

# Verifying online signatures through an iterative device independent model

by

Samiha Tahsin

18101265

Robin Molla

21241081

Omran Jamal

18101263

A thesis submitted to the Department of Computer Science and Engineering  
in partial fulfillment of the requirements for the degree of  
B.Sc. in Computer Science

Department of Computer Science and Engineering  
Brac University  
January 2023


© 2023. Brac University  
All rights reserved.

# Declaration

It is hereby declared that

1. The thesis submitted is my/our own original work while completing degree at Brac University.
2. The thesis does not contain material previously published or written by a third party, except where this is appropriately cited through full and accurate referencing.
3. The thesis does not contain material which has been accepted, or submitted, for any other degree or diploma at a university or other institution.
4. We have acknowledged all main sources of help.

**Student's Full Name & Signature:**



Samaha Tahsin  
18101265



Robin Molla  
21241081



Omran Jamal  
18101263

# Approval

The thesis/project titled “Verifying online signatures through an iterative device independent model” submitted by

1. Samiha Tahsin (18101265)
2. Robin Molla (21241081)
3. Omran Jamal (18101263)

Of Fall, 2022 has been accepted as satisfactory in partial fulfillment of the requirement for the degree of B.Sc. in Computer Science on January 23, 2023.

## Examining Committee:

Supervisor:  
(Member)

---

Md Saiful Islam  
Senior Lecturer  
Department of CSE  
School of Data and Sciences  
BRAC University

Co-supervisor:  
(Member)

---

Rafeed Rahman  
Senior Lecturer  
Department of CSE  
School of Data and Sciences  
BRAC University

Program Coordinator:  
(Member)

---

Name of Program Coordinator  
Program Coordinator  
Department of CSE  
Brac University

Head of Department:  
(Chair)

---

Sadia Hamid Kazi  
Chairperson  
School of Data and Sciences  
Brac University

## **Ethics Statement**

This is optional, if you don't have an ethics statement then omit this page

## Abstract

Hand signatures are getting used from as early as we invented writing. In 3100 BC, we found examples of people using words and symbols to denote their identity. It has also been used as a method of identification. Modern society kept hand signatures for many purposes like the authentication of banking and real estate fields. The recent trend of working from home and business on the go created a necessity to bring the signature from paper to smartphone. Statistics also indicated that it is a user-preferred method of verification. In this paper, we proposed a novel method to verify online signatures using an iterative approach that is device independent. It will be helpful to bring the signatures from paper to smartphones. In this method, we have created a model per signatory, based on their behavioral pattern on each point based on time and distance from the start of the signature. We also considered the difference between the signatory's own signatures while training. We worked with different derived datapoints like velocity, angular velocity etc. We have achieved 8% EER on the MCYT dataset and 20% EER on the Mobisig dataset.

**Keywords:** Signature verification; Machine Learning; e-signature; Online Signature Verification

## **Dedication (Optional)**

A dedication is the expression of friendly connection or thanks by the author towards another person. It can occupy one or multiple lines depending on its importance. You can remove this page if you want.

## **Acknowledgement**

Firstly, a huge respect and gratitude to our supervisor Md Saiful Islam sir who has accompanied us through the whole research and has made us familiar with the thesis process. He has given clear, precise, and helpful feedback that helped us to improve the paper. Our co-supervisor Rafeed Rahman sir was also available whenever we needed help.

Secondly, to all the teachers that taught us at the university. Their contribution is to every bit of progress that we have made. The whole learning experience that we acquired from the university has helped us to face challenges and solve them. Knowledge acquired from different courses helped us.

We, as a team, solved a lot of challenges together. It wouldn't be possible without the help of The Almighty.



# Table of Contents

Declaration	i
Approval	ii
Ethics Statement	iv
Abstract	v
Dedication	vi
Acknowledgment	vii
Table of Contents	viii
List of Figures	x
List of Tables	xi
Nomenclature	xii
<b>1 Introduction</b>	<b>1</b>
1.1 Overview . . . . .	1
1.2 Importance / Usefulness . . . . .	1
1.3 Current Scenario / Motivation . . . . .	2
1.4 Research Objectives . . . . .	3
1.5 Thesis Outline . . . . .	4
<b>2 Literature Review</b>	<b>5</b>
2.1 Related Work . . . . .	5
2.2 Background Analysis . . . . .	6
2.2.1 Signature . . . . .	6
2.2.2 Signature Verification Identification . . . . .	6
2.2.3 Comparing Online and Offline Signature Verification . . . . .	6
2.2.4 Feature Types . . . . .	7
2.2.5 Mobisig Dataset . . . . .	7
2.2.6 MCYT Dataset . . . . .	8
<b>3 Implementation</b>	<b>10</b>
3.1 Methodology . . . . .	10
3.2 Datasets . . . . .	11

3.3	Train-Test Split . . . . .	12
3.4	Data Pre-processing . . . . .	12
3.5	Training . . . . .	13
3.6	Inference . . . . .	14
3.7	Evaluation . . . . .	14
<b>4</b>	<b>Result and Analysis</b>	<b>16</b>
<b>5</b>	<b>Conclusion</b>	<b>18</b>
5.1	Conclusion . . . . .	18
5.2	Future Work . . . . .	18
	<b>Bibliography</b>	<b>21</b>

