L-Labs (2023), **confidential**, 1–1

ARTICLE TYPE

Secure Signature

Abstract

This project's goal was to devise an impregnable electronic signature validation system for end devices, primarily tablets. Although signature-based authentication is widely used, vulnerabilities still persist. To address this, our solution utilizes a recurrent neural network (RNN) model, capturing signature dynamics like location and pressure, contrary to conventional image processing methods that are still widely used in the field, and are susceptible to orchestrated noise attacks. Statistical analysis of the resultant model demonstrates an impressive 18-fold error rate improvement compared to the client's initial solution.

The Problem

A signature serves as a biometric credential for validating an individual's identity and confirming the acknowledgment or endorsement of a document. Despite the proliferation of digital security measures, signature-based authentication remains prevalent in the 21st century. Thus, our client requested us to develop a novel solution to electronically validate a signature in an end device (i.e., tablet) in such a manner that a professional attacker would not be able to hack it.

The Solution

Our research endeavors unveiled that the prevailing paradigms for signature authentication predominantly revolve around image processing techniques. However, this approach has a notable susceptibility within the method itself – the susceptibility to orchestrated perturbations introduced as specific noise into the image. This revelation underscored the potential for hackers to exploit this vulnerability to compromise the integrity of the authentication process. Subsequent consultation with experts specializing in art and its authentication corroborated our findings, accentuating that the signature, while a visually discernible element, is essentially an outcome of the signing process intricacies. Consequently, this realization shifts the focus from the superficial analysis of the signature image to delving into the underlying dynamics of the signing procedure. This implies that authenticating the signer's identity goes beyond mere image recognition; it necessitates a comprehensive comprehension of the physiological and behavioral nuances embedded in the act of signing itself. This insight underscores the urgency of adopting a holistic approach that encompasses not only the visual elements but also the multifaceted aspects of the signing process to bolster the robustness and security of signature authentication systems. To this end, we used a recurrent neural network (RNN) based model to capture the location, pressure, and other metrics of the signing process over time and matching them to a set of previously available samples.

The Outcome

Comparing the obtained results to the solution the client had before the project, we statistically reveal a 18-fold improvement in the error rate of the proposed model.