AI HAND PATTERN AUTHENTICATION METHOD

by
Liron Kesem

A thesis

submitted in partial fulfillment

of the requirements for the degree of

Master of Science in Electrical and Computer Engineering

Boise State University

December 2021

BOISE STATE UNIVERSITY GRADUATE COLLEGE

DEFENSE COMMITTEE AND FINAL READING APPROVALS

of the thesis submitted by

Liron Kesem

Thesis Title: AI Hand Pattern Authentication Method

Date of Final Oral Examination: 2 July 2021

The following individuals read and discussed the thesis submitted by student Liron Kesem, and they evaluated the student's presentation and response to questions during the final oral examination. They found that the student passed the final oral examination.

Sin Ming Loo Ph.D.	Chair, Supervisory Committee
Liljana Babinkostova Ph.D.	Member, Supervisory Committee
Charmaine C. Sample Ph.D.	Member, Supervisory Committee

The final reading approval of the thesis was granted by Sin Ming Loo Ph.D., Chair of the Supervisory Committee. The thesis was approved by the Graduate College.

ACKNOWLEDGMENT

I would like to thank the people who supported me in completing my thesis work. Thanks go to Prof. Sin Ming Loo for accepting me as his M.Sc. student. He provided keen insight and scientific support for my research and pushed me to exceed my own expectations. From the very beginning, Dr. Loo guided me on how to correctly choose an academic worthy research topic, conducting the proper academic paper survey. He also provided extensive and always useful feedback on the thesis itself. Above all, Prof. Loo always knew to ask the correct questions and challenge my theory.

I am grateful to my parents, Miriam and Hillel Yitzhak, for nurturing my interest in science from early on. They are always excited to discuss every aspect of my work, and make an effort to really understand my research, which has led to much useful feedback, and moral support during my graduate studies.

Finally, I would like to thank my husband Mike Kesem for many contributions small and large to my research.

ABSTRACT

As technology evolves, we need better tools to secure our sensitive data on our smartphones. The common method is two factor authentication. This thesis offers a unique biometric authentication method. This authentication method was utilized by solving a simple maze. It is based on the idea that abnormal hand gestures could be flagged as a security threat. The maze is just a simple tool designed to limit the user's hand movements and compare it against the same user's machine learning model. The maze captures the uniqueness of writing - graphology. This thesis shows two different maze configurations. Maze A is wider and each participant solves the maze three time periods throughout the day (i.e., morning, afternoon, night). Maze B is narrower and each participant solved the maze within one sitting. The data collected by this thesis shows 93.66% model prediction accuracy for maze A, and 94% model prediction accuracy on maze B.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF SYMBOLS

C	cost function
η	learning rate
$\sigma(z)$	sigmoid function
a	activation function
b	bias
w	weight
y	label
z	neuron's output

ABBREVIATIONS

Adam	Adaptive Moment Estimation algorithm
AI	Artificial Intelligence
BN	Batch Normalization
CNN	Convolution Neural Network
DA	Data Augmentation
FC	Fully Connected
ML	Machine Learning
NN	Neural Network
ReLu	Rectified Linear Unit
LSTM	Long Short Term Memory
ReLU	Rectified Linear Units
SGD	Stochastic Gradient Descent
SMS	Short Message Service
VGG16	Visual GeometryGroup with 16 layers

CHAPTER 1:

INTRODUCTION

Smartphones have become an inseparable part of our daily lives. We use them to set our morning alarm for work or school, communicate with friends and family anywhere around the world, listen to music, read the news, watch YouTube videos, check our emails, etc. Even employees can access a company's emails and network via their smartphone. Thus, securing our smartphone is essential and vital, since it entails the most sensitive information of our personal and work lives.