# List of Figures

1.1	Expected market share of hardware and software in 2030 . . . . .	2
2.1	Mobisig Data (Genuine Signature) . . . . .	7
2.2	Mobisig Data (Forged Signature) . . . . .	8
2.3	MCYT Data (Genuine Signature) . . . . .	9
2.4	MCYT Data (Forged Signature) . . . . .	9
3.1	Methodology . . . . .	10
3.2	MobiSig: User 12, Signature 0 (Genuine) . . . . .	11
3.3	MobiSig: User 12, Signature 0, Domain: Distance, Reduced (Genuine)	12
3.4	MobiSig: User 12, Signature 0, Domain: Time, Reduced (Genuine) .	13
3.5	MobiSig: User 12, Signature 0, Domain: Time, Reduced, Velocities (Genuine)) . . . . .	13
3.6	MobiSig: User 12, Signature 0, Domain: Time, Reduced, Accelera- tions (Genuine) . . . . .	14
3.7	Variance at specific points of user own signature . . . . .	14
3.8	Threshold vs FRR, FAR - Mobisig . . . . .	15
3.9	Threshold vs FRR, FAR - MCYT . . . . .	15
3.10	Threshold vs FRR, FAR - MCYT + MobiSig . . . . .	15

# List of Tables

# Nomenclature

The next list describes several symbols & abbreviation that will be later used within the body of the document

*EER* Equal Error Rate

*FAR* False Acceptance Rate

*FRR* False Rejection Rate

# Chapter 1

## Introduction

### 1.1 Overview

Authentication is an integral part of security. There have been several methods of authenticating, such as through physiological biometric authentication and behavioral biometric authentication. Physiological biometric authentication includes iris scanning, fingerprint scanning, handscan recognition etc. On the other hand, behavioral biometric authentication can include handwritten signature, voice recognition, etc.

Also, recognition includes two parts here: identification and verification. A handwritten signature has been used to verify a person, and there have been several ways to prevent forgery in this case. However, identifying through handwritten signatures has not been part of our everyday lives yet.

The two types of signature verification methods commonly used are offline verification and online verification. In case of offline signature verification the signature is derived from a hard copy such as paper and then verified through its features by images. For online verification, the signature is extracted through smart phones where a person can sign and several features can be determined through dynamic characteristics, such as speed, pressure, shape etc.

For verification of signatures, the features can be extracted both globally and locally. Global features include the average time spent for signing, the total time taken, the pressure applied, and overall it states the relationship of the whole signature process. On the other hand, the local features include the x and y coordinates, pressure, in relation to each point of the signature.

Signature Verification is widely used for banking transaction and consumer verifications, electronic payments, access control systems, criminal investigations, and so on.

### 1.2 Importance / Usefulness

In 2021, the signature verification market was valued at 1.6 Billion USD globally.[10] The covid-19 pandemic increased the popularity of online signatures as we needed

to keep working from the home. Remote work is also getting popular after the pandemic. Identity theft is a major threat to security as we are gradually depending on the internet for more sensitive deals and businesses. Autograph was very popular before the invention of smartphones that allows selfie with a celebrity. But the necessity of signature is growing along with digital methods of biometric authentications. Currently, banks usually allow a limited amount of transactions using multi-factor authentication based on OTP. Some are using fingerprints as well. But the reliability of hand signature is unchanged. The banking system still issues cheques and signature-based authentication. Real estate businesses also heavily depend on the signature. Working from home and running a business in remote places is a recent trend. And this has created a necessity to bring the signature from paper to online. Reducing the cost of papers, maintaining the papers, and shipping documents across the world. And most importantly allowing people to make deals from home. Peterson M. (2015) found that 82% companies spend billions of dollars on paper. [3]

The online signature market is split into major two fields, hardware, and software. In this paper, we will be trying to make an algorithm that reduces the cost of hardware. Pramod B et al(2021) stated that the software segment of the signature market will

Figure 1.1: Expected market share of hardware and software in 2030



get a huge boost in 2030.[9] Banking, financial services, and insurance is rapidly changing to provide services digitally from the users' end. The banking sector still requires a user's signature for a large amount of transactions, while other biometric authentication systems like fingerprint and mobile-based multi-factor authentication systems allow them to make small transactions because other factors cannot reliably guarantee that the request has been made by the real customer.

### 1.3 Current Scenario / Motivation

There is a huge processing cost for handling the documents, especially when they are signed. Still, 41% of companies need signatures on their documents. Online signatures can save 66% of files from missing[6] and reduce 80% shipping costs by getting rid of the papers (Pramod B et al, 2021).

Also, 48% of the companies need the documents duplicated several times by a photocopier machine. Papers are not eco-friendly as they are produced from trees. Collecting physical signatures from door to door, and verifying the signatures are

also full-time work involving a good human force. Pramod B et al (2021) found that businesses saved 86% of document costs by switching to online signatures while reducing 80% of the errors.[7] Manual signature verification in physical paper is not much reliable and efficient as it highly depends on the individuals who are verifying the authenticity and it still leaves a huge gap to exploit in different ways. Forbes reported that getting rid of the manual processes will increase 70-80% efficiency. [8] Keeping that signed document safe and secure for a long period of time is also costly. The above research inspired us to find out a way to make a system to automate the verification process while reducing the cost of authenticating it.

## 1.4 Research Objectives

Signature has been used as an behavioral authentication system for several centuries. There are several digital physiological biometric authentication e.g. fingerprint scanning, face recognition etc. introduced in the last decade that are getting used in a lot of fields. Verifying signatures was a manual process and there was no reliable way to prevent forgery. Signature forgery is a task that can bring a lot of reward to the perpetrator if he is successful.

