JÓVENES EN LA CIENCIA
REVISTA DE DIVULGACIÓN CIENTÍFICA

ENCRIPTACIÓN POR MEDIO DE POLINOMIOS ORTOGONALES

Moreno Vázquez, Francisco Javier (1), Cabal Yépez, Eduardo (2), Ledesma-Carrillo, Luis Manuel

1 [Colegio de Nivel Medio Superior, Escuela de Nivel Medio Superior de Salamanca] | [fj.morenovazquez@ugto.mx]

2 [Departamento de Estudios Multidisciplinarios, División de Ingenierías, Campus Irapuato-Salamanca, Universidad de Guanajuato] | [educabal@ugto.mx]

3 [Departamento de Estudios Multidisciplinarios, División de Ingenierías, Campus Irapuato-Salamanca, Universidad de Guanajuato] | [l.m.ledesmacarrillo@gmail.com]

Resumen

Vivimos en una era donde todo lo que nos rodea, todo con lo que interactuamos, todo aquello que nos ayuda en nuestro estudio o trabajo (smartphones, tablets, laptops) está sumergido en una gran cantidad y daos y señales de los cuales la gran mayoría de estos son datos personales, tales como cuenta bancaria, domicilio, lugares que frecuentamos, etc. Debido a esto estamos expuestos a que toda esta información e imágenes sea fácilmente vulnerada y utilizada con fines ilícitos violando nuestra privacidad e integridad. Por ello, se han diseñado procesos y mecanismos de encriptación para mantener, bajo muchos niveles de seguridad, un nivel de confianza en la información. La encriptación es, entonces, el proceso de volver inaccesible información que un usuario considere valiosa, y todo esto se logra mediante procesos computarizados en los cuales se realizan operaciones matemáticas de diferentes niveles de complejidad para mantener segura la información ingresada.

Abstract

This is an era where everything that surrounds us, everything we interact with, everything that helps us in our study or work (smartphones, tablets, laptops) is immersed in a large number of data and signals, which the of them are personal data, such as bank accounts, addresses, places frequently visited, etc. Hence, personal information, as data and images, is exposed to being easily stolen and used for illicit purposes breaking our privacy and integrity. Therefore, encryption processes and mechanisms have been designed to maintain, under many levels of security, a level of confidence on information. Encryption is the process of making inaccessible information that a user considers valuable, and all this is achieved through computerized mechanisms on which mathematical operations of different levels of complexity are performed to keep the information entered safe.

Palabras Clave MATLAB; Llave pública; Llave privada; Matriz de Hadamard; Encriptación

INTRODUCCIÓN

Marco Teórico

Criptografía

La palabra Criptografía proviene del griego "kryptos" que significa oculto, y "graphia", que significa escritura. La Criptografía es una técnica, o un conjunto de técnicas, que originalmente tratan sobre la protección o el ocultamiento de la información frente a observadores no autorizados. [1]

Criptosistemas

Puede definirse formalmente un criptosistema como una quintupla (M, C, K, E, D), donde:

1. M representa el conjunto de todos los mensajes sin cifrar (la imagen).
2. C representa el conjunto de todos los posibles mensajes cifrados, o criptogramas.
3. K representa el conjunto de claves que se pueden emplear en el criptosistema.
4. E es el conjunto de transformaciones de cifrado o familia de funciones que se aplica a cada elemento de M para obtener un elemento de C. Existe una transformación diferente Ek para cada valor posible de la clave k.
5. D es el conjunto de transformaciones de descifrado, análogo a E. [1]

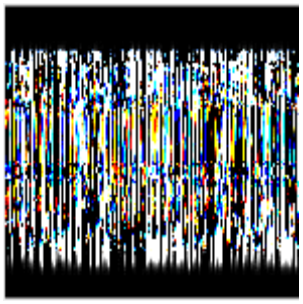

IMAGEN 1: Ejemplo Imagen Encriptada

- *Criptosistemas simétricos*

  Son aquellos que emplean una misma clave tanto para cifrar como para descifrar. Presentan el inconveniente de que para ser empleados en comunicaciones la clave k debe estar en posesión tanto en el emisor como en el receptor, lo cual nos lleva preguntarnos cómo transmitirles a los participantes en la comunicación esa clave de forma segura. [1]

- *Criptosistemas asimétricos*

  Son aquellos que emplean una doble clave (kp,kP), kp se la conoce como clave privada y kP se la conoce como clave pública. Estos criptosistemas deben cumplir además que el conocimiento de la clave pública kP no permita calcular la clave privada kp. Sin la clave privada (que no es deducible a partir de la clave pública) un observador no autorizado del canal de comunicación será incapaz de descifrar el mensaje cifrado. [1]

Matrices de Hadamard

Una matriz de Hadamard de orden N es una matriz formada por 1's y -1's tal que sus filas son ortogonales. Dada una matriz de Hadamard, podemos encontrar otra equivalente en la cual la primera fila y la primera columna consistan enteramente de +1's. Tal matriz de Hadamard se denomina normalizada. [2]

Jacques Salomon Hadamard

Fue un matemático francés (1865 – 1963) el cual hizo grandes contribuciones en:

a) teoría de números

b) teoría de la función compleja

c) geometría diferencial

d) ecuaciones en derivadas parciales

e) Identidad de Hadamard

Identidad de las Matrices de Hadamard

Sea H una matriz de Hadamard de orden *n*, debido a sus propiedades de ortogonalidad entre sus columnas y filas se llega a cumplir la siguiente identidad:

$$HH^{\mathrm{T}} = nI_n$$

IMAGEN 2: Identidad de Hadamard

Donde **H** es la matriz de Hadamard de orden *N;* $\mathbf{H}^{\mathbf{T}}$ es la matriz transpuesta de la matriz de Hadamard; **n** es el tamaño de la matriz de Hadamard; **In** es la matriz identidad de orden *N*.

Esta identidad en las matrices de Hadamard, además de sus propiedades ortogonales y que solo se conforma de 1's y -1's hacen que la matriz de Hadamard sea el medio perfecto y más fiable para encriptar señales, imágenes o cualquier dato que pueda agruparse en matrices.

Antecedentes

Hasta la década de 1970, la criptografía era un área estudiada y usada solamente por cuerpos de inteligencia militar, ya que en un comienzo esta fue utilizada para interceptar y descifrar códigos enemigos. Durante 1980, las industrias financieras y telecomunicaciones comenzaron a implementar dispositivos criptográficos de hardware. La primera aplicación criptográfica de marcado masivo fue el sistema de telefonía móvil digital a finales de los años ochenta. [3]

MATERIALES Y MÉTODOS

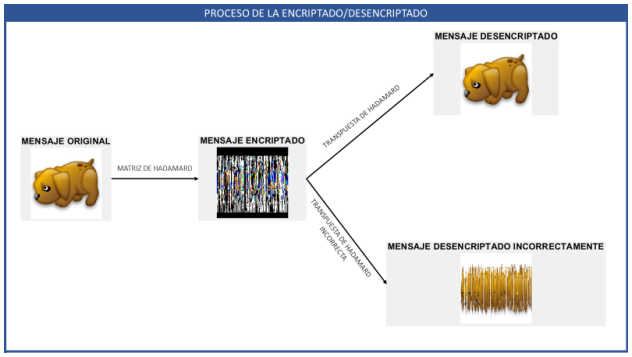

IMAGEN 3: Proceso para llevar a cabo la encriptación y la desencriptación de una imagen

Fases de la encriptación

Fase 1. Generación de la llave pública y privada

La llave pública utilizada en este método de encriptación siempre es la misma, una matriz de Hadamard de orden N de acuerdo con el tamaño de la imagen. La llave privada se logra crear por medio de un movimiento aleatorio de filas y columnas las cuales son mezcladas varias veces para lograr una matriz completamente diferente a la original. Las columnas las cuales fueron cambiadas se guardan y son datos los cuales el que recibe y el que envía el mensaje conocen.

Fase 2. División de los planos de colores

Las imágenes a las cuales estamos acostumbrados a utilizar no son solamente una imagen, son 3 imágenes diferentes cada una de ellas contiene una variación diferente de los colores primarios Rojo, Azul y Verde, es por esto por lo que se separan estas 3 diferentes matrices para poder llevar a cabo el proceso de encriptación.

Fase 3. Generar la llave privada

Por medio de un cambio aleatorio se intercambian columnas y filas de la matriz de Hadamard para que se genere una llave única y la encriptación pueda ser lo más segura posible.

Fase 4. Encriptar cada plano de la imagen

Se realiza una sencilla multiplicación de matrices entre los valores de cada plano de color de la imagen con la matriz de Hadamard ya con las columnas y filas intercambiadas.

Fase 5. Unir los planos encriptados

Se realiza una nueva matriz y al igual como se hizo para extraer los planos de la imagen, estos planos son reubicados y unidos a una nueva imagen.

Fases de la desencriptación

Fase 1. División de los planos de colores

La imagen encriptada es separada en cada plano de color para poder trabajar los planos por separado y desencriptar de uno en uno.

Fase 2. Identidad de las matrices de Hadamard

Basándonos en las diferentes propiedades de la matriz de Hadamard y recordando la identidad de Hadamard (imagen 2), lo que buscamos es conseguir una matriz identidad, es decir, una matriz que no afecte nuestra matriz inicial es por ello que la matriz de la imagen encriptada es multiplicada por la transpuesta de la matriz de Hadamard que se utilizo como llave privada y después es dividida por el tamaño de la matriz.

Fase 3. Unir los planos desencriptados

Los planos desencriptados son unidos en una nueva matriz del modo inverso al cual los planos fueron extraídos.

RESULTADOS Y DISCUSIÓN

Utilizamos una imagen cuadrada de 512 pixeles para que coincidiera con la naturaleza cuadrada de la matriz de Hadamard de igual tamaño.

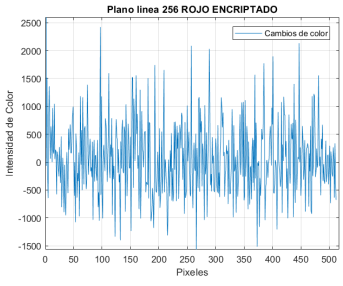

IMAGEN 5: Intensidad de color en la fila 256 plano rojo, imagen encriptada

IMAGEN 4: Intensidad de color en la fila 256 plano rojo, imagen original

En las siguientes imágenes se muestran los llamados “planos de línea” de la imagen, los cual son toda una fila que se extrajo de la imagen para ver cuáles son las variaciones en la intensidad del tono en la línea extraída (que en este caso es la fila 256 del plano rojo de la imagen mensaje).

En la imagen 4 se visualiza cual es la variación original de los tonos de rojo en el mensaje. En la imagen 4 se puede ver como se vio afectada está variación debido a la encriptación utilizando una matriz de Hadamard. Y en la imagen 6 se ve como al aplicar la lógica de desencriptación utilizando la identidad de Hadamard se vuelve a obtener el mismo patrón de intensidades que en la imagen original. Como una muestra de lo siguiente, si intentamos desencriptar la imagen con una matriz de Hadamard la cual no contenga la llave privada que le aplicamos, esta imagen se verá distorsionada y no nos devolverá el mismo patrón de intensidades, lo cual se observa en la imagen 7.

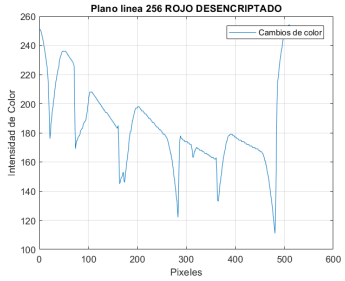

IMAGEN 6: Intensidad de color en la fila 256 plano rojo, imagen desencriptada

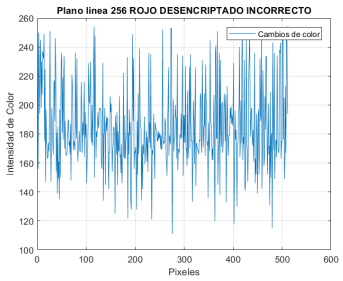

IMAGEN 7: Intensidad de color en la fila 256 plano rojo, imagen desencriptada incorrectamente

CONCLUSIONES

Se logró crear un algoritmo de encriptación y desencriptación para proteger codificar una imagen y mantener un nivel de seguridad al hacer uso de estas, se propone en un futuro aumentar el nivel de seguridad haciendo un manejo más intensivo de las matrices de Hadamard para usarlas de lleno en señales eléctricas y electrónicas.

AGRADECIMIENTOS

Primeramente, agradecer al Dr. Eduardo Cabal Yépez brindarme la oportunidad de participar en su proyecto de investigación y el apoyo que me brindó muchísimas facilidades a lo largo del proyecto, también agradecer a mi co-asesor el Dr. Luis Manuel Ledesma Carrillo por los consejos y apoyo en el trabajo realizado.

También agradecer a la Universidad de Guanajuato la invitación a este programa, ya que como estudiantes este tipo de actividades nos ayudan a crecer como persona y como estudiante.

REFERENCIAS

[1] Recuperado de: http://www.dma.fi.upm.es/recursos/aplicaciones/matematica_discreta/web/aritmetica_modular/criptografia.html
[2] Recuperado de: http://www.scielo.sa.cr/pdf/rmta/v18n2/a01v18n2.pdf
[3] Zavala Díaz Jonathan, Cabal Yépez Eduardo, (2017) “Encriptación por medio de polinomios ortogonales”, Jóvenes en la Ciencia, Vol. 3 no. 2, Verano de la Investigación Científica, pp 2333-2334