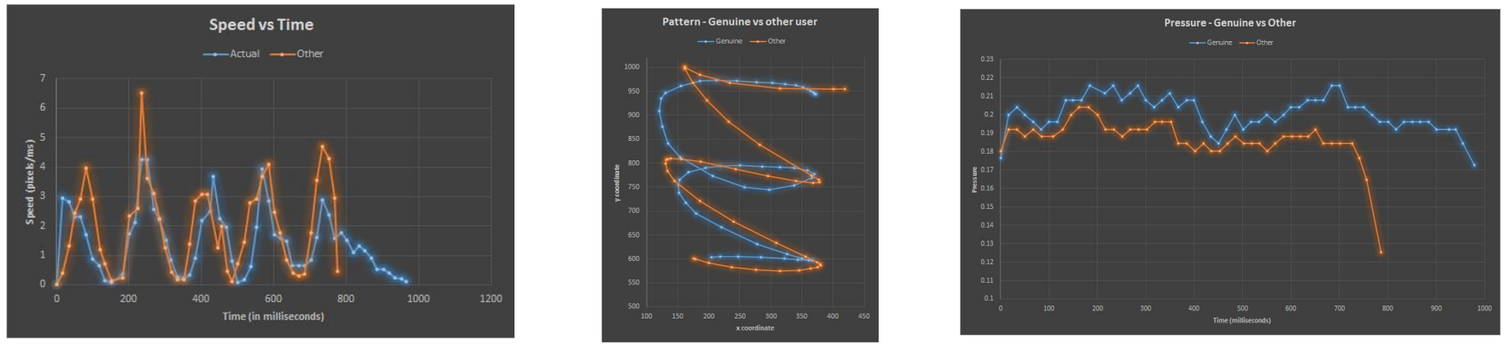


Figure 1: Proposed Model

- Create an Android application to collect data
- Convert data to plots and images (as shown in Figure 2)
- Identify important features to train the classifier
- Model formulation of Convolutional Neural Network and the binary classification model
- Training and testing the model

Note: If time permits, we will implement **Online Machine Learning** to incorporate behavioral changes in humans.

Data – Sample plots and images



(a) *(b)* *(c)*

Figure 2: Sample plots of **actual data** (a) Speed vs Time graph (b) Haptic Gesture plot (c) Pressure vs Time graph

Evaluation Metric

The system can be evaluated using the following two metrics:

- ROC – AUC
- Confusion Matrix

Timeline

First Evaluation
- Android Application
- Data collection and preprocessing

Second Evaluation
- Feature extraction
- Neural Network and Binary classification model

Final Evaluation
- Working model after training and testing
- Performance Improvement and Online Machine Learning

References

[1] A. Chahar, S. Yadav, I. Nigam, R. Singh and M. Vatsa. A Leap Password based Verification System. *IEEE 7th International Conference on Biometrics Theory, Applications and Systems (BTAS)*, 2015.

[2] I. Nigam, M. Vatsa and R. Singh. Leap signature recognition using hoof and hot features. *IEEE International Conference on Image Processing (ICIP)*, 2014.