Recently the use of handwritten signatures has decreased in many fields by the newly introduced physiological biometric authentication systems. As individuals now don't use signatures on a daily basis, they don't have a very fixed signature. There are a lot of variations in their signature. This verification makes it difficult to verify the authenticity of it. One of our main challenges is to verify the authenticity of the signatory even if the signature varies a lot.

Though there are some robust physiological biometric authentication systems introduced, signature verification is still a reliable system for many reasons. There has been a lot of controversy about physiological biometric authentication. It requires an external device, so it is very expensive when it comes to a company like a bank, government offices, courier companies that need to verify authentication of a large number of individuals on a regular basis. The second problem that we are going to solve is introducing cheap authentication without the need of external or third party devices.

In physiological biometric authentication, another human security is sometimes required. For example, we cannot rely on facial or audio recognition on a user who is staying at home. University of Washington scientists have developed a system that can synthesize Obama's facial expressions and speech both. There has been a lot of study on deep fake in recent years. These are going to make facial recognition penetrable. On the other hand, fingerprint based authentication is also left in metal and glasses that makes the individual trackable. Mr Krissler, member of Chaos Computer Club, claimed to reproduce fingerprints from just photographs. Facial recognition also makes the individual trackable through cameras. UCL developed a system named 'My Text in Your Handwriting' that can mimic someone's handwriting. In signature verification, as it is a behavioral biometric authentication system, users can change it easily. Our challenge is to make a system that can deal with



mechanically reproduced signatures.

Ease of deployment as a service is another problem that needs addressing. Our system is deployable at significantly low cost. Existing devices on the user's hand can be used as terminal devices.

## 1.5 Thesis Outline

The aim of this research is to establish a cost-effective and efficient method to verify online signatures. These signatures can be hand-drawn on mobile displays and does not need any extra stylus, it is optimized for drawing on screens themselves. Also, using a stylus may provide a lot more data for the signature such as azimuth, pen-tilt and pressure, however using our algorithm, we can determine the authenticity without collecting those data therefore it is equally effective as using a stylus.

In the first chapter (Chapter 01), we give a summary of how signature is used as part of authentication and what are the types of signature verification method. We also provide an insight of how different features of signatures are extracted and where signature verification is mostly used. We also showcase the current scenario of the signature verification industry and how it is a much cost effective method to shift to online signature verifications for daily use and which industries mostly make use of it.

In the second chapter (Chapter 02), we show the related work done by different researchers around the world and how we took inspiration from them. It outlines their results and also what kind of algorithms they used for doing their research.

We described the implementation of our algorithm in the third chapter (Chapter 03), and highlighted all the steps of the process. It includes pre-processing, training, inference and evaluation steps for the algorithms.

In Chapter four (Chapter 04), we talk about the result and analysis of our algorithm and also showcases the comparative advantages of using our algorithm.

Finally, in Chapter five (Chapter 05), we draw the conclusion and focus on the future work with signature verification and authentication.

# Chapter 2

## Literature Review

### 2.1 Related Work

The verification of signatures has been an extensive subject of research for several years. Online signature verifications have been associated with the DTW algorithm which takes a sample as input and then aligns the signature nonlinearly with respect to the stored signature. However, a new technique was proposed through an Extreme Points Warming by Chan and Wah (2003), which took the extreme points of a signature and made the actual and the forged signatures more comparable. This paper presents that this technique is an improvement over the DTW technique since the computation time decreased by the factor of 11.

M. A. U. Khan et al (2006) determines the verification through a more dynamic approach such as velocity.[1] In this paper, a signature is segmented based on strokes and the velocity of the signature is broken down into three parts, low, medium and high. A histogram is then used to depict these velocities and the medium velocity is found out to be the most stable form of verification using Euclidean distances for the strokes.

Marianela et al (2013) explore the idea of verification through Legendre polynomials and explores more dynamic time dimension functions. For the time functions, pen coordinates, pressure, velocity, and acceleration were used for the verification of online signatures.[2] They segment the signatures according to the Legendre polynomial. However, the interesting thing about this paper is that they took different language data sets, such as Chinese and Dutch.

Luiz G. Hafemann, Robert Sabourin and Luiz S. Oliveira published their paper on offline handwritten signature verification in 2017 which included research based on signature verification in the last 5 to 10 years, recent and future prospects.[4] It also included the problems and challenges done while conducting this kind of research. It then demonstrated Deep Learning Methods of verification which provided a superior result compared to the existing algorithms. They then compared the algorithms on some metrics that are universally concluded as the comparative basis for signature verification known as FAR (False Acceptance Rate), FRR (False Rejection Rate) and EER (Equal Error Rate). We were inspired by this research to take a functional approach instead and to compare our results using the same metrics on the

Mobisig database and MCYT database for online signatures.

In 2019, another paper was published by Chuang Li, Xing Zhang, Feng Lin, Zhiyong Wang, Jun'E Liu and Rui Zhang who used a stroke-based RNN for writer-independent online signature verification.[5] Here the authors used a novel stroke-based bidirectional RNN architecture to break down the signature into multiple patches or strokes and extracted the features. They also measured their results in terms of EER and they found out that it can reduce the EER by 33% which is far better than normal RNN. They also implemented their algorithm on both MCYT and Mobisig algorithms.

