STEGONOMONO: A WEBSITE FOR DETECTING STEGANOGRAPHY ON MONOCHROMATIC IMAGES

ALBERTO MANUEL GARCÍA GRIMALDOS, ANA BEATRIZ MOJICA, GERMÁN RICARDO MORALES CASTRO

ASIGNATURAS INVOLUCRADAS

MODELADO Y SIMULACIÓN, SEGURIDAD INFORMÁTICA, DESARROLLO ORIENTADO A WEB

DOCENTES INVOLUCRADOS
DIEGO JAVIER PARADA SERRANO, JUAN SEBASTIÁN GÓMEZ ROSAS

UNIVERSIDAD PONTIFICIA BOLIVARIANA
ESCUELA DE INGENIERÍA
FACULTAD DE INGENIERÍA DE SISTEMAS E INFORMÁTICA
BUCARAMANGA
2019

STEGONOMONO

1. Especificación de la situación problemática

Diariamente se están desarrollando avances en el campo de la seguridad informática, lo que deja desprotegidas a algunas plataformas menos enteradas de estos temas nuevos.

La esteganografía es un método para el ofuscamiento de datos (o archivos) en archivos, que busca ser difícilmente identificable; muchas plataformas se protegen de la esteganografía de compresión (los archivos contienen comprimidos de otros archivos). Entre los distintos tipos de esteganografía, encontramos la LSB (less significant bit), la cual es más difícil de detectar que la esteganografía de compresión, por lo que muchas plataformas en internet no realizan una verificación para protegerse de los posibles archivos maliciosos subidos a estas.

¿Cómo crear un sistema de detección de esteganografía LSB en imágenes monocromáticas de un tamaño determinado por medio de un API pública?

2. Objetivos

2.1. Objetivo General: Desarrollar una plataforma web que sirva un API público para detección de esteganografía en imágenes monocromáticas mediante redes neuronales, para mejorar la seguridad en plataformas a las que se puedan subir imágenes.

2.2. Objetivos Específicos: Determinar las características de una red neuronal para reconocer esteganografía en imágenes monocromáticas.

Modelar una red neuronal para reconocer esteganografía en imágenes monocromáticas de un tamaño específico.

Implementar la IA desarrollada en una plataforma web que sirva API públicas para la detección de esteganografía en imágenes monocromáticas.

3. Justificación

Hoy en día cualquier persona puede usar estenografía para poder mandar un mensaje o alguna instrucción escondida en una imagen que puede ser subida fácilmente a twitter y llegar a atacar a los usuarios sean expuestos a la imagen. Esto es posible dado a que algunas imágenes que pueden parecer completamente inofensivas a simple vista tengan una segunda función escondida en algunos pixeles que hayan sido alterados y sin ser detectados.

Investigadores de Trend Micro han descubierto en el 2017 un grupo de hackers que usan esteganografía para ocultar comandos maliciosos dentro de una imagen publicada en Twitter. Aunque se vea como una imagen común para el ojo humano, el comando “/print” está oculto en su metadata, lo que hace que el malware mande una captura de pantalla de la máquina afectada a un servidor de comando y control. Además de tomar capturas de pantalla, el malware también se le puede dar otra

variedad de comandos como tomar el nombre de la cuenta, obtener nombres de archivos de directorios específicos, o tomar una lista de procesos en ejecución.

Twitter y varios otros sitios de redes sociales no disponen de un proceso de filtro para poder encontrar, identificar y rechazar imágenes que hayan sido alteradas por medio de estenografía, y esto significa que estos sitios en general son menos seguros debido a esto.

Nosotros proponemos desarrollar un sistema para la identificación de imágenes alteradas con estenografía para que no permita que este tipo de imágenes sean subidas y por ende hacer más segura la plataforma.

4. Contexto actual

https://ieeexplore.ieee.org/abstract/document/959097

https://ieeexplore.ieee.org/abstract/document/958299

https://www.sciencedirect.com/science/article/pii/S0165168409003648

NOTA: Las fuentes anteriores son de las pocas que existen sobre el tema en la actualidad.

El software busca asemejar los sistemas de control y monitoreo de virus en archivos, utilizados por aplicaciones donde existe un constante tráfico de archivos.

Se desea tener una especie de “antivirus” para imágenes.

5. Cronograma de Actividades

Actividad 1.1. :Lectura e investigación sobre las redes neuronales y su aplicabilidad para la detección de esteganografía en imágenes	2	Julio 29, 2019	Agosto 12, 2019
Actividad 1.2. :Caracterizar los procesos de esteganografía en imágenes monocromáticas y sus diferencias con imágenes libres de esteganografía.	2	Julio 29, 2019	Agosto 12, 2019
Actividad 2.1. : Diseñar el algoritmo con enfoque de redes neuronales que permita clasificar imagenes monoromáticas con y sin esteganografía.	3	Agosto 12, 2019	Agosto 31, 2019
Actividad 2.2. : Conformar un conjunto de datos de prueba de imágenes monocromáticas con esteganografía, que permitan entrenar la rede neuronal.	3	Agosto 12, 2019	Agosto 31, 2019
Actividad 2.3. : Implementar el algoritmo con enfoque de redes neuronales para clasificación de imágenes monocromáticas con	4	Agosto 31, 2019	Septiembre 30, 2019
Actividad 2.4: Validar la correcta ejecución del algoritmo con el conjunto de datos de prueba	1	Septiembre 30, 2019	Octubre 4, 2019
Actividad 3.1. : Diseñar el servicio web que contendrá y servirá la API	1	Octubre 4, 2019	Octubre 6, 2019
Actividad 3.2. : Acoplar la IA en una API para servir	1	Octubre 6, 2019	Octubre 10, 2019
Actividad 3.3. : Implementar el servicio de APIs dentro del proyecto web	1	Octubre 10, 2019	Octubre 18, 2019
Actividad 4.1. : Documentar el desarrollo del proyecto	1	Octubre 18, 2019	Octubre 25, 2019
Actividad 4.2. : Presentar los resultados en la Jornada de Socialización de Proyectos Integradores y de Aula	1	Octubre 21, 2019	Octubre 25, 2019
Actividad 4.3. : Elaborar un video de máximo tres minutos sobre el proyecto	1	Octubre 18, 2019	Octubre 25, 2019
Actividad 4.4. :			

Fechas Importantes para tener en cuenta en el cronograma:

- Ver el anexo con las actividades y fechas más relevantes.

6. Alcances

Se espera tener una web publicada en internet, que sirva un API para la detección de esteganografía en imágenes monocromáticas de un tamaño en específico. El servidor debe tener aseguramiento básico basado en normas ISO. La red neuronal debe tener una precisión de más del 90%.

7. Presupuesto

Asumiendo que el contratante posea una infraestructura de redes, estos serían los costos.

