Herramienta de apoyo para la identificación de usuarios que ejercen violencia digital, mediante esteganografía en imágenes

Trabajo Terminal No. 2 0 2 0 - B 0 1 8

*Alumnos: Cortés Zanabria Oscar Uriel, Flores Islas Angelica Margarita, *Páramo Romero Luis Antonio*

Directores: Moreno Cervantes Axel Ernesto, Díaz Santiago Sandra

**e-mail: lparamor1400@alumno.ipn.mx*

Resumen – Las redes sociales son una herramienta de comunicación muy poderosa, sin embargo, pueden traer consigo acciones de violencia digital como la divulgación de contenido visual no autorizado, por lo que en este trabajo se presenta un mecanismo que inserta en una imagen información cifrada que nos permita identificar al causante de esta infracción, utilizando algoritmos esteganográficos.

Palabras clave – Criptografía, Esteganografía, Sexting

1. Introducción

Debido a que en los últimos años el internet ha tenido un gran impacto en la cotidianidad humana, las repercusiones de su uso poco ético han sobrepasado la barrera digital. Un ejemplo es el *sexting*, que consiste en compartir imágenes de índole sexual, personal o de otros, por medio de internet, el riesgo que se corre es que dichas imágenes sean publicadas y por consiguiente viralizadas sin permiso del propietario [1]. Esto da lugar a consecuencias negativas a corto y largo plazo, tales como ciberacoso, chantaje, daño emocional e incluso intento o consumación de suicidio [2].

Para que acciones como estas sean castigadas, en primer lugar, es necesario conocer al responsable de la divulgación del contenido, una forma de facilitar esta tarea es insertar datos que identifican su dispositivo. Esta información no debe ser perceptible para cualquier usuario, por lo que debe estar oculta. Existe un recurso enfocado a este propósito, la esteganografía, que es una técnica de ocultación de datos utilizada principalmente en aplicaciones de seguridad de la información. Es similar a las técnicas de marca de agua y criptografía, pero se diferencian en diversos aspectos. La marca de agua rastrea principalmente copias ilegales o reclamos de propiedad de medios digitales, no está diseñado para la comunicación. Por otro lado, la criptografía codifica los datos con la combinación de permutaciones y sustituciones para que los receptores no deseados no puedan percibir la información procesada [3] .

Finalmente, el término técnico “esteganografía” en sí se deriva de las palabras griegas *steganos*, que significa "cubierto", y *graphia*, que significa "escritura". La esteganografía es el arte de la comunicación oculta. La mera existencia de un mensaje es secreta [4]; transmite información al incrustar mensajes en objetos de cubierta de apariencia inocente, como imágenes digitales, para ocultar la existencia misma de la comunicación. Como resultado, la esteganografía es el arte y la ciencia del contrabando de datos.[5]

Existen diferentes aplicaciones que tratan de resolver problemas relacionados, las cuales son descritas en la siguiente tabla:

SOFTWARE	CARACTERÍSTICAS	PRECIO EN EL MERCADO
ExifTool[6]	Lee metadatos cronometrados (por ejemplo, seguimiento de GPS) de videos MOV / MP4 / M2TS / AVI. Geoetiqueta imágenes de archivos de registro de seguimiento de GPS Genera registros de seguimiento a partir de imágenes geoetiquetadas. Copia metainformación entre archivos (incluso archivos de formato diferente).	Gratuita

SSuite Picsel[7]	Protege todos sus mensajes de texto utilizando cifrado esteganográfico. Se ejecuta en todos los sistemas operativos Windows: 32 y 64 bits	Gratuita
Hide'N'Send[8]	Utiliza algoritmos esteganográficos modernos: F5 y LSB, y también sus opciones con codificación matricial. Para el cifrado se puede utilizar uno de los siguientes algoritmos: AES, RC4, RC2	Gratuita
¡Watermark Pro[9]	La lista de funciones de marca de agua del software incluye opciones como Firma, Texto de arco, StegoMark o Metadatos que permiten agregar marcas de agua visibles e invisibles a fotos y videos.	30 dólares

Tabla 1. Sistemas que abordan problemáticas similares

En este trabajo explicaremos una visión general sobre cómo abordaremos la problemática haciendo uso de la esteganografía para incrustar en imágenes los datos que se mencionan anteriormente.

2. Objetivo

Objetivo General

Diseñar un mecanismo para la inserción de información cifrada dentro de archivos de imagen que permita identificar al usuario responsable de su divulgación, mediante algoritmos esteganográficos.

