Encriptamiento de imágenes mediante CPC

Trabajo Terminal No. 2020 - A041

Alumnos: *Bautista Barroso Luis Alberto

Directores: Luna Benoso Benjamín, Silva García Víctor Manuel

**luis.bautista_escom.ing@outlook.com*

Resumen – En este documento se presenta la propuesta de desarrollar una plataforma web para el encriptamiento de imágenes y texto haciendo uso del método Chaotic Pi Ciphering (CPC). Esto ayuda a reforzar la seguridad al almacenar o compartir estos tipos de archivos digitales a través de la red y evitar el uso indebido por terceros.

Palabras Clave – Análisis de Imágenes, Aplicación Web, Criptografía, Seguridad Informática, Caos, CPC.

1. Introducción

Millones de fotos y textos son enviados a través de las redes sociales y aplicaciones de mensajería instantánea, mediante técnicas de programación informática los piratas cibernéticos pueden llegar a conseguir estos archivos de manera muy sencilla y utilizarlos a su conveniencia y de forma ilegal. Hoy en día ningún sistema es completamente seguro, por lo que es muy peligroso subir estos documentos de suma importancia en estos sistemas.

De igual forma cuando se tiene un archivo privado que no se desea que sea revisado por terceras personas, es necesaria una forma de dejarla oculta en una computadora. Desde hace tiempo, para evitar estos problemas se utilizan diferentes técnicas de cifrado en las cuales las imágenes se vuelven ilegibles gracias a un algoritmo que desordenan sus componentes y se basan principalmente en métodos iterativos[1]. Así, cualquier persona que no disponga de las llaves correctas no podrá acceder a la información que contiene. Es por ello que para ayudar a solucionar esta problemática se realizará un sistema en la cual el usuario encriptará una imagen con una clave que sólo él conocerá y que será necesaria a la hora de desencriptarla, de esta forma logrará almacenar o compartir la imagen encriptada a través de redes sociales sin vulnerar la seguridad al momento de compartir la imagen. En la actualidad existen varios algoritmos implementados en diferentes plataformas como lo son: Data Encryption Data (DES) ,triple-DES, Blowfish y Advanced Encryption Standard (AES).

Se decidió aplicar el método CPC para el encriptado de imágenes por la seguridad que dicho método provee, ya que es seguro en el proceso de encriptación y desencriptación, no genera perdida información en la imagen, por la comprobación de seguridad a través de diversos tipos de ataques como el diferencial, fuerza bruta y las sensibilidades de cifrado y descifrado.

Por otra parte el método que utilizaremos es de clave simétrica, esto quiere decir que este tipo de cifrado es muy fácil de usar y le ayudará al usuario entender con facilidad nuestra plataforma de web, ya que solo se requiere de una llave. La criptografía de clave simétrica es rápida y utiliza menos recursos informáticos que otras formas de cifrado. Su distribución de llaves es muy eficiente dado que la misma llave se utiliza para encriptar y desencriptar la información, esta debe distribuirse a todo aquel que necesita acceder los datos y por último no es necesario disponer de una tercera parte confiable.

Otro punto que se tomará en cuenta para la implementación de la plataforma web es la seguridad, tomaremos en cuenta las herramientas necesarias para fortalecer nuestra plataforma y cuidar adecuadamente las comunicaciones de los usuarios y su información personal contra alguna amenaza y de esta forma obtener como resultado un sitio web seguro de calidad.

En la actualidad existen diversos sistemas similares con el tema de encriptación de imágenes:

Software	Características	Precio en el mercado
Cifrar online[3]	Página web que cifra y descifra texto a partir del algoritmo AES	Gratuito
Codificador base64 online[4]	Página web que cifra texto, archivos e imágenes a través del algoritmo base64	Gratuito
Encriptar y Cifrar en MD5 online[5]	Página web que cifra texto a partir del algoritmo MD5	Gratuito

2. Objetivo

Desarrollar una aplicación web para el encriptamiento y desencriptamiento de imágenes y textos utilizando el método Chaotic Pi Ciphering (CPC) para fortalecer la seguridad al momento del almacenaje o distribución de estos.

3. Justificación

El "Reporte Global de Riesgos 2019"[6], publicado por el Foro Económico Mundial, indica que el fraude o robo de datos cibernético se constituye como el riesgo global con mayor probabilidad de ocurrencia en este año en el área de la informática.

El robo de datos es particularmente relevante hoy en día debido a que la interacción con nuestro entorno se realiza cada vez más a través de herramientas tecnológicas: teléfonos que registran la geolocalización permanente del usuario; instituciones financieras que conocen nuestros patrones de consumo; redes sociales que permiten identificar nuestros círculos de amistades, las noticias que leemos, nuestros gustos y preferencias; relojes que conocen nuestros hábitos de deporte, de sueño y hasta nuestro ritmo cardiaco; así como cada vez más nuevos productos y servicios que son y serán capaces de obtener información acerca de los aspectos más íntimos de la vida.

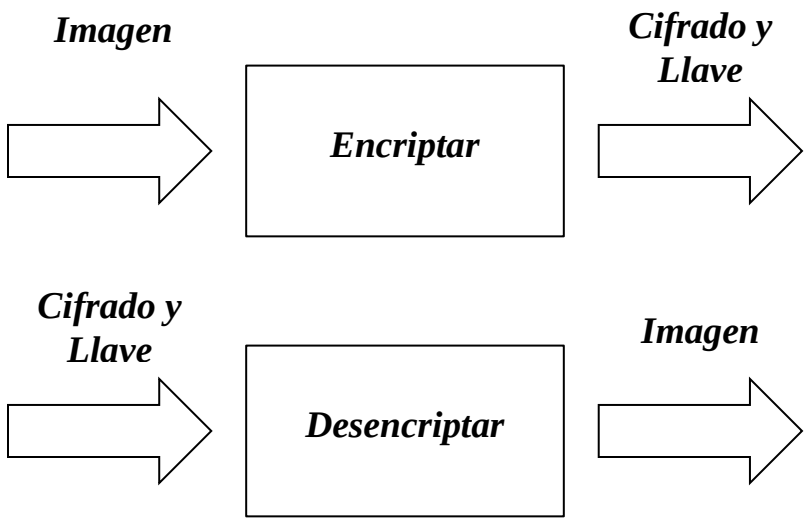
Desde los inicios de la computación, se llegó a la conclusión de que no existe sistema informático que sea infalible. Por lo tanto, los riesgos y la vulnerabilidad a la que se encuentran sujetos los datos personales de todos los miembros de la sociedad contemporánea representan un foco de alerta, pero sobre todo una llamada a la acción.

Entre los archivos más comúnmente robados en internet se encuentran las imágenes, es por esto que la presente solución tiene como objetivo atacar la problemática expuesta mediante una página web para que el usuario logre cifrar una imagen con el uso del método Chaotic Pi Ciphering (CPC)[7] para la encriptación y desencriptación de estos archivos atenuando la posibilidad de su distribución y o uso no autorizado de los mismos y la página web dará como resultado una imagen encriptada.

Cabe mencionar que el método CPC fue seleccionado por ser seguro en el proceso de encriptación y desencriptación, ya que presenta una fuerte resistencia a diversos ataques como el diferencial, fuerza bruta y las sensibilidades de cifrado y descifrado, además de no generar pérdida de información en la imagen.

4. Productos o Resultados esperados

Entradas y salidas del sistema:



Productos esperados:

1. Sistema funcional en la web.
2. Documentación técnica de la aplicación.
3. Código implementado
4. Manual del usuario

5. Metodología

La metodología que utilizaremos es SCRUM, porque reduce los riesgos al conocer las funcionalidades de cada rol y la velocidad a la que avanza el proyecto[2]. Esta metodología nos ayudará a priorizar los módulos que aportaran mayor valor a nuestro criptosistema y a la organización de una manera iterativa, recibiendo constantemente retroalimentación de tanto el área criptográfica como tanto el área de web para adaptar la construcción del producto a las cambiantes necesidades del proyecto.

Otra razón por la cual utilizaremos esta metodología es porque los procesos son iterativos y se manejan dentro de períodos de trabajos muy específicos, lo cual nos facilitará enfocarnos en funcionalidades muy puntuales por cada periodo.

Además el método de trabajo y la revisión será continua para tener una mayor calidad de software. Los procesos del marco de referencia propician naturalmente esta forma de trabajo: las reuniones diarias de todo el equipo, la constante retroalimentación y la transparencia de las metas, tiempos y avances.

6. Cronograma

Nombre del alumno: Bautista Barroso Luis Alberto TT No

Título del TT: Encriptamiento de imágenes mediante CPC

Actividad	Ago	Sep	Oct	Nov	Dic	Ene	Feb	Mar	Abr	May	Jun

Analizar y comprender el método Chaotic Pi Ciphering											
Recopilación de información sobre las herramientas de web											
Implementación del método Chaotic Pi Ciphering											
Evaluación de TT1.											
Construcción de interfaces de la plataforma web											
Desarrollo del front end de la plataforma web											
Generación del Manual de Usuario											
Desarrollo del back end de la plataforma web											

Unión del código Chaotic Pi Ciphering con la plataforma web											
Pruebas											
Reingeniería											
Evaluación de TT II											

7. Referencias

[1] R. Felipe; A. Isabel; S. Augusto; M. David. (2017). Images Encryption Algorithm Using the Lorenz's Chaotic Attractor (vol. 22)[Online]. Available: https://www.redalyc.org/pdf/4988/498853957007.pdf

[2] Scrum.org. What is Scrum[Online]. Available: https://www.scrum.org/resources/what-is-scrum

[3] Cores Tech. Cifrar Online[Online]. Available:https://cifraronline.com/

[4] base64decode.org.Base64[Online]. Available:https://www.base64decode.org/

[5] MD5ONLINE.ES.(2012-2019). CIFRAR MD5[Online]. Available: https://md5online.es/cifrar-md5

[6] World Economic Forum. (2019). Inestabilidades tecnológicas. Informe de riesgos mundiales 2019, 14 edición. 2020, enero 23[Online]. Available: https://www.weforum.org/.

[7]S. Victor; R. Eduardo; G. Marlon; F. Rolando; V. Eduardo; "A novel method for image encryption based on chaos and transcendental numbers", IEEE Acces, vol. 7, pp. 163729-163739, Octubre 2019.

8. Alumnos y Directores

Bautista Barroso Luis Alberto.- Alumno de la carrera de Ing. en Sistemas Computacionales en ESCOM, Especialidad Sistemas, Boleta: 201763013198, Tel. 5536609217, email luis.bautista_escom.ing@outlook.com

Firma: _____

Silva García Victor Manuel.- Doctorado en Ciencias de la Computación por el CIC del IPN. Áreas de interés: seguridad informática y criptografía. Tel. 57296000 ext. 52549 email vsilvag@ipn.mx

Firma: _____

Luna Benoso Benjamín.- Licenciatura en Física y Matemáticas por la ESFM, Doctorado en Ciencias de la Computación por el CIC del IPN. Áreas de interés: criptografía, image analysis y data science. email mobius_95@hotmail.com

Firma: _____

RV: [ADVERTENCIA, MENSAJE EXTERNO] RV: Protocolo final TT2020-A041

Luis Bautista <luis.bautista_escom.ing@outlook.com>
Jue 03/02/2022 7:31
Para: bettoapellido@gmail.com <bettoapellido@gmail.com>

De: Victor Manuel Silva Garcia <vsilvag@ipn.mx>
Enviado: miércoles, 2 de febrero de 2022 11:59
Para: Luis Bautista <luis.bautista_escom.ing@outlook.com>
Asunto: RE: [ADVERTENCIA, MENSAJE EXTERNO] RV: Protocolo final TT2020-A041

Estimado Luis:

Acuso de recibido y estoy de acuerdo con el documento anexo.

Saludos

Dr. Víctor Manuel Silva García

De: Luis Bautista <luis.bautista_escom.ing@outlook.com>
Enviado: martes, 1 de febrero de 2022 23:13
Para: Victor Manuel Silva Garcia <vsilvag@ipn.mx>
Asunto: [ADVERTENCIA, MENSAJE EXTERNO] RV: Protocolo final TT2020-A041

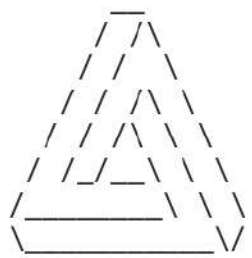
Confirmas Acuse de Recibido del protocolo

De: Benjamín L. <mobius_95@hotmail.com>
Enviado: viernes, 28 de enero de 2022 12:07
Para: Luis Bautista <luis.bautista_escom.ing@outlook.com>
Asunto: Re: Protocolo final TT2020-A041

Hola Luis.

Recibí y estoy de acuerdo con el documento anexo.

Saludos.



Dr. Benjamín Luna Benoso
ESCOM-IPN

De: Luis Bautista <luis.bautista_escom.ing@outlook.com>
Enviado: viernes, 28 de enero de 2022 04:17 p. m.
Para: Victor Manuel Silva Garcia <vsilvag@ipn.mx>; Benjamin Luna Benoso <mobius_95@hotmail.com>
Asunto: Protocolo final TT2020-A041

Hola buenas tardes profesores
Escribo para compartirles la última versión del protocolo que fue aprobada para el trabajo terminal TT2020-A041. Del mismo modo, les pido su acuse recibido para confirmar que estén enterados y están de acuerdo en que esta versión de utilizar para el disco que se entregara en la CATT.
De ante mano, muchas gracias.
¡¡Saludos!!