Online signatures are acquired using a digital tablet which provides all the trajectories of the signature, as well as the variation in pressure with respect to time. Therefore, online signature verification achieves higher recognition rates than offline signature verification. Nowadays, forensic document examiners distinguish between forgeries, in which an impostor tries to imitate a given signature of another person and disguised signatures, in which the authentic author deliberately tries to hide his/her identity with the purpose of denial at a later stage. The disguised signatures play an important role in real forensic cases but are not considered in recent literature.

In this study, we used online signatures acquired using a WACOM Intuos4 digitizing tablet with a sampling rate of 200Hz, a resolution of 2000 lines/cm and a precision of 0.25mm. The pressure information is available in 1024 levels. Online signatures contain a set of samples, each sample corresponds to the point coordinates on the digitizing tablet along with the corresponding pressure (Xt; Yt; Pt) where t corresponds to time. From those three basic signals, four other are extracted: distances, angles, speeds and angular speed. In order to compare the questioned signature with the reference signature, the differences between their corresponding features are computed at both the signal level and the histogram level.

This study has been evaluated on ICDAR2009 signature verification competition dataset and a new dataset of online signatures collected at Qatar University (QU-dataset). This dataset contains signatures of genuine signatures, forgeries and disguised of 194 persons. To the extent of our knowledge, this dataset is the only one that contains disguised online signatures. The best individual performing feature for the ICDAR2009 dataset is the pressure histogram difference which reaches 8% equal error rate (EER). The pressure signal difference is the best individual performing feature for the QU-dataset (29% EER). The combination of features led to 7% EER on the ICDAR2009 dataset and 22% EER on the QU-dataset.

This online signature verification system deals with both forgeries and disguised signatures. Several features have been proposed and combined using different classifiers reaching promising performance for disguised signatures detection.