## **2.2 Background Analysis**

### **2.2.1 Signature**

Signatures are a method by which someone depicts their identity and uniqueness. This has been a way of legal identification since the start of civilization. Other means of identification include biometric verifications. However, signatures are the most non-intrusive form of biometric technique with which people identify themselves in administrative institutions and financial transactions in our everyday lives.

As technology develops and the virtual world becomes part of our everyday lives, online signatures are becoming more common. The two methods through which digitization is bringing changes to signature are online and offline methods of verification. Signing using tablets and smartphones are becoming increasingly popular and it is becoming essential to determine whether these are verifiable.

### **2.2.2 Signature Verification Identification**

Verification is the process of establishing validity whereas identification is the process of recognizing the origin. For both verification and identification, biometrics play a vital role. While signatures are not as unique as biometric ways of identification such as fingerprint, iris scanning, they can be verified in other ways. It is more of a behavioral form of verification. Therefore, verifying it dynamically has stood to be of more importance. The problem that lies here is to identify between the actual verified signature of a person and the forged signature. Therefore, while verifying we need to make sure that some certain characteristics of the original signature remain intact which can be identified dynamically and differ from person to person through psychological and physiological differences. This will result in identifying which of the signatures are forged.

### **2.2.3 Comparing Online and Offline Signature Verification**

Offline verification includes taking an image of a signature from a hard copy, such as paper and feeding it into a smartphone/tablet and processing it through the im-

age. This includes going through the characteristics of the signature from its stable components such as its shape. Online Signature Verification is more dynamic, as it captures the characteristics of the signature on a per-time basis, such as, during the time a person is signing using a stylus on a tablet. This includes velocity, pressure, acceleration, etc. Online verification captures more of the extra essence compared to offline as we can compare the eventual shape and also the dynamic characteristics.

## 2.2.4 Feature Types

In the case of online signature verification, there are two types of feature sets we can draw out and they can be divided in two methodologies as well. The methodologies are known as parametric and functional. The parametric method leads to using only global features of a signature. Global features are defined in relation to the parameters of the signature as a whole, such as the average time required for a signature to be written, and displacement, and there are several hundred parameters that can be considered with this case. With the parametric feature approach, it is more prone to errors because it does not consider the local features. The other approach is the functional approach which is more time-consuming in nature. It makes use of the local features of a signature, which means how a specific point in a signature behaves such as velocity, acceleration and direction of the pen movement and compares these features to that of a forged signature.

## 2.2.5 Mobisig Dataset

Mobisig is a publicly available database that consists of signatures that were drawn by fingers. This dataset was accumulated through 83 users, who signed on a touch-screen device. It was developed in 3 sessions which led to 45 original signatures and 20 skilled forgery signatures for each of the users. The mobisig database was tested using two methods, one that uses local features of a signature using a function-based approach and another that uses more global features with feature based approach. This dataset gives us the base of evaluating signatures on the same standard for comparing different algorithms.

Figure 2.1: Mobisig Data (Genuine Signature)

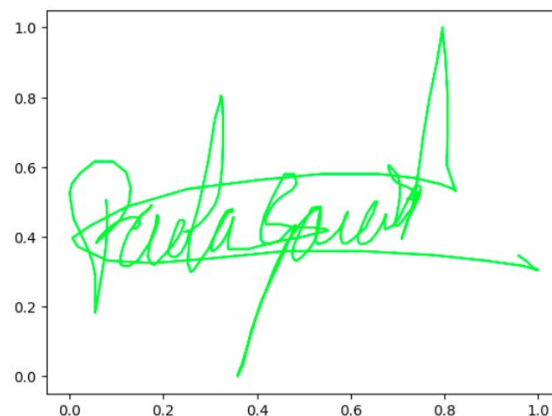
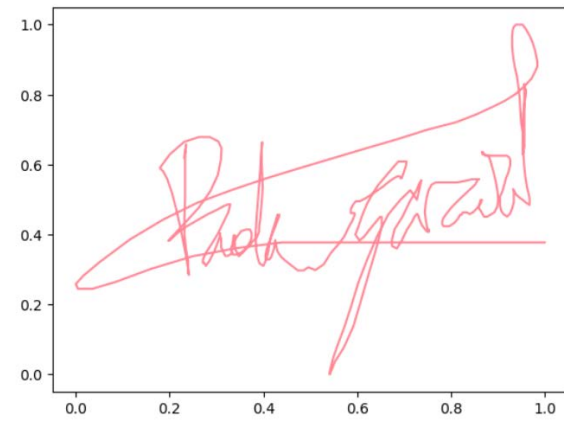


Figure 2.2: Mobisig Data (Forged Signature)



## 2.2.6 MCYT Dataset

The MCYT project was carried out by the Biometric Research Laboratory - ATVS, of the Universidad Politecnica de Madrid, which consists of a database that contains a set of signatures. It contains the details of signature traits. It is a multi-modal database containing:

- The number of individuals who signed
- The number of modalities per individual
- The number of samples for each modality

The online signature in this dataset was collected after each individual registered their fingerprints. The on-line signature was obtained using a graphics table, and this dataset was obtained by using a WACOM pen tablet and model INTUOS A6 USB. Each of the individuals provided 25 original signatures. On the other hand, 25 skilled forgeries were also made for each user. The skilled forgeries tried to imitate the static images of the signature to try to copy them with at least 10 attempts and then produced highly skilled forgeries.