To enhance the security of corporate systems, such as smartphones, security savvy entities are deploying multi-factor authentication to add an additional layer of protection. Multi-factor authentication is based on three factors (3F): 1) Something You Know (e.g., a password), 2) Something You Have (e.g., a token device or Short Message Service (SMS)), 3) Something You Are (e.g., fingerprints or voiceprints). Even with deployment of multi-factor authentication, it is still possible to bypass the multi-factor authentication process. Consider the scenario in which a smartphone is stolen (Something You Have). If the smartphone is not protected and does not have a screen lock, the thief can reset the password on financial apps, or even obtain user information from the device (Something You Know). A Phishing attack is another way to steal a user's credentials, where the victim opens an email or message and is tricked into clicking on a malicious link- which can lead to obtaining the *Something*

You Have and Know. Even *Something You Are* can be defeated. For example, one can use a universal fingerprint (real or synthetic fingerprints that can fortuitously match with a large number of fingerprints [5]) which can crack 65% of real fingerprints [6], or one can use the victim's biometric sampling, such as a fingerprint, voice recording or photo, which can be obtained from the device.

To avoid the previously mentioned Phishing attacks, a person's signature has been used as verification tool. A user's signature is a tool used for user verification and has been in use for many years. More recently, signatures have emerged as a biometric recognition tool. The user needs to provide their signature which leads them to stored data in the system. However, if the stored biometric data were to be compromised, the data would be valuable to the hacker hands (e.g., it can be used to forge signed documents). This led us to think about a safer way to incorporate the user's unique attributes to grant access to sensitive data on their mobile devices.

1.1 Unique Hand Pattern for Authentication

This research introduces an alternative/additional approach for biometric signature using the Artificial Intelligence (AI) model to classify the user's "unique hand pattern" on a given benchmark. Within this new approach, the user was asked to solve a maze. The maze was chosen arbitrarily, with the purpose of confining the user's hand movement within an arbitrary framework. The maze features, such as spaces between maze lines and round or square lines, are important factors to consider. Solving the maze is not the objective, rather just the mean. The goal is confining the user's movement freedom to a confined area to capture the user's unique hand movement. From previous research [7–9], each person has a unique hand pattern which could be used as another layer of protection against cyber-attack attempts on sensitive

information such as financial or corporate applications.

Instead of applying the obvious user hand autograph, we decided to increase the security by applying the only factor that a cyber-attacker could not access, which is the user's unique hand movement within a narrow space. When the hacker records the user solution, he will need to match the user's finger size and hand-movement. However, matching the user's finger size and hand movement will be hard to mimic-because the maze solution will be given in real time. Thus, this will be another tool to prevent attackers from attempting to forge the user's autograph.

1.2 Thesis Outline

The following chapter discusses an introduction to neural networks. In Chapter 3, the related work in biometric authentication is presented. In Chapter 4, the approach of authentication is discussed. The details of neural networks and results are presented in Chapters 5 and 6, respectively. It is followed by the summary and conclusions in Chapter 7.

CHAPTER 2:

BACKGROUND

In this chapter we will introduce the Machine Learning (ML) mathematical background. This chapter also includes the unique ways to improve machine learning accuracy (the ability of the model to predict the desired input). Lastly, we discuss the importance of datasets, and how to improve datasets by applying data augmentation practices.

First, it is important for us to define Artificial Intelligence (AI), Machine Learning (ML), and Deep Learning since people often use them interchangeably, without fully understanding the difference between them. Artificial Intelligence (AI) is any computer program that performs tasks that normally require human intelligence, such as decision-making [10]. Machine Learning (ML) is a subset of AI that enables self-learning data and then applies that learning without the need for human intervention [10]. Deep Learning is a subset of ML that is composed of a set of algorithms reaching new levels of accuracy for solving many important problems, using image recognition, sound recognition, etc [10].

2.1 A Simple Neural Network

A neural network is a ML model that is composed of neurons. Their name and structure are inspired by the human brain, mimicking the way that biological neurons signal to one another [11]. For any given input and label vector, a neural network tries to "fit" the outputs to the input. A neuron takes several binary inputs, as shown in Figure 2.1, to produce a single binary output. The following equation shows the first operator- summation:

$$z = \sum w_i x_i + b \tag{2.1}$$

Where z-output from the summation operator, x_i-input, b-bias and w_i-weights. ML training refers to the adjustment of weights (w_i) and biases (b). This means that the values of the weights and biases go through multiple iterations to determine the best values to represent the dataset.

