Financiado por la Unión Europea NextGenerationEU
Gobierno de España · Vicepresidencia Primera del Gobierno · Ministerio de Asuntos Económicos y Transformación Digital · Secretaría de Estado de Digitalización e Inteligencia Artificial
Plan de Recuperación, Transformación y Resiliencia
España | digital 2026
incibe_ Instituto Nacional de Ciberseguridad

Gonzalo de Francisco Rodríguez
presenta el resumen del trabajo

Técnicas de Inteligencia Artificial Supervisadas y No Supervisadas para el Análisis de Información Digital en Dispositivos de Almacenamiento

Luis Alberto Martínez Hernández,
Ana Lucila Sandoval Orozco,
Luis Javier García Villalba

Actas VIII JNIC, atlanTTic, 61-68, (2023).

28 de marzo de 2024

SERIE DE RESÚMENES EN ESPAÑOL

Palabras clave: Clasificación de Información, Dispositivos de Almacenamiento, Extracción de Entidades, Informática Forense, Inteligencia Artificial, NLP, Reconocimiento de Entidades, RoBERTa.

Introducción

EL auge de la tecnología en las últimas decadas ha supuesto un mundo cada vez más conectado a Internet, con el incremento de datos compartidos y descargados a través de la red que ello supone. Este aumento del flujo de datos atrae a cada vez más ciberdelincuentes, cuyo número de sospechosos ha crecido considerablemente en los últimos años. Es común que en las detenciones de estos sospechosos se incauten dispositivos tecnológicos que puedan contener pruebas para un delito, y es aquí donde entra en juego la informática forense, cuyo objetivo es la aplicación de técnicas científicas y analíticas especializadas en infraestructuras tecnológicas (como pueden ser ordenadores, smartphones, servidores o la red) que permiten identificar, preservar, analizar y presentar datos válidos dentro de un proceso legal.

1. Metodología

El análisis de los datos es el punto más crítico del proceso de investigación y el que conlleva más tiempo no solo por la variedad de formatos (audio, imagen, textos, vídeos, ...) a los que se enfrentan los investigadores, sino también por la gran cantidad de datos almacenados en los dispositivos incautados. Esto supone una tarea cada vez más ardua para los analístas, que deben buscar relaciones entre documentos para generar pruebas que puedan ser presentadas en un juicio. No obstante, el área de la inteligencia artificial ofrece diversas herramientas de las que los investigadores se sirven para automatizar este proceso.

En primer lugar, encontramos el área de investigación y desarrollo denominada Procesamiento del Lenguaje Natural (NLP, del inglés Natural Language Porcessing), que se centra principalmente en el análisis y la generación de lenguaje escrito y hablado. Su uso se ha extendido a diversos sectores profesionales con el objetivo de descubrir, clasificar, organizar o buscar contenidos de forma automática, lo que permite un uso más eficiente del tiempo, una reducción de costes y una ágil toma de decisiones. Una de las aplicaciones de la NLP son las herramientas detectoras de Reconocimiento de Entidades Nombradas (NER, del inglés Named-Entity Recognition), que emplean tecnología de aprendizaje automático, reglas y corpus lingüísticos para identificar entidades basadas en palabras o frases y clasificarlas a partir de un conjunto de elementos con características similares. Estas herramientas permiten etiquetar texto en función de su contexto, lo que permite diferenciarlo de las demás categorías.

Una vez se ha etiquetado el texto, se procede a la extracción de relaciones (RE, del inglés Relation Extraction) semánticas entre dos o más entidades de un determinado tipo previamente identificadas para realizar su clasificación en una serie de características como “hijo de”,“empleado de”, “vive en” o “está en”, adquiriéndo conocimientos estructurados a partir de datos no estructurados y permitiéndo realizar búsquedas inteligentes para reducir el tiempo de análisis de archivos en un proceso forense.

Existen métodos de extracción supervisados y no supervisados. En cuanto a los supervisados, se utilizan en diversas aplicaciones en las que es necesario extraer relaciones específicas entre entidades en datos no estructurados, como análisis de sentimientos o seguimiento de las redes sociales. Este método garantiza que las relaciones extraídas del texto son las más relevantes, pero denota dificultad para incluir nuevas

relaciones, requiere un conjunto de datos etiquetados y sólo es eficaz para un conjunto reducido de tipos de relaciones entre entidades. En lo que respecta a los no supervisados, emplean reglas empíricas más generales para la agrupación de textos, la detección de anomalías, o el descubrimiento de relaciones adicionales. Sin embargo, estos modelos pueden ser más difíciles de interpretar y validar que los modelos supervisados, ya que no existe un conjunto de datos etiquetados con el que comparar los resultados.