Figure 2.3: MCYT Data (Genuine Signature)

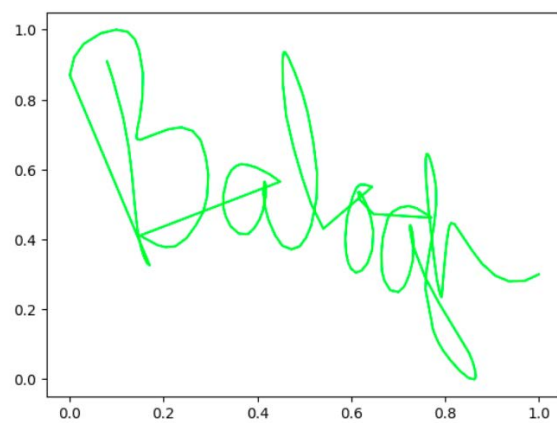
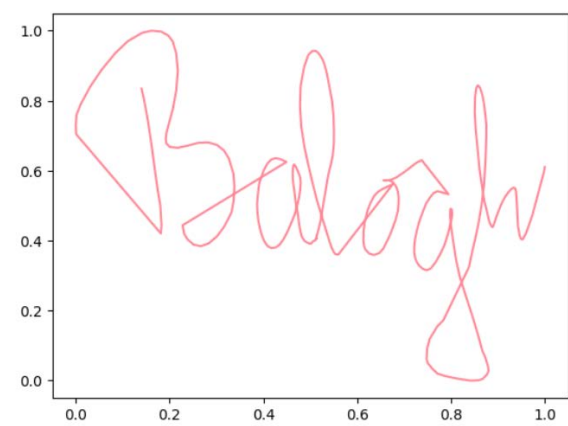


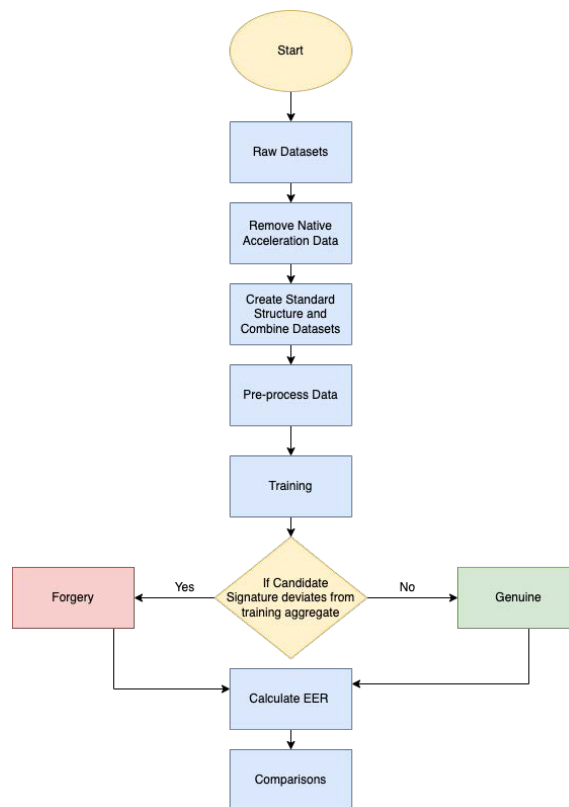
Figure 2.4: MCYT Data (Forged Signature)



# Chapter 3

## Implementation

Figure 3.1: Methodology



### 3.1 Methodology

The workflow consists of raw datasets namely Mobisig and MCYT datasets, that are publicly available datasets. Since both the datasets consisted of pen-tilt, acceleration and pen pressure data, we had to remove them since we are using a mobile device. We are checking for hand-drawn signatures on mobile devices and hence we do not need those features.

Since both the data sets had different properties and feature names and were in different formats, we standardized them to be digestible for our algorithm and stored

them as JSON for easy reading and writing. We also then combined them to form a larger data set with the same structure( Number of signatures).

To make the data ready for training, we derived more features as a feature engineering step, and then made a standard embedding of size  $x$ . The set of signatures for each signatory is then aggregated into a single model signature in the training step. Each of the signatories has its own unique model.

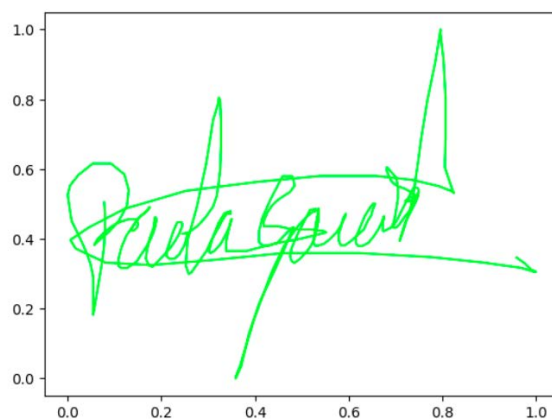
If one of the candidate's signatures deviates from the training aggregate model by a certain threshold, then we determine that signature as a forgotten signature, otherwise, it is a genuine signature.

To calculate EER, we manipulated the threshold value iteratively using the Newton-Raphson method to find a value for which the rate of false positive (FAR) and false negative (FRR) are equal across our entire combined dataset.

## 3.2 Datasets

Although there has been a large amount of research done on private signature databases, we are using a publicly available dataset. This is because we will not be able to compare the signature datasets on a public comparative basis. We are using two existing public databases for implementing our algorithm. We are using the Mobisig database and MCYT database. Both datasets go through a similar process of collecting signatures from individuals over a period of time. They require the individuals to provide sets of their own signatures first, and then a collection of forged signatures are obtained. The forgers are provided with an image of the original signature and they are allowed to copy it more than once to make it as perfect as they want. All these signatures are then pre-processed and algorithms are implemented.

