UNIVERSIDAD GALILEO

FACULTAD DE INGENIERÍA DE SISTEMAS, INFORMÁTICA Y CIENCIAS DE LA COMPUTACIÓN



**DOCUMENTACIÓN**

**SIGNATURE FORGERY DETECTION**

KEVIN JOSÉ HERNÁNDEZ MARROQUÍN

CARNÉ 17001095

SEMINARIO PROFESIONAL II

OCTAVO SEMESTRE

GUATEMALA, XX DE YY DE 2020

**Índice**

[Introducción 2](#_Toc47281805)

[**¿Cuál es el Problema?** 2](#_Toc47281806)

[**¿Cuál es la solución?** 2](#_Toc47281807)

[Objetivo General 3](#_Toc47281808)

[Objetivos Específicos 3](#_Toc47281809)

[Retos, Limitaciones y Problemas 4](#_Toc47281810)

[Approaches 5](#_Toc47281811)

[Modelos Propuestos 6](#_Toc47281812)

[Links 7](#_Toc47281813)

[References 8](#_Toc47281814)

# **Introducción**

## **¿Cuál es el Problema?**

La falsificación ha sido un problema acarreado desde la antigüedad. Desde falsificar el oro hasta hoy en día en falsificar firmas y otros artefactos de gran valor.

Entre estos objetos de valor, se pueden encontrar como guitarras firmadas por grandes guitarristas, y solo con el hecho de tener su firma su precio en el mercado es bastante elevado; lo mismo sucede con otros objetos cuyos precios tienen la misma naturaleza.

A veces los estafadores replican esas firmas con tal de ganar mucho dinero y eso perjudica a los vendedores.

En otros casos, la falsificación de la firma puede llevarse a tal extremo de consumar contratos en nombre de otra persona con el fin de perjudicarla.

La única forma de corroborar la veracidad de la firma es la palabra de un experto (en caso de objetos de valor) o la palabra de la persona portadora.

## **¿Cuál es la solución?**

Una solución para detectar si la firma fue falsificada, es por medio de una máquina, es decir, por medio de AI.

Dado que un AI observa los objetos de manera objetiva aplicando la matemática, nunca dará un veredicto sesgado o influenciado por opiniones subjetivas.

Además, un AI puede extraer características latentes y detectar patrones que no son obvias para el ojo humano, entonces pueden ser una herramienta útil a la hora de analizar una firma en cualquier situación.

# **Objetivo General**

Diseñar una aplicación móvil que posibilite la discriminación entre firmas auténticas y falsificadas.

# **Objetivos Específicos**

* Investigar proyectos similares previamente publicados.
* Consultar asesores para tomar las mejores decisiones.
* Diseñar una aplicación móvil empleando Flutter y Firebase.
* Diseñar una arquitectura orientado a Deep learning que pueda discriminar entre firmas auténticas y falsificadas

# **Retos, Limitaciones y Problemas**

Los retos en el desarrollo de este proyecto son:

* Conseguir datasets bastantes amplio para el problema.
* Escoger un modelo óptimo y posteriormente mejorarlo.
* Tener un accuracy muy alto.
* Garantizar que se equivoque en lo menos posible a la hora de someterse a nuevas firmas.
* Escalabilidad.

Los problemas potenciales detectados son:

* El mantenimiento.
* Deployment del proyecto.
* Tiempo de entrenamiento del modelo.
* Encontrar o implementar una interfaz que logre comunicar al usuario con el modelo AI.
* Mecanismos de seguridad.
* Pocos simples de entrenamiento.
* Estandarización de las imágenes.
* Procesamiento de las imágenes

Las limitaciones analizadas son las siguientes:

* Tiempo de trabajo limitado a 6 meses o menos.
* El poder computacional disponible.
* Compatibilidad entre versiones.
* La carga de trabajo de los otros 5 cursos del octavo semestre.
* Limitado a los approaches de: Writter-Dependent y Writter-Independent
* Trabajar en márgenes donde el capital financiero invertido es de $0.00.

