

DeepSign: Deep On-Line Signature Verification

Authors - Ruben Tolosana, Ruben VeraRodriguez, Julian Fierrez, Javier Ortega-Garcia

The verification of handwritten signatures, the amount of publicly available data is scarce, which makes it difficult to test the real limits of deep learning. In addition to the lack of public data, it is not easy to evaluate the improvements of novel proposed approaches as different databases and experimental protocols are usually considered. The main contributions of this study are –

- 1) Authors provided an in-depth analysis of state-of-the-art deep learning approaches for on-line signature verification.
- 2) They present and describe the new DeepSignDB, on-line handwritten signature biometric public database. This database is obtained through the combination of some of the most well-known databases. It comprises more than 70K signatures acquired using both stylus and finger inputs from a total 1526 users. Two acquisition scenarios are considered, office and mobile, with a total of 8 different devices. Additionally, different types of impostors, number of acquisition sessions and forgery samples are considered.
- 3) They proposed a standard experimental protocol and benchmark to be used for the research community in order to perform a fair comparison of novel approaches with the state-of-the-art architectures.
- 4) Time-Aligned Recurrent Neural Networks was proposed for this. This approach combines the potential of Dynamic Time Warping and Recurrent Neural Networks to train more robust systems against forgeries. TA-RNN system outperforms the state of the art, achieving results even below 2.0% EER when considering skilled forgery impostors and just one training signature per user.

POINTERS –

- 1) 23 time-functions were extracted using X and Y spatial coordinates and pressure of each signature.
- 2) Dynamic Time Warping DTW was applied in order to convert the 23 original time functions into 23 pre-aligned time functions before introducing them to the RNNs.
- 3) The proposed TA-RNN system could extract more meaningful features as time sequences. All the 23 time-functions per signature, DTW were used as input of the network. The first layer of the network was composed of 2 Bi-Directional Gated Recurrent Unit (BGRU) hidden layers with 46 memory blocks, with shared weights.
- 4) For the second input layer, the 1st two parallel BGRU hidden layers were used. For the final layer, a feed-forward neural network layer with a sigmoid activation was used.
- 5) The DeepSignDB database was used, which was divided into train (70%) and test (30%) dataset. Both RNN and TA-RNN systems were implemented using Keras framework using TensorFlow as the back-end.

PERFORMANCE –

- 1) **STYLUS WRITING INPUT SCENARIO** - Analysing skilled forgeries, TA-RNN approach outperforms everyone. For the scenario of considering just 1 training signature per user, TA-RNNs achieves an absolute improvement of 7.0% and 4.3% EERs compared with the DTW and RNN systems, respectively. writer-independent TA-RNN approach shows a high ability to generalise well along different scenarios, users, and devices, achieving EERs even below 2.0% in challenging scenarios where dynamic skilled forgery impostors and just one training signature per user are considered. Similar results are obtained for the scenario of increasing the number of training signatures to 4. TA-RNNs achieves an absolute improvement of 6.0% and 4.6% EERs compared with the DTW and RNN systems, respectively. Upon analysing the random forgery results. Similar results are observed among the DTW and TA-RNNs. For the case of using just 1 training signature, TA-RNNs is able to outperform the robust DTW in 5 out of 9 different datasets, achieving a final 1.5% EER for the whole DeepSignDB evaluation dataset, an absolute improvement of 0.3% EER compared with the DTW system. This result improves further when number of training signatures is increased to 4, with EERs very low.
- 2) **FINGER WRITING INPUT SCENARIO** – TA-RNNs performed better than DTW and RNNs. For the scenario of considering just 1 training signature per user, TA-RNNs achieved 2.8% and 4.8% EERs compared to DTW and RNN system. In the case of random forgeries, the DTW system slightly performed better than the proposed TA-RNN system.

FUTURE PROSPECTS –

- 1) Performing a fair comparison of the state-of-the-art architectures
- 2) Evaluating limits of these architectures
- 3) Carrying out exhaustive analysis of finger input scenario.