

Identificación de contraseñas manuscritas sobre pantallas táctiles



Cristian Rodríguez Rodríguez

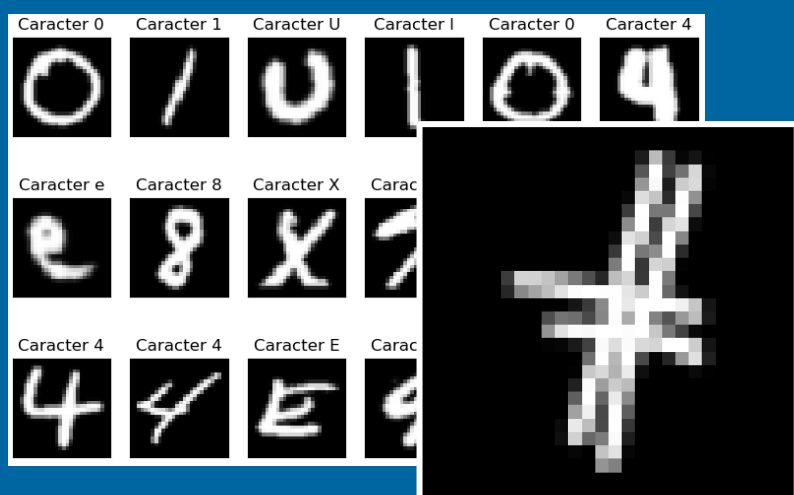
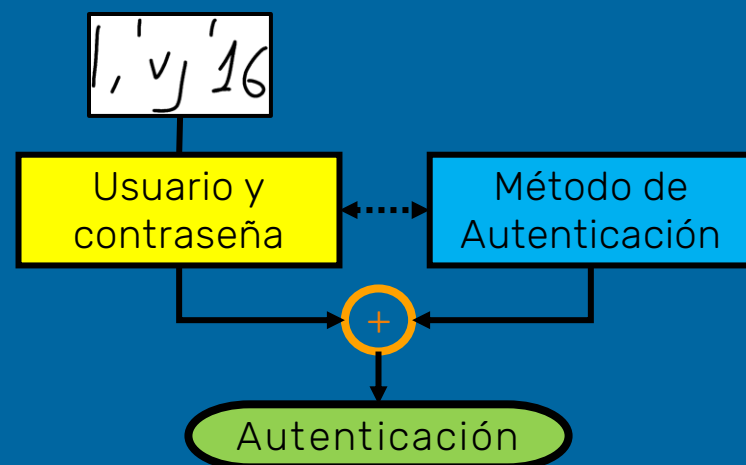
Carlos M. Travieso González

Máster Universitario en Ingeniería de Telecomunicación, diciembre 2023

Introducción y objetivos

El proyecto se centra en la implementación de un sistema de autenticación basado en técnicas de Aprendizaje Automático (AA). El objetivo es la verificación de contraseñas manuscritas en pantallas táctiles.

El sistema se compone por dos subsistemas. Un primer subsistema se encarga del Reconocimiento Óptico de Caracteres (OCR). Mientras que el segundo se encarga de autenticar biométricamente la autoría del usuario.



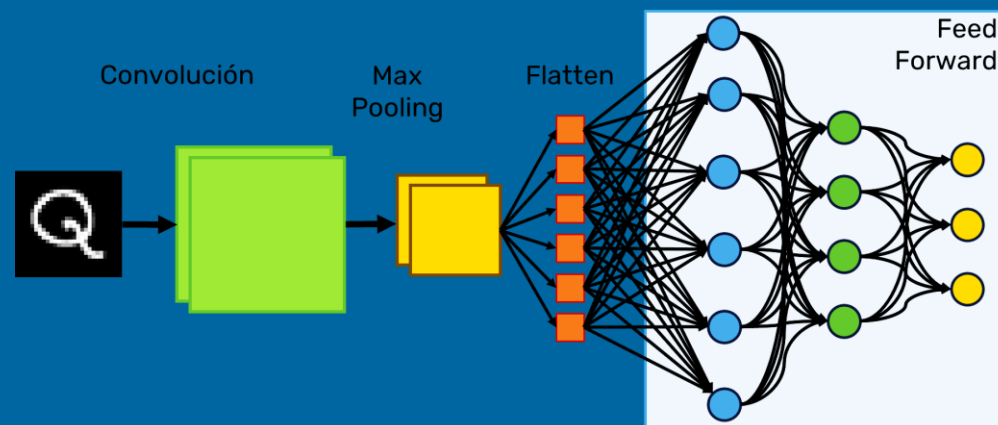
Metodología

El sistema se construye sobre dos bases de datos, una de contraseñas y otra de impostores. De estas contraseñas se extraen los caracteres de manera independiente para poder identificarlos con el OCR.

El sistema de OCR se validará midiendo la precisión mientras que el detector de intrusos se medirá con la precisión y con la tasa de error igual (ERR).

Se han validado modelos de AA (kNN, SVM, Random Forest y Naive Bayes) para entrenar el sistema, permitiéndole aprender patrones y características únicas de la escritura.

Posteriormente, se han validado técnicas de Aprendizaje Profundo (DL), Feed Forward, Convolutional Neural Networks (CNN), para mejorar la capacidad de generalización del OCR ante escrituras más complejas.



Resultados y conclusiones

Se ha realizado un ajuste de hiperparámetros de todos los modelos de AA y DL validados y utilizado técnicas de validación cruzada para obtener el valor más realista posible.

La extracción de los caracteres tiene un 88,67% de acierto provocado a unos errores que se han catalogado. El OCR presenta una precisión del 94,5% con potencial de crecimiento ajustando ciertos parámetros identificados de la base de datos. El detector de intrusos presenta una precisión del 99,65% con una EER de 0,00155.

El sistema desarrollado en este proyecto es un sistema muy robusto frente a falsificaciones, pero con problemas a la hora de detectar las contraseñas.