Objetivos Particulares

- Estudiar los algoritmos esteganográficos existentes.
- Conocer la estructura de los formatos de imagen más utilizados.
- Determinar qué información es de utilidad para identificar al usuario responsable de la divulgación de imágenes ajenas.
- Estudiar los recursos del sistema operativo necesarios para detectar los archivos de imagen a tratar y saber cómo hacer uso de ellos mediante la programación de señales.
- Implementar mediante programación de señales la detección de entrada y salida de archivos a nivel de sistema operativo para aplicar el mecanismo sobre ellos.
- Determinar los mecanismos criptográficos para proveer privacidad a la información insertada.
- Desarrollar una aplicación de usuario para recuperar la información contenida en las imágenes.

3. Justificación

En los sistemas computacionales, se ha priorizado la privacidad del usuario protegiendo su identidad de manera individual, sin embargo, cuando la integridad de otro usuario se ve amenazada, es de interés averiguar información sobre el causante de dicho problema. Como futuros ingenieros en sistemas somos conscientes de que la vida digital es tan importante como la vida real y el gran impacto que puede causar el mal uso del contenido personal en internet.

Esta problemática es un tema de interés actual, incluso en varios estados de México, recientemente se han estipulado un conjunto de legislaciones encaminadas a reconocer la violencia digital y sancionar delitos que violen la intimidad sexual: la ley olimpia.

La denominada "Ley Olimpia" surge a raíz de la difusión de un video de contenido sexual no autorizado de una mujer en el estado de Puebla; derivado de ello se impulsó una iniciativa para reformar el Código Penal de dicha entidad y tipificar tales conductas como violación a la intimidad; acción que se ha replicado en 17 entidades federativas. Entre las sanciones que se imponen están multas económicas y hasta 8 años de prisión [10].

Nosotros planteamos un mecanismo que sirva como herramienta en el proceso de identificación de los infractores, mediante el desarrollo de un algoritmo que introduzca en los archivos multimedia, específicamente imágenes, datos cifrados sobre el primer usuario que los comparte, autor, y el segundo, quien viola la confianza. Esta información será tratada con el uso de técnicas esteganográficas para mantenerla oculta ante los usuarios. Además, será necesario que el mecanismo se ejecute en segundo plano para poder detectar los archivos a manipular, por lo que necesitamos trabajar a un nivel lo suficientemente bajo que nos permita acceder a determinados recursos del sistema operativo.

Actualmente, los procedimientos utilizados para resolver esta problemática son complicados y requieren muchas herramientas y pasos sistemáticos, por lo que nuestra solución pretende brindar una alternativa más sencilla.

Consideramos que es un proyecto económica e intelectualmente alcanzable, pues si bien desconocemos algunos de los temas, tenemos los conocimientos en áreas relacionadas que nos permiten adquirir esas nuevas habilidades.

4. Productos o Resultados esperados

Al concluir el desarrollo del prototipo, se espera que este forme parte del sistema que se muestra en la Imagen 1, donde el sujeto A (autor) crea una imagen que será procesada por nuestro prototipo, se producirá una nueva imagen que incluye sus datos cifrados, que es la que recibe el sujeto B (infractor), posteriormente la imagen es procesada por nuestro prototipo, se producirá una nueva imagen que ahora incluye los datos cifrados del sujeto A y del sujeto B, acto seguido el sujeto B hace pública esta imagen.