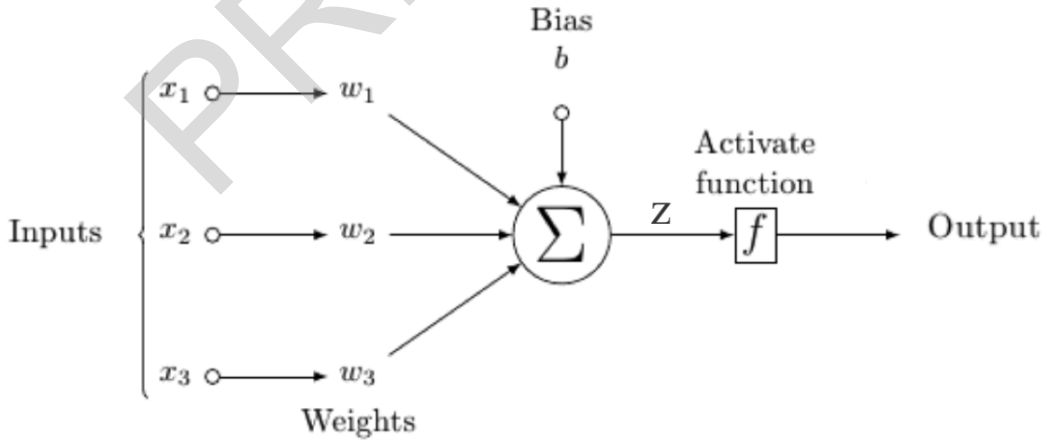

Figure 2.1: Neuron

After the summation operation, the output (z also shown in Figure 2.1) funnels

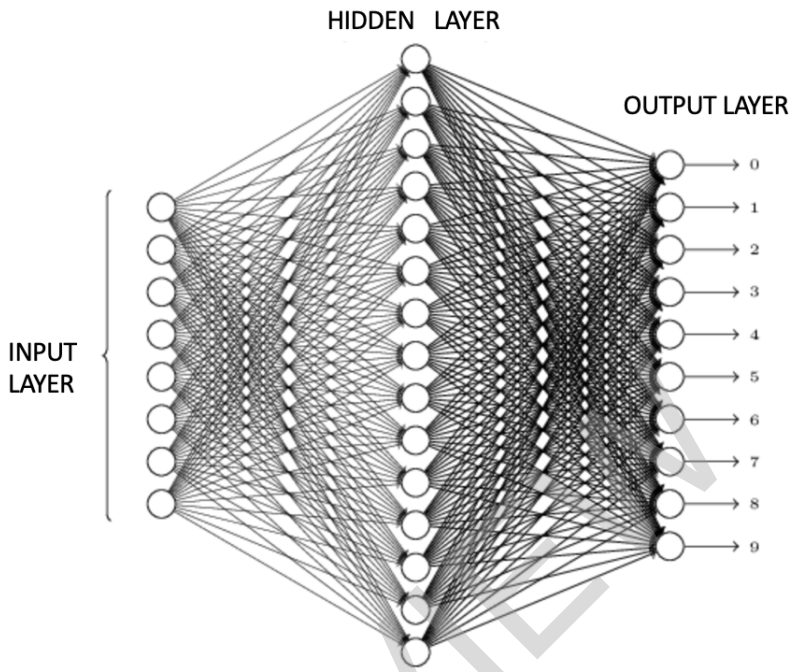

Figure 2.2: Neural Network

through an activation function- f. An activation function determines whether the output (z in our case) should be activated or not.

As we can see from Figure 2.2, a neural network can be multi-layered (e.g., input, hidden and output layer) and have multiple neurons for each layer. The layers have been calculated using Equation 2.1. Again, the result goes through an activation function. An activation function can be one of the following: