ACADEMIC RESEARCH POSTER TEMPLATE

DeepSign - Deep Online Handwritten Signature Verification

Sai Abhinav Reddy Badinehal and Sai Sandeep Lankisetty

Introduction

Verifying online handwritten signatures is a challenging task. Moreover, applying Deep learning to it makes it more difficult as there is lack of publicly available data. So, to overcome this problem we are using TA-RNN deep learning method which creates robust models against skilled forgeries.

TA-RNN Method

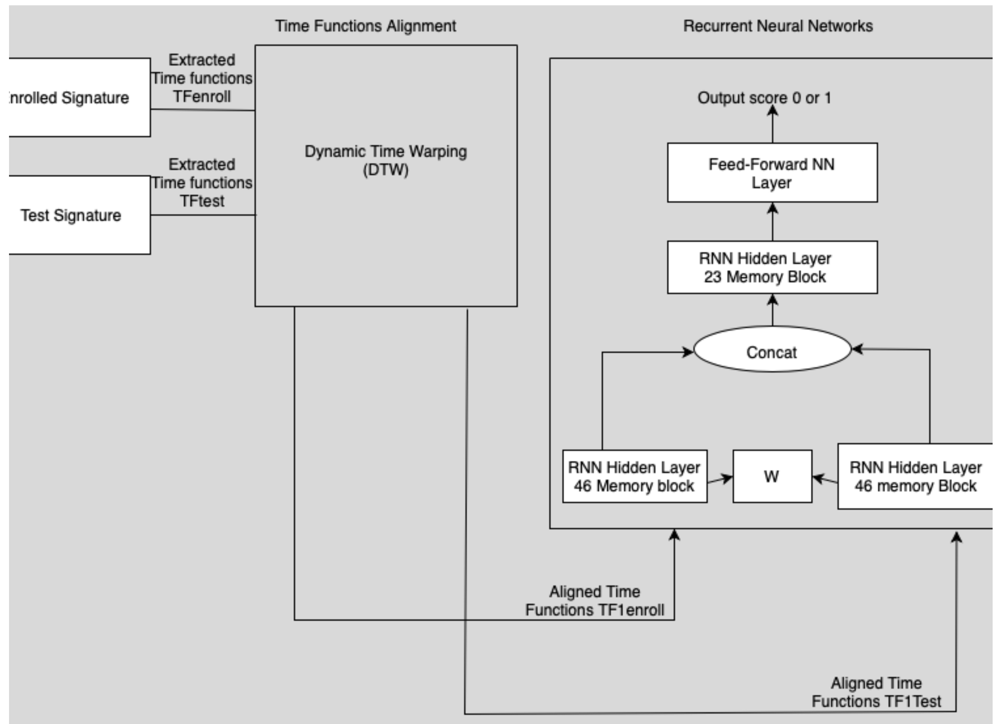
This Approach takes the input signatures and extract their temporal dynamics and do the following

Time Functions Alignment

- DTW is used here to optimally wrap time functions along time axes to calculate similarity.
- Now this is sent to RNN's to extract more meaningful features.

Recurrent Neural Networks

- First layer has two parallel BGRU hidden layer.
- Second layer has one BGRU hidden layer.
- Final layer is feed forward Neural Network layer with sigmoid activation.
- Output Score of 0 or 1 to tell its genuine or forgery.



TA-RNN Architecture.

MOBISIG Data Analysis

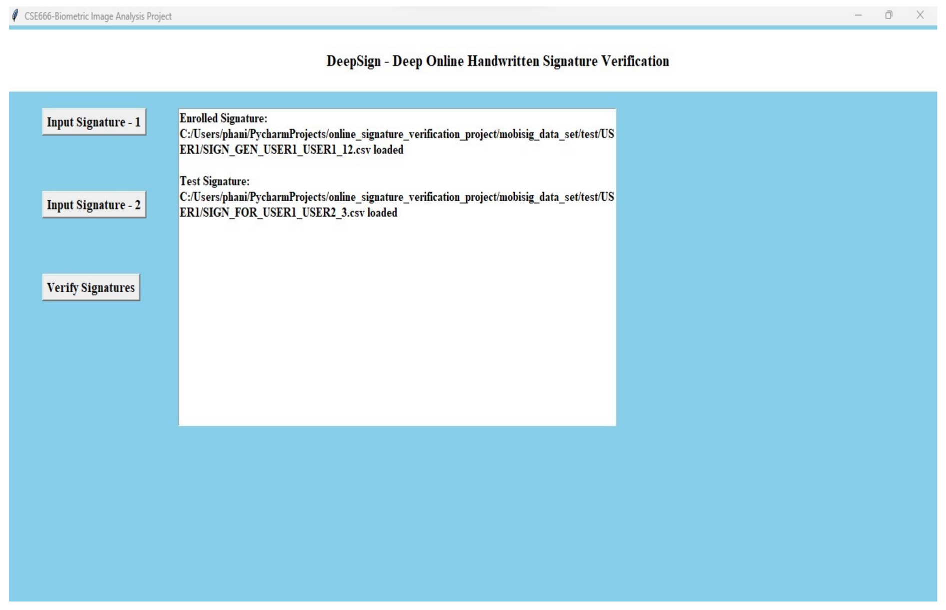
This dataset contains of 83 Users. Each users has 65 signatures.

- In those 65 signatures 45 are genuine and 20 are forgery signatures.
- These signatures are recorded in interval of 3 sessions.
- In each session 15 genuine signatures are recorded and in last 2 sessions 10 each forgery signatures are recorded.
- The dataset file contains below temporal dynamics of 13 different discrete values.

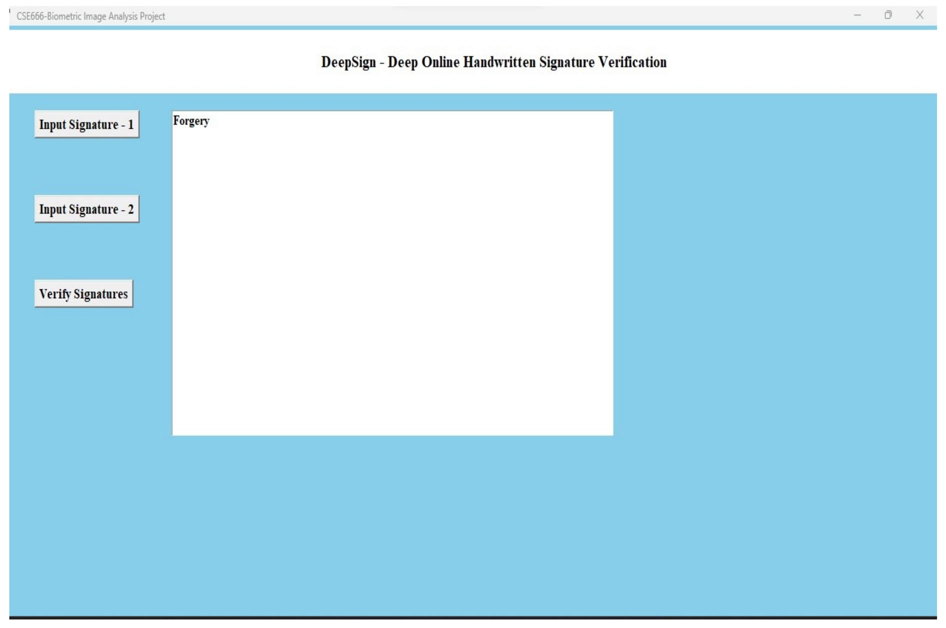
Number	Features
1-2	X,Y-coordinate
3	Pen- pressure
4	Time stamp
5	Finger area
6-7	Velocities-X,Y
8-10	Acceleration-X,Y,Z
11-13	Gyroscope-X,Y,Z