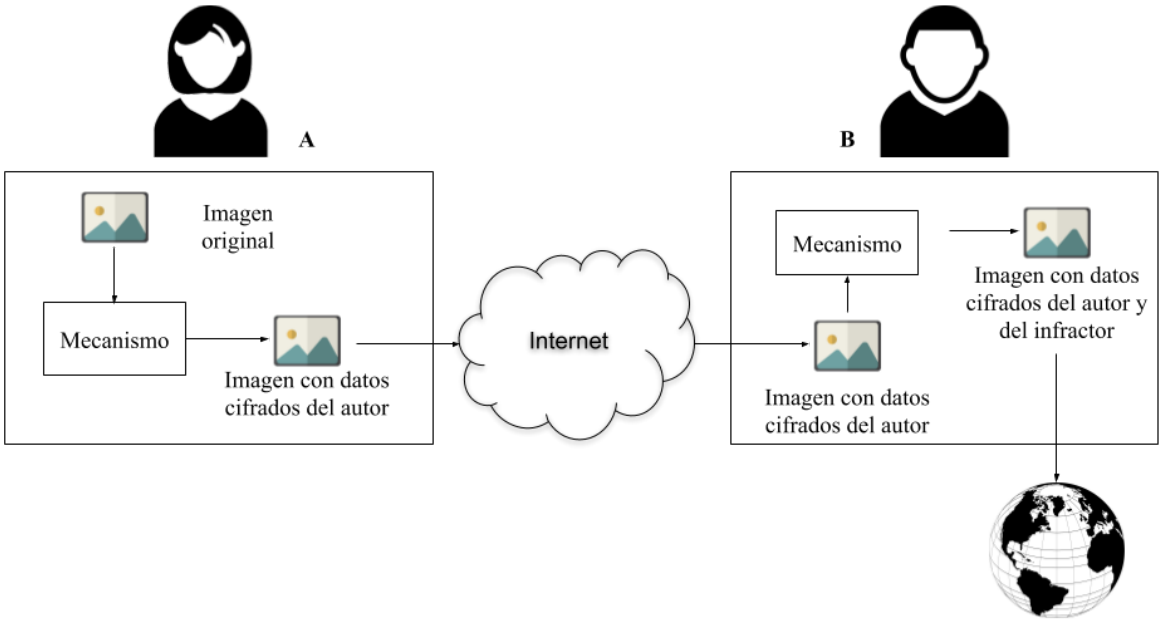

Imagen 1. Diagrama a bloques del funcionamiento general

El funcionamiento general del mecanismo se muestra en la Imagen 2, se recibe una imagen y junto con los los datos cifrados del usuario, se aplica un algoritmo esteganográfico para generar una nueva imagen que contiene los datos cifrados del usuario.

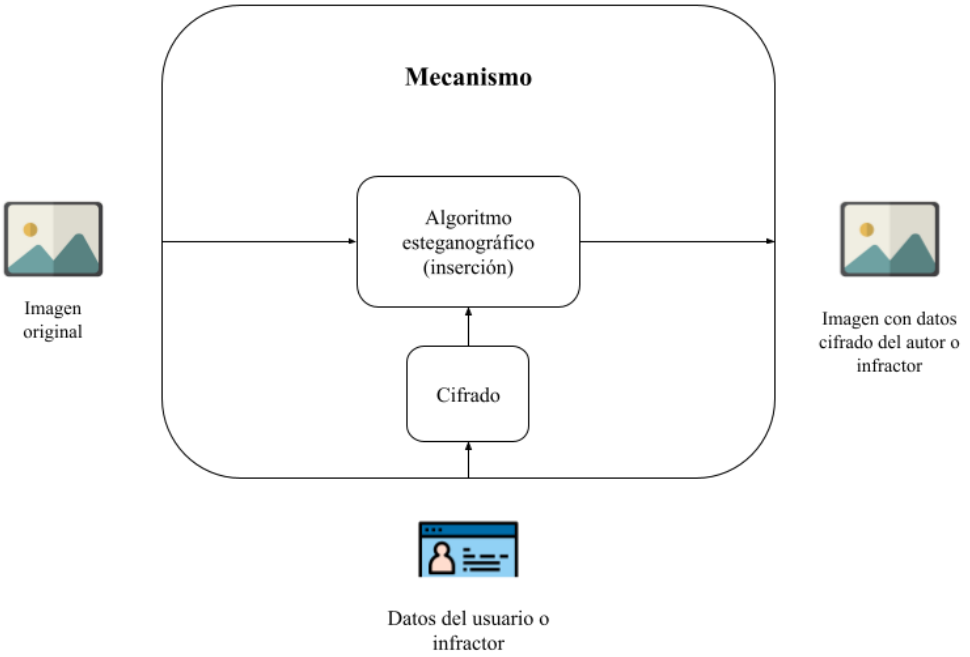

Imagen 2. Diagrama a bloques del funcionamiento del mecanismo

Además del mecanismo, elaboraremos una aplicación para que usuarios autorizados puedan recuperar la información contenida en las imágenes, la cual realizará el proceso inverso del mecanismo señalado en la imagen 2; un manual para facilitar su utilización y la documentación relacionada a todo el proyecto.