Figure 3.2: MobiSig: User 12, Signature 0 (Genuine)





### 3.3 Train-Test Split

The data-set is then split for training and testing, we are using 70% for the training set and 30% for the test set. The training set would be used for training our algorithm and the testing set would be used to test against the trained set.

### 3.4 Data Pre-processing

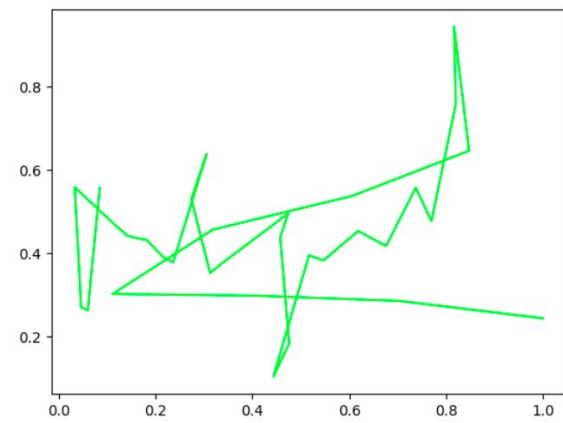
The data is first normalized, and all the x and y values are then converted from 0 to 1 for both MCYT and Mobisig datasets. The MCYT dataset did not contain any feature with the timestamp, however, the Mobisig contained a timestamp feature due to its hardware characteristics when collecting the signatures. For the MCYT dataset, we based the dataset by determining the sample rate was 100 samples a second.

We then straighten the points first before committing to the other steps in pre-processing; this is so that we do not lose the bounding box information for the original signature, often useful for visualization and visual confirmation by the original signature's owner.

We then categorized the signatures into those that are forged and those that are genuine signatures.

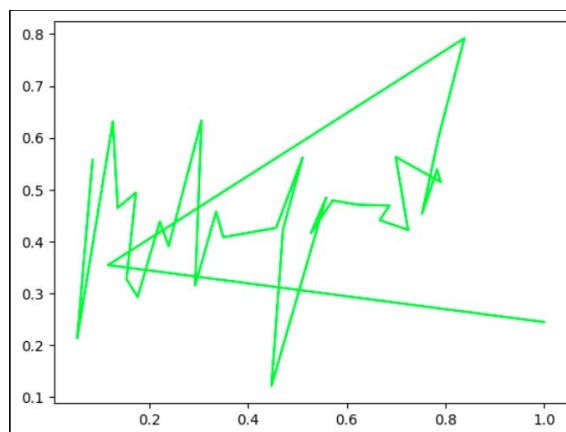
We then tagged each of the points of the signature by the distance traveled by the finger while drawing the signature using Euclidean distance in Cartesian co-ordinate plane. This is a new feature that we engineered to help us authenticate the original signature.

Figure 3.3: MobiSig: User 12, Signature 0, Domain: Distance, Reduced (Genuine)



We also then tagged each of the points of the signature by time duration. Since the MCYT dataset did not have any time stamp feature, we calculated 100 samples equal to 1 second.

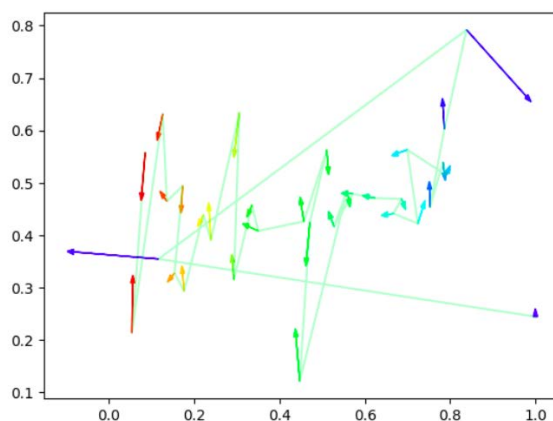
Figure 3.4: MobiSig: User 12, Signature 0, Domain: Time, Reduced (Genuine)



The signatures that are in the datasets could be any number of samples long so we formatted it to a standardized frame count. We created the sample twice, one for time and one for distance-based.

We also derived angle, speed and added them as features for both datasets. Then, we derived the acceleration, angular change, and angular velocity.

Figure 3.5: MobiSig: User 12, Signature 0, Domain: Time, Reduced, Velocities (Genuine)



## 3.5 Training

For training the dataset, we took the genuine signatures of each signatory and compared them with all the signatures of that specific signatory by finding out the difference in all the combinations of his signatures. We have created a histogram to find out at which point a signatory makes how much distance. In other words, which part of the signature tends to be more different, and which part tends to be more similar. We took all the differences and calculated the mean and median for each of the differences in the features.