Study	Classifiers	Database		Experimental Protocol			Performance in EER
		Name	#Users	#Train Users	Input	#Train Sig.	
Lai and Jin (2018)	GARU + DTW	Mobisig	83	70	Finger	5	Skilled = 10.9%
Li et al. (2019)	LSTM	Mobisig	83	70	Finger	1	Skilled = 16.1%
R. Tolsana(2021)	TA-RNN's	DeepSignDB	1526	1084	Finger	1	Skilled = 13.8%
						4	Skilled = 11.3%
Our Work	TA-RNN's	Mobisig	83	70	Finger	4	**Skilled= 9.03%**

State of Art comparisons



Testing comparisons on unseen data

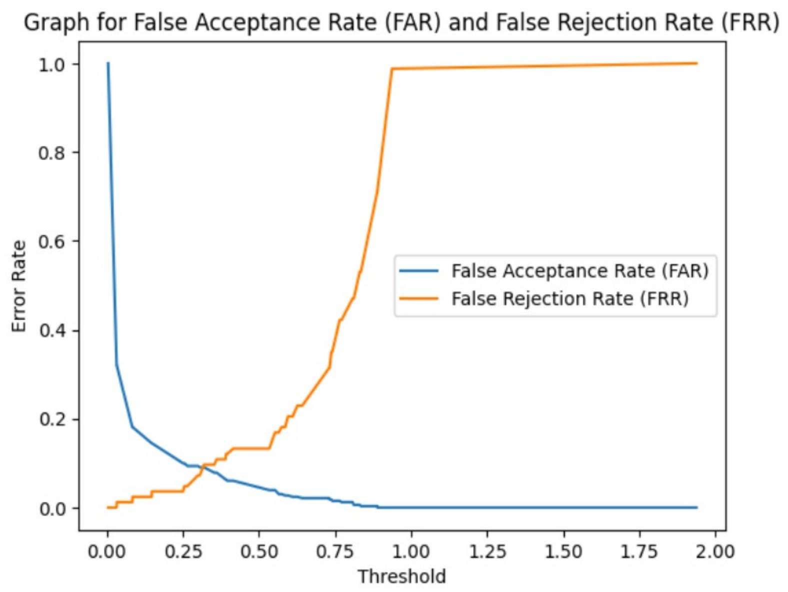


Output of comparisons

Results

Experimental Protocol:

- Here we divided no of users into development 70 and test 13 users.
- Then we are randomly taking 4 training signatures per user which means 4 genuine and 4 forgery signatures per user.
- Next, we are doing genuine-genuine comparisons and genuine- forgery comparisons
- Finally, the unseen data of test users is verified to check accuracy of model.



Experimental Results

After performing the experiment as described in the above protocol. We calculated EER with those 4 training samples which resulted in 9.03% EER. With fewer training samples we were able to achieve lower EER when compared with the state of art. The comparisons are tabulated as in table and then in case of test users we use them to check how well our model is able to predict genuine and forgeries on unseen data. The figures for them are shown above.

Conclusion

.We have performed author claimed TA-RNN approach on mobisig database. Our primary goal is as follows :

- In authors work on DeepSign they were able to outperform many stylus case scenarios but not finger scenarios.
- We wanted to improve the performance in case of finger scenarios by pretraining the model to create robust system against skilled forgeries.
- So we chose mobisig dataset and applied author proposed TA-RNN to it.
- Finally, we were able to achieve some low EER rate when compared with previous state of art and model prediction on unseen data is accurate.

Future Scope

- Use the model trained for transfer learning approaches because the publicly available data is scarce.
- TA-RNN approach can be used in key stroke biometrics, neuro-metric related tasks.

References

1. Exploring Recurrent Neural Network by R.tolosana
2. Recurrent adaptation networks for online signature verification by Lai and Jin.
3. Online signature verification using deep learning and feature representation using legendre polynomial coefficients by A.Hefny
4. A stroke-based RNN for writer-independent online sig-nature verification by Li