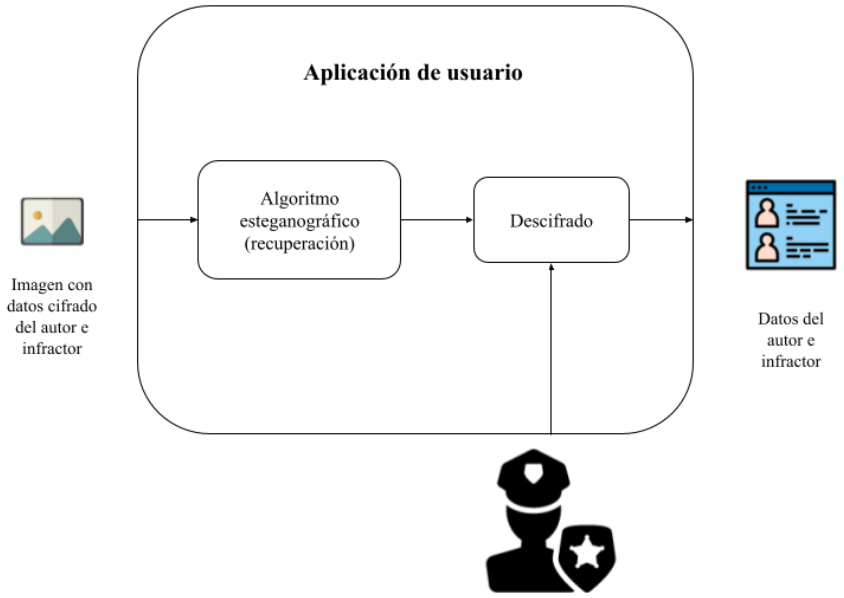

Imagen 3. Diagrama a bloques del funcionamiento de la aplicación de usuario.

5. Metodología

Durante el desarrollo de este proyecto tomaremos características de la metodología XP (Programación Extrema). Esta elección se basa en las cuatro etapas fundamentales para la construcción del prototipo que propone esta metodología: planificación, diseño, codificación y pruebas, pues dividir el desarrollo de esta manera nos proporciona un enfoque más ordenado.

Los principios de desarrollo incremental de esta metodología se adaptan a nuestra idea de crear el prototipo poco a poco, iniciando con las funcionalidades básicas hasta llegar a nuestro objetivo.

Una de las características a destacar es el gran peso en la etapa de la codificación, esta metodología sugiere utilizar ciertas normas y formato de codificación, sin embargo, a diferencia de lo que estipula XP, no programaremos en parejas, sino todo el equipo a la vez.

6. Cronograma

Nombre del alumno(a): Cortés Zanabria Oscar Uriel TT No.: 2020 - B018
Título del TT: Herramienta para la identificación de usuarios que ejercen violencia digital, mediante esteganografía en imágenes

Actividad	FEB	MAR	ABR	MAY	JUN	AGO	SEP	OCT	NOV	DIC
Determinación de los recursos del sistema operativo										
Estudio de programación de señales										
Análisis del mecanismo y aplicación										
Diseño del mecanismo y aplicación										
Evaluación TT 1										
Generación del código del mecanismo										
Generación del código de la aplicación										
Pruebas y optimización										
Documentación										
Elaboración de reporte técnico										
Elaboración de manual de usuario										
Evaluación TT 2										

Nombre del alumno(a): Flores Islas Angelica Margarita TT No.: 2020 - B018
Título del TT: Herramienta para la identificación de usuarios que ejercen violencia digital, mediante esteganografía en imágenes

Actividad	FEB	MAR	ABR	MAY	JUN	AGO	SEP	OCT	NOV	DIC
Estudio de algoritmos esteganográficos										

Determinación del algoritmo de cifrado a utilizar										
Análisis del mecanismo y aplicación										
Diseño del mecanismo y aplicación										
Evaluación TT 1										
Generación del código del mecanismo										
Generación del código de la aplicación										
Pruebas y optimización										
Documentación										
Elaboración de reporte técnico										
Elaboración de manual de usuario										
Evaluación TT 2										

Nombre del alumno(a): Páramo Romero Luis Antonio TT No.: 2020 - B018
Título del TT: Herramienta para la identificación de usuarios que ejercen violencia digital, mediante esteganografía en imágenes

Actividad	FEB	MAR	ABR	MAY	JUN	AGO	SEP	OCT	NOV	DIC
Investigación de la estructura de los formatos de imagen.										
Determinación de los datos que serán de utilidad para la identificación del usuario infractor.										
Análisis del mecanismo y aplicación										
Diseño del mecanismo y aplicación										
Evaluación TT 1										
Generación del código del mecanismo										
Generación del código de la aplicación										
Pruebas y optimización										
Documentación										
Elaboración de reporte técnico										
Elaboración de manual de usuario										
Evaluación TT 2										

7. Referencias

[1]D. Arab L. and P. Díaz G., "Impacto de las redes sociales e internet en la adolescencia: aspectos positivos y negativos", *Revista Médica Clínica Las Condes*, vol. 26, no. 1, p. 10, 2015. Disponible: https://reader.elsevier.com/reader/sd/pii/S0716864015000048?token=8C26DE7B647E62F304DB5ABBAE66D044B5C0E8D9E26362114E0BF54CD25E491EE742D8062107C6BBA69C8FB255B1639B. [Consultado 27- Oct- 2020].