Equipos e insumos: $0

Pago desarrollador front-end: $3’000.000

Pago desarrollador back-end: $12’000.000

Pago desarrollador machine learning: $20’000.000

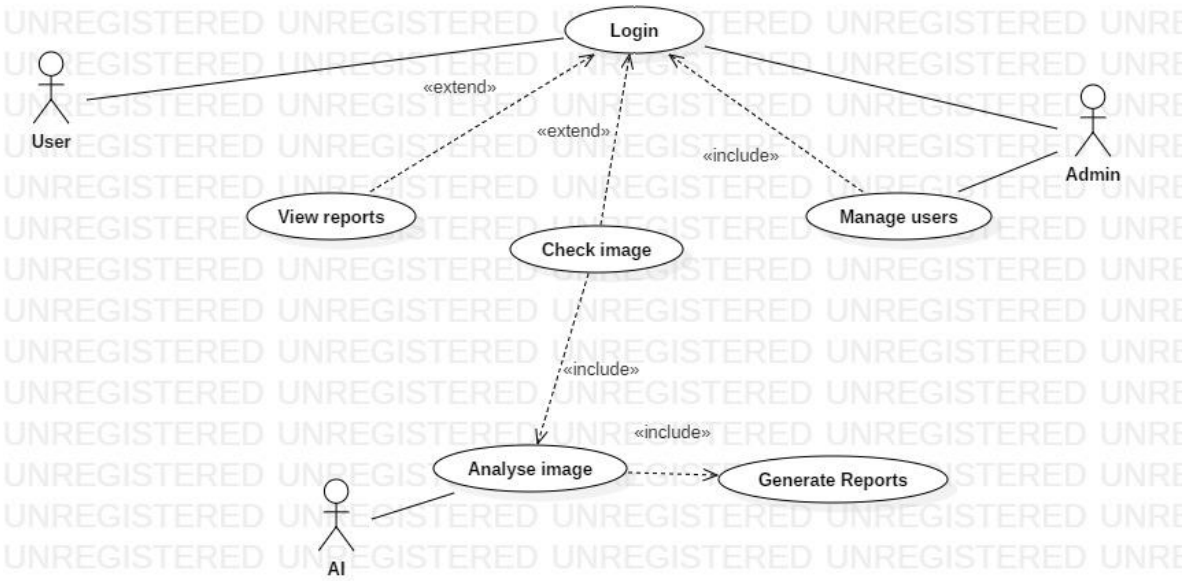
Pago ensamblador: $5’000.000

Pago experto seguridad informática: $5’000.000

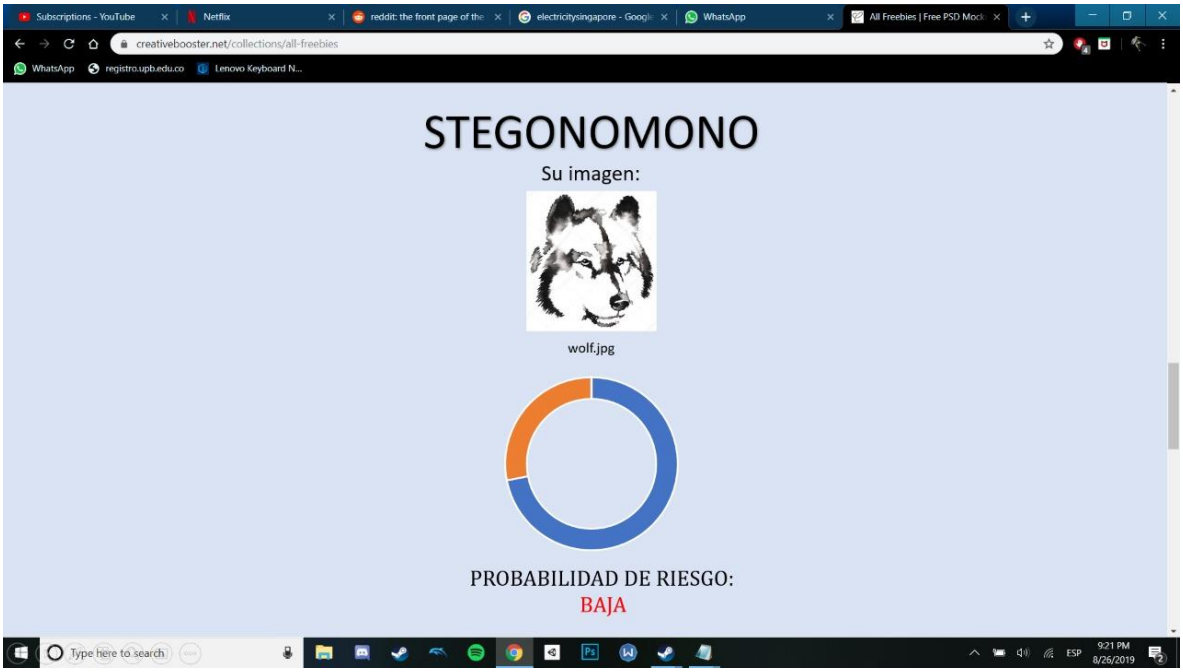
Pago ingeniero de redes: $7’000.000

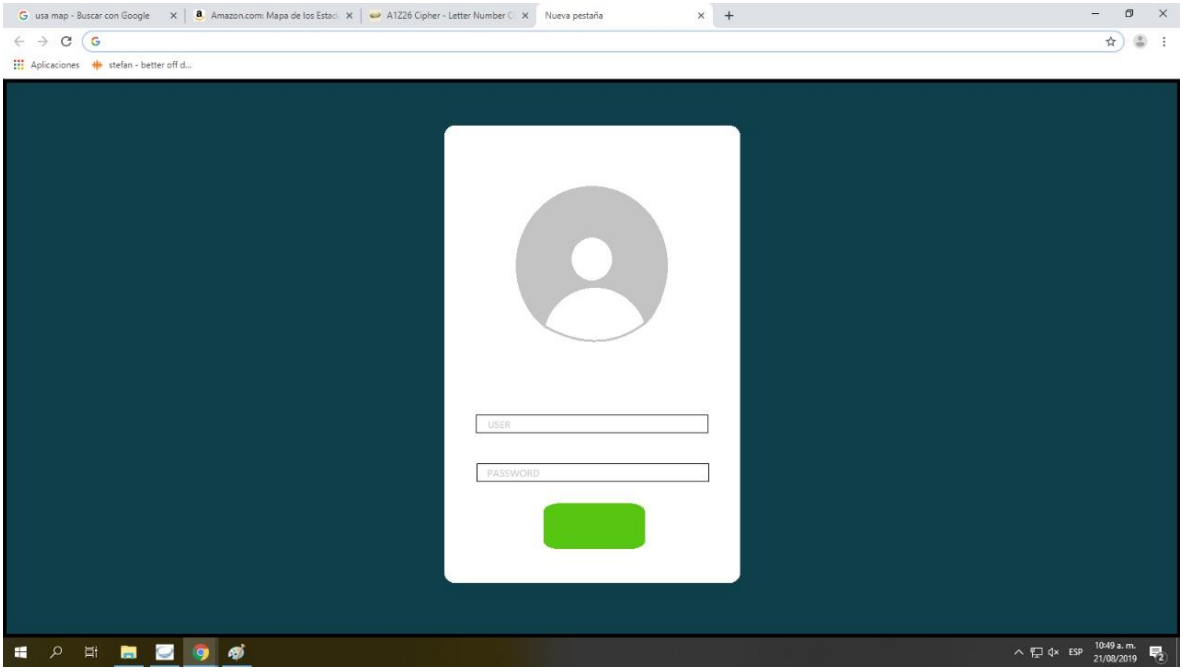
9. Resultados

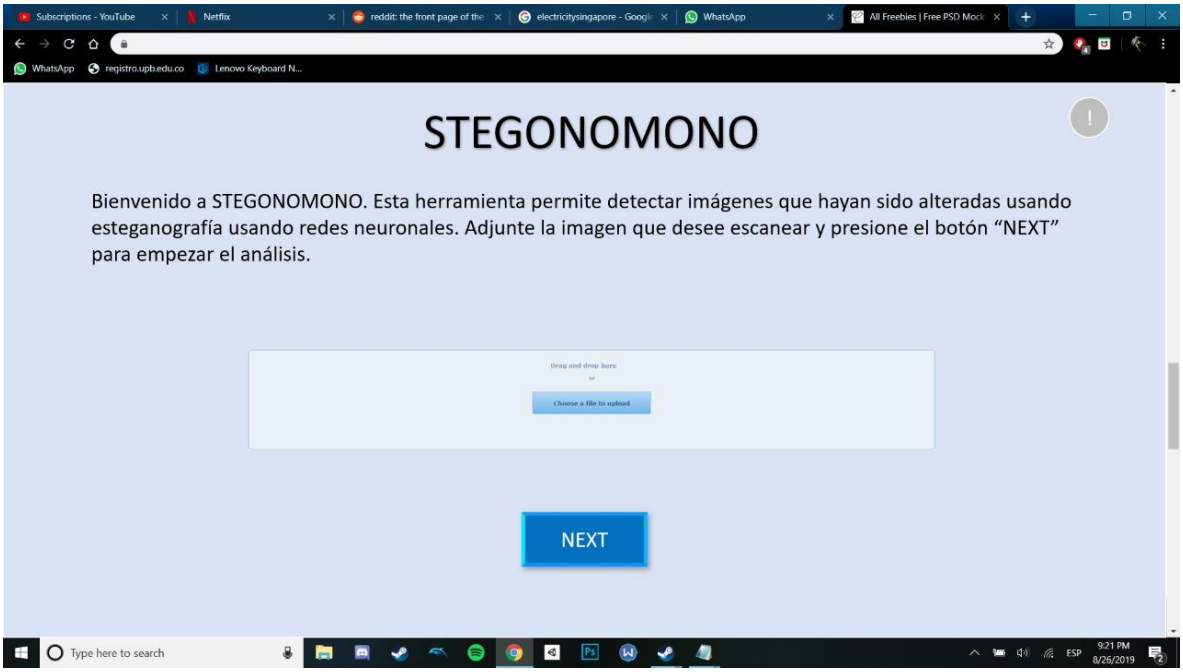
Casos de uso



Vistas de usuario


STEGONOMONO
Su imagen:
wolf.jpg
PROBABILIDAD DE RIESGO:
BAJA


USER
PASSWORD



Requerimientos Funcionales:

1. El servicio de detección debe poder recibir una imagen monocromática de dimensiones específicas para determinar si existe esteganografía LSB en ella o no

2. Se debe contar con un API para brindar el servicio de la aplicación

3. Se deben generar reportes sobre la probabilidad de esteganografía en la detección

4. La plataforma web debe presentar informes de cuantas imágenes fueron detectadas como alteradas

5. Los informes deben ser generados automáticamente después de escanear una imagen

Requerimientos No Funcionales:

1. Todos los usuarios deben acceder a la aplicación y autenticarse para poder usarla

2. La plataforma debe contar con acceso ilimitado de usuarios (capacidad de procesamiento flexible de AWS)

3.Se deben utilizar redes neuronales para la identificación de esteganografía en imágenes monocromáticas

4. Se debe desarrollar usando el stack de desarrollo MERN

5. La precisión de la red neuronal debe ser superior al 90%

Escenarios de prueba

Imagen limpia, imagen con esteganografía, se recibe algo distinto a una imagen,

10. Referencias

[1] W. Wei. (2018, diciembre 18). New Malware Takes Commands From Memes Posted On Twitter. En línea. Disponible: https://thehackernews.com/2018/12/malware-twitter-meme.html

[2] D. Renza, D. M. Ballesteros, R. Rincón. (2016, junio). Método de ocultamiento de píxeles paraesteganografía de imágenes en escala degris sobre imágenes a color En línea. Disponible: http://www.scielo.org.co/pdf/ince/v12n23/v12n23a09.pdf