# **Requerimientos**

## **Requerimientos de Usuario**

* Registrar usuarios y sus respectivas firmas.
* Tomar fotos de las firmas empleando el teléfono móvil.
* Enviar fotos de las firmas al AI para su evaluación de autenticidad.
* Clasificar firmas en: **auténticas** o **falsificadas**.

## **Requerimientos del Sistema**

* El modelo AI debe tener un accuracy arriba del 80%.
* Debe ser escalable.
* La interface debe ser User Friendly.
* El backend debe ser robusto.

# **Approaches**

* **Deep Learning:**

Es la opción más factible. Estos no necesitan de datasets de entrenamiento amplios y pueden ser muy efectivos al encontrar patrones de datos que no conocen.

* + **One Shot Learning:**

Modelos candidatos: Siamese Networks y Matching Networks.

Son redes optimizadas para encontrar características latentes de imágenes. Lo característico de estas redes es que pueden dar criterios en base a un solo sample.

* + **K Shot Learning:**

Modelos candidatos: K Nearest Neighborhood, Gaussian Prototypical Neural networks, Meta Transfer learning, Bayesian program Learning y Hierarchical Bayesian.

Son redes que tienen muy buen desempeño al darles una cantidad muy reducida de samples.

* **Machine Learning:**

Es la opción menos considerada. Debido a las restricciones impuestas por la naturaleza del problema no es una solución factible. Los modelos de este tipo necesitan un dataset de entrenamiento bastante amplio con una cantidad numerosa de samples por cada categoría. Además, no son escalables y se deben de volver a entrenar por cada nueva clase que se introduce.

# **Modelos Propuestos**

* Generative Adversarial Neural Networks.
* CNN architectures:
  + LetNet
  + AlexNet
  + VGG16
  + VGG19
  + Google Inception
  + Hierarchical Bayesian Program Learning
  + Resnet:
  + Gaussian Prototipycal Neural Networks:
    - <https://arxiv.org/pdf/1812.02391v3.pdf>
    - Stronger than Prototypical Networks
    - Has a trustworthy range (overcomes variance)
    - Meta Learning:
      * Accumulate experience from learning multiple tasks
      * Helps deep neural nets converge faster while reducing the probability to overfit when using few labeled training data only
  + Siamese (One Shot Learning-Deep Learning Algorithm):
  + Prototypical Networks (Few shot learning-Deep learning Algorithm):

Disadvantages:

* + - Lack of Generalization
    - Use of mean to decide center and does not support variance

Advantages:

* + - Given K shots (samples), the AI tries to classify new data.

A partir de una observación, intenta extraer las características esenciales y en base a ello clasifica.

Referencias:

* <https://medium.com/@connorshorten300/one-shot-learning-70bd78da4120>
* <https://www.cs.cmu.edu/~rsalakhu/papers/oneshot1.pdf>
* SVM
* Random Forests
* XGBoost
* ResNet

# **Links**

Datasets:

* <http://www.iapr-tc11.org/mediawiki/index.php/Datasets_List>
  + All Datasets
* <https://www.hackerearth.com/challenges/hackathon/axis-hackathon/custom-tab/resource-center/#Resource%20Center>
  + 98MBs
* <http://www.iapr-tc11.org/mediawiki/index.php?title=ICFHR_2012_Signature_Verification_Competition_(4NSigComp2012)>
* <http://www.vision.caltech.edu/mariomu/research.html>
* <http://www.iapr-tc11.org/mediawiki/index.php/Datasets_List>
* <http://www.iapr-tc11.org/mediawiki/index.php?title=ICFHR_2010_Signature_Verification_Competition_(4NSigComp2010)> (this one is currently used)

# **References**

* Marcus Liwicki, Muhammad Imran Malik , Linda Alewijnse, Elisa van den Heuvel, Bryan Found,. "ICFHR2012 Competition on Automatic Forensic Signature Verification (4NsigComp 2012) ", Proc. 13th Int. Conference on Frontiers in Handwriting Recognition, 2012