Figure 3.6: MobiSig: User 12, Signature 0, Domain: Time, Reduced, Accelerations (Genuine)

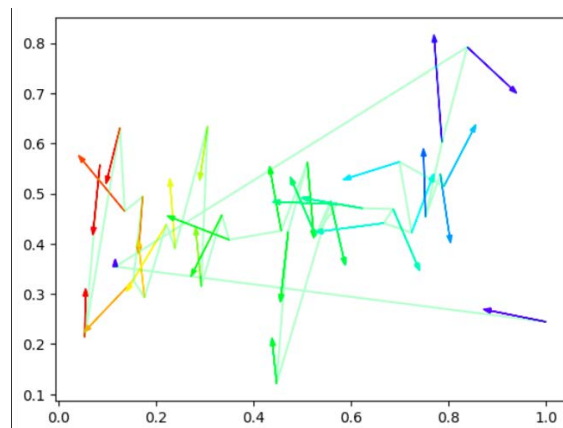
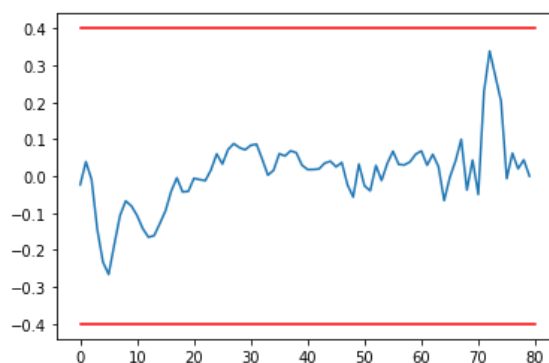


Figure 3.7: Variance at specific points of user own signature



## 3.6 Inference

For each feature, we then subtracted the mean and median from the corresponding feature from the test signature set. We then check to see whether the resulting difference between each feature overcomes a certain threshold,  $t$ . If the difference overcomes the threshold, it is fake and if below or equal to the threshold, then it's a genuine signature.

## 3.7 Evaluation

Before we evaluate, we pick a random threshold. We then run the inference function for every signature in the test set and we tally up to observe how many signatures result in false positives and how many result in false negatives. This is where we derive the FRR and the FAR.

The graph below shows that the intersection point between the FRR and the FAR function. This is our threshold. This is determined with the help of Netwon Raphson Method. The FRR and FAR functions are not fully linear, they are approximately exponential, therefore we used this method to determine the threshold.

Figure 3.8: Threshold vs FRR, FAR - Mobisig

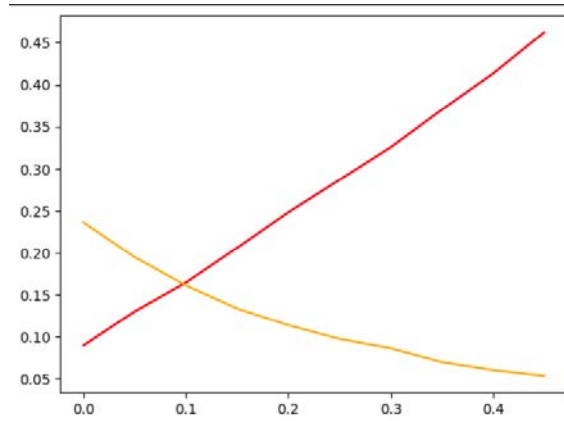


Figure 3.9: Threshold vs FRR, FAR - MCVT

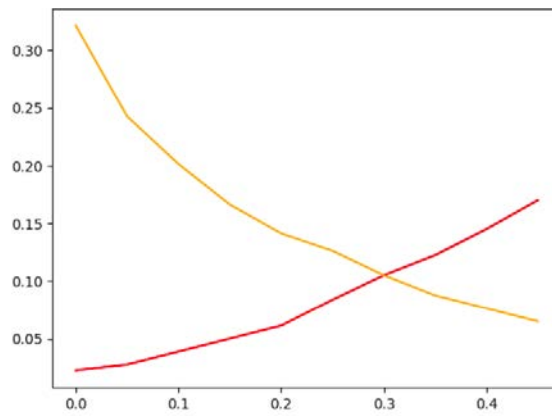
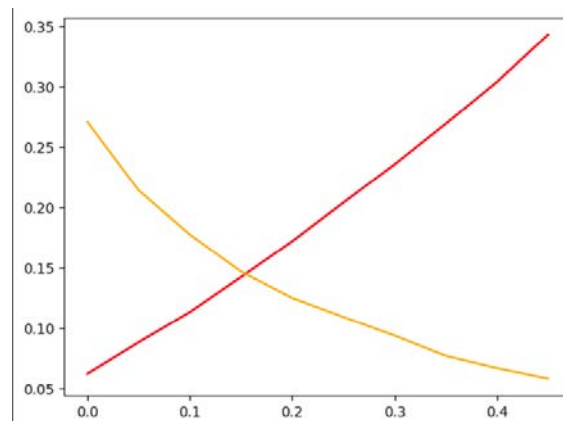


Figure 3.10: Threshold vs FRR, FAR - MCVT + MobiSig



# Chapter 4

## Result and Analysis

Algorithms	MCYT(EER (%))	Mobisig (EER (%))
Signpin	8%	20%
Deep Learning Method	13.3%	22.3%
Stroke-based RNN	10.46%	16.8%

We achieved an EER percentage rate of 8% for MCYT Dataset whereas for Mobisig Dataset we achieved a EER of 16.8%. For the MCYT Dataset, we achieved a better result compared to the Stroke-based RNN itself.

We have several operational advantages compared to existing algorithms. Our signatures can be collected using low end devices. In the pre-processing stages, we normalize all signatures in the same sampling size. Other programs require high-end devices with high touch sampling rates. It takes only 5 ms to run an inference in the Intel i5 8th gen processor. So, inference can be run in very limited computational resources like system memory, processor and persistent storage.

Differences in devices used to collect signatures don't affect the performance of the algorithm because we are interpolating all signatures into a standard size of  $6 \times 2 \times N$  vector. It allows us to get signatures from a web app. Also, different touch sampling rate doesn't cause performance issues.