[2]A. SD, "Las consecuencias del sexting", *Kaspersky.es*, 2016. [Online]. Disponible: https://www.kaspersky.es/blog/sexting-y-sus-consecuencias/7692/. [Consultado: 27- Oct- 2020].

[3]S. Kumar Dubey and K. Dubey, "Steganography, Cryptography and Watermarking: A Review", International Journal of Innovative Research in Science, Engineering and Technology, vol. 6, no. 2, 2017. Disponible: http://www.ijirset.com/upload/2017/february/76_21_Steganography.pdf. [Consultado 29- Oct- 2020].

[4]I. Cox, M. Miller, J. Bloom, J. Fridrich and T. Kalker, Digital Watermarking and Steganography, 2nd ed. Oxford, UK.: Morgan Kaufmann Publishers, 2008.

[5]E. Houssein, M. Ali and A. Hassanien, "An Image Steganography Algorithm using Haar Discrete Wavelet Transform with Advanced Encryption System", *Proceedings of the Federated Conference on Computer Science and Information Systems*, vol. 8. Disponible: 10.15439/2016F521 [Consultado 29- Oct- 2020].

[6]"ExifTool by Phil Harvey", *Exiftool.org*, 2020. [Online]. Disponible: https://exiftool.org/. [Consultado: 28- Oct- 2020].

[7]"SSuite Picsel Steganography Encryption", SSuite Office Software, 2020. [Online]. Disponible: https://www.ssuitesoft.com/ssuitepicselsecurity.htm. [Consultado: 28- Oct- 2020].

[8]"Hide'N'Send", Download.com. [Online]. Disponible: https://download.cnet.com/Hide-N-Send/3000-2092_4-75728348.html. [Consultado: 28- Oct- 2020].

[9]"iWatermark Pro for Mac - #1 Watermark App to Protect Photos | Plum Amazing", Plum Amazing, 2019. [Online]. Disponible: https://plumamazing.com/product/iwatermark-pro-for-mac/. [Consultado: 28- Oct- 2020].

[10]"Ficha Técnica: Ley Olimpia", *Ordenjuridico.gob.mx*. [Online]. Disponible: http://ordenjuridico.gob.mx/violenciagenero/LEY%20OLIMPIA.pdf. [Consultado: 29- Oct- 2020].

8. Alumnos y Directores

Angelica Margarita Flores Islas.- Alumno de la carrera de Ing. en Sistemas Computacionales en ESCOM, Especialidad Sistemas, Boleta:2015140234 , Tel.5526161203 , email afloresi1401@alumno.ipn.mx.

Luis Antonio Páramo Romero.- Alumno de la carrera de Ing. en Sistemas Computacionales en ESCOM, Especialidad Sistemas, Boleta:2015120912 , Tel.5526514110 , email lparamor1400@alumno.ipn.mx.

Oscar Uriel Cortés Zanabria .- Alumno de la carrera de Ing. en Sistemas Computacionales en ESCOM, Especialidad Sistemas, Boleta:2015010219 , Tel.5576503053 , email ocortesz1400@alumno.ipn.mx.

Axel Ernesto Moreno Cervantes M. En C. En CINVESTAV en 2004, ISC En ESCOM-IPN en 2000. Profesor de ESCOM (Depto. ISC) desde 2004, áreas de interés. Redes de computadoras, sistemas distribuidos, educación. Ext. 52032, email axelernesto@gmail.com

Sandra Díaz Santiago - Doctorado en Ciencias en Computación en CINVESTAV-IPN, en 2014, Maestría en Ciencias (Matemáticas) en la UAM-Iztapalapa, 2005. Licenciatura en Computación en UAM-Iztapalapa, en 1998. Profesor en ESCOM (Departamento de Ciencias e Ingeniería de la Computación), desde 2004, Áreas de Interés: Criptografía, Pseudoaleatoriedad, Seguridad Demostrable, Ext 52022, email sdiazs@gmail.com, sdiazsa@ipn.mx.