Máster en Técnicas Estadísticas

PROPUESTA DE TRABAJO FIN DE MÁSTER (Modalidad B)
Curso 2024-2025
MÁSTER EN TÉCNICAS ESTADÍSTICAS

Título	1. Estudio y desarrollo de adversarial attacks y mecanismos de defensa en redes neuronales convolucionales
Nombre de la Empresa **Tutor/a en la empresa** **Tutor/a académico/a**	GRADIANT, CENTRO TECNOLÓXICO DE TELECOMUNICACIÓN DE GALICIA Carmen García
Descripción del trabajo a realizar	Un ataque adversario consiste en modificar sutilmente una imagen original de tal manera que los cambios sean casi imperceptibles para el ojo humano. La imagen modificada se llama imagen adversaria y cuando se envía a un clasificador se clasifica erróneamente, mientras que la original se clasifica correctamente. Las aplicaciones de estos ataques en la vida real pueden ser muy graves; por ejemplo, se podría modificar una señal de tráfico para que un vehículo autónomo la malinterprete y provocar un accidente. En estas prácticas se trabajará en algoritmos del estado del arte en lo relativo a los adversarial attacks a CNNs, así como en mecanismos de defensa para evitar que un modelo pueda ser vulnerable e este tipo de ataques.
Recomendaciones	Conocimiento técnicos valorables phyton y conocimientos básicos de Machine y Deep Learning
Fechas de las practicas*	A convenir con el/la alumn@
Lugar de trabajo y horario*	Vigo, Pontevedra / horario a convenir con el/la alumn@.
Prácticas remuneradas	Marca con una x: ☐ Sí × ☐ No
Convenio	A través de la universidad

Otras observaciones	

* Campo obligatorio para prácticas no remuneradas