Our algorithm has better signatory awareness. It can be trained by only 10 signatures of a signatory. Personal error rates are also taken into account in the SignPin algorithm. The baseline of all signatures is calculated for all metrics in two different domains. We are using 6 metrics over two domains:

Metrics:

- Cartesian Coordinates (x, y values)
- Stylus/Finger Travel Angle (derived) - determined slope with next data point
- Stylus/Finger Travel Speed (derived) - Normalized based on time and distance, then determined speed at every point.
- Styles/Finger Acceleration (derived)
- Stylus/Finger Angular Velocity (derived)

- Stylus/Finger Angular Acceleration (derived)

Domains:

- As a function of travel distance.
- As a function of elapsed time.

# Chapter 5

## Conclusion

### 5.1 Conclusion

To sum up, our approach to verifying signatures have been successfully reached the target we planned. Our main goal was to make a very handy and portable system to verify signatures on the go, instant and reliable verification, and allow businesses to go paperless. In this research, we have created an algorithm with medium-level accuracy but allowing businesses to get rid of the papers. It has addressed the very real issues that will be able to create a great impact in the online signature verification use cases. For example, data collection has a major bottleneck in that it requires high-end devices. Our algorithm can treat signatures from variable types of devices similarly and process them accordingly. It reduces a huge hardware cost. Our attempt to make a computationally cheap algorithm also brought good success.

Signature verification is very relevant for verification processes like contract papers, cheques, legal documents, etc. These types of contracts and authentication will still depend on signature verification for security. This research can make a good step ahead to make this possible.

### 5.2 Future Work

Some improvement updates can make our research very impactful. Our algorithms can visualize which part of the signature is too different. This will be very helpful for the manual verifier. Some improvements will be able to increase the accuracy of each signatory as well.

Using our own signature preprocessing system will reflect that it can meet the business need of different types of devices with different sampling rates. Our algorithm is computationally cheaper than all other algorithms, allowing businesses to make it cheaper to install and implement. Other papers didn't include the necessary computational resources, so we don't have the option to make a comparison about the computational resource. But we know that it is very important to the business. Because it reduces the necessity of expensive servers and hardware for the end-users.

It is also possible to make a Software-as-a-Service, which can be used by multiple companies at once. There are several companies like HelloSign, DocuSign. We can bring some changes in the data collection processes that will allow us to get a better insight into the behavioral pattern.



# Bibliography

- [1] M. Khan, M. Niazi, and M. Khan, “Velocity-image model for online signature verification,” *IEEE Transactions on Image Processing*, vol. 15, no. 11, pp. 3540–3549, 2006. DOI: 10.1109/TIP.2006.877517.
- [2] M. Parodi and J. C. Gómez, “Legendre polynomials based feature extraction for online signature verification. consistency analysis of feature combinations,” *Pattern Recognition*, vol. 47, no. 1, pp. 128–140, 2014, ISSN: 0031-3203. DOI: <https://doi.org/10.1016/j.patcog.2013.06.026>. [Online]. Available: <https://www.sciencedirect.com/science/article/pii/S0031320313002781>.
- [3] M. Peterson, “82 percent of companies still spending billions on paper,” *Corp Magazine*, 2015. [Online]. Available: <https://www.corpmagazine.com/industry/technology/82-percent-companies-still-spending-billions-paper>.
- [4] L. G. Hafemann, R. Sabourin, and L. S. Oliveira, “Offline handwritten signature verification — literature review,” in *2017 Seventh International Conference on Image Processing Theory, Tools and Applications (IPTA)*, IEEE, Nov. 2017. DOI: 10.1109/ipta.2017.8310112. [Online]. Available: <https://doi.org/10.1109%5C%2Fipta.2017.8310112>.
- [5] C. Li, X. Zhang, F. Lin, *et al.*, “A stroke-based rnn for writer-independent online signature verification,” in *2019 International Conference on Document Analysis and Recognition (ICDAR)*, 2019, pp. 526–532. DOI: 10.1109/ICDAR.2019.00090.
- [6] “57 essential e-signature statistics: 2021 market share analysis data,” *Finances Online*, 2020. [Online]. Available: <https://financesonline.com/25-essential-e-signature-statistics-analysis-of-trends-data-and-market-share>.
- [7] B. FELIX, “82 percent of companies still spending billions on paper,” *LunarPen*, 2020. [Online]. Available: <https://lunarpen.com/blog/tag/electronic-signature-statistics>.
- [8] Adobe, “Accelerate your sales performance: Believe it, e-signatures can transform your business,” *Forbes Insights*, 2021. [Online]. Available: [https://www.forbes.com/forbesinsights/adobe\\_e-signatures/index.html](https://www.forbes.com/forbesinsights/adobe_e-signatures/index.html).
- [9] P. B, S. K, and B. Y, “Digital signature market by component (hardware, software, and services), deployment model (on-premises and cloud), and industry vertical (bfsi, education, human resource, it telecommunication, government, healthcare life science, real estate, and others): Global opportunity analysis and industry forecast, 2021-2030,” *Allied Market Research*, 2021, ISSN: 0031-3203. [Online]. Available: <https://www.sciencedirect.com/science/article/pii/S0031320313002781>.

- [10] I. Group, “Signature verification market: Global industry trends, share, size, growth, opportunity and forecast 2022-2027,” *IMARC Group*, 2021. [Online]. Available: <https://www.imarcgroup.com/signature-verification-market>.