En segundo lugar, también encontramos la Comprensión del Lenguaje Natural (NLU, del inglés Natural Language Understading), rama del NLP que se encarga de la comprensión automática de un texto dado, y que presenta múltiples aplicaciones como razonamiento automático, traducción, preguntas y respuestas, recopilación de noticias y comandos por voz, entre otros. Dentro de este subcampo existen distintos algoritmos que han demostrado una gran eficiencia en la detección de entidades, como pueden ser BERT (del inglés Bidirectional Encoder Representations from Transformers, técnica basada en redes neuronales para el pre-entrenamiento del NLP que implementa la bidireccionalidad, es decir, el análisis de la misma frase de izquierda a derecha y de derecha a izquierda desde la palabra clave para comprender en profundidad el contexto y la temática de cada oración), XLNet (modelo que supera las limitaciones de BERT mediante el pre-entrenamiento autoregresivo, mejorando el rendimiento al abordar las limitaciones de la información bidireccional) o GPT (del inglés Generative Pre-trained Transformer, modelo de NLP basado en deep learning que permite generar textos similares a los humanos a partir de una entrada de texto). Sin embargo, el modelo que superó en precisión y rendimiento a los modelos anteriores fue el algoritmo desarrollado por Facebook denominado RoBERTa, modelo basado en BERT que proporciona una gran flexibilidad y puede adaptarse a una amplia gama de tareas como la clasificación de textos, el reconocimiento de entidades, el análisis de sentimientos o el procesamiento de textos en varios idiomas. El proceso de pre-entrenamiento mejora en comparación con BERT, utilizando pre-entrenamiento sin restricciones, lo que ayuda a mejorar su capacidad para identificar características semánticas y sintácticas. Este modelo puede ser útil para equipos con recursos limitados que quieran aprovechar las ventajas del aprendizaje automático pre-entrenado sin tener que invertir tiempo en entrenar modelos personalizados desde cero.

2. Resultados

Los avances en diferentes campos del aprendizaje automático como el Procesamiento del Lenguaje Natural permiten la creación de arquitecturas que aumentan el rendimiento de la extracción y análisis de información en dispositivos, realizando un proceso de búsqueda inteligente tratando de encontrar relaciones entre archivos a partir de la búsqueda de un determinado término, lo que, en un proceso de análisis forense, puede aportar ventajas como una mayor precisión en la extracción e identificación de pruebas, identificación de patrones en los textos y vinculación de datos, reducción de errores humanos y automatización de tareas repetitivas, permitiendo a los investigadores centrarse en tareas más complejas y llegar a conclusiones más sólidas y precisas.

3. Discusión/Conclusiones

Como hemos visto existen múltiples algoritmos de inteligencia artificial que permiten realizar un análisis exhaustivo de la información contenida en dispositivos extraíbles en un proceso forense empleando técnicas de Procesamiento del Lenguaje Natural para la clasificación automática de documentos. No obstante, la rama del NLP todavía presenta varios retos sin resolver, cuyo número se amplía conforme lo hace la demanda, como por ejemplo la comprensión de las abreviaciones, las variaciones y errores sintácticos y ortográficos, la mezcla de distintos lenguajes, el uso de extranjerismos, coloquialismos empleados solo en determinadas culturas o el uso de frases sarcásticas. Todos estos ejemplos presentan dificultades a los algoritmos de NLP para identificar y detectar el contexto de una frase, y constituyen desafíos abiertos a los que se enfrentan los desarrolladores tecnológicos para generar herramientas que utilicen técnicas de inteligencia artificial para analizar la información en un proceso forense digital.

4. Valoración del documento original

El documento proporciona una visión general de cómo la inteligencia artificial, especialmente el procesamiento del lenguaje natural y el aprendizaje automático, se está utilizando en el ámbito de la informática forense. Se destacan los avances en la extracción y análisis de datos, así como los desafíos persistentes que enfrentan los investigadores en este campo. Además, se plantea la importancia de seguir desarrollando herramientas y algoritmos que puedan abordar eficazmente las complejidades del análisis forense en un entorno digital en constante evolución.

Referencias

· Luis Alberto Martínez Hernández, Ana Lucila Sandoval Orozco, Luis Javier García Villalba,, *"Técnicas de Inteligencia Artificial Supervisadas y No Supervisadas para el Análisis de Información Digital en Dispositivos de Almacenamiento"*, , Actas de las VIII Jornadas Nacionales de Investigación en Ciberseguridad, Vigo (21 a 23 de junio de 2023).