ENCRIPTACIÓN DE DATOS MEDIANTE EL CIFRADO DE HILL: RECURSO DIDÁCTICO PARA MATRICES INVERTIBLES

Luciano N, Cancellieri**, Luciano Savoie**, Ernesto Klimovsky*, Mercedes Gaitán*
Universidad Tecnológica Nacional, Facultad Regional Paraná.
Avenida Almafuerte 1033 (3100) Paraná, Entre Ríos, Argentina

*Tutor
**Autor en correspondencia
E-mail de contacto: cancellieriln@gmail.com - erklimo@gmail.com

Resumen

El objetivo de este trabajo es presentar un método didáctico complementario en la cátedra Álgebra y Geometría Analítica (AyGA), destinado a estudiantes de Ingeniería Electrónica. Se busca contribuir a generar competencias genéricas de las establecidas por el Consejo Federal de Decanos de Ingeniería (CONFEDI) para un ingeniero. Para la conformación de esta herramienta educativa, se recurre a una aplicación en el campo de la Ingeniería que consta del empleo de Álgebra Lineal para la encriptación de datos, focalizado en la utilización de matrices invertibles. En este desarrollo se incluyen conceptos introductorios de la cátedra Sistemas de Comunicaciones y también se incorporan recursos de software que se desprenden de la cátedra Informática I, lo que permite realizar una articulación interdisciplinar con AyGA. Como resultado, se obtuvo un recurso didáctico para la enseñanza. Se elaboró la resolución analítica de una aplicación práctica y, además, se logró la implementación del algoritmo matemático desarrollado en una aplicación de software. La labor realizada muestra una aplicación del Álgebra Lineal en el área de la Ingeniería, reafirmando la importancia de que el estudiante en el aula adquiera la noción de la relevancia de esta materia en su carrera universitaria.

Introducción

La presente investigación se desarrolla dentro del PID “Aportes de Matemática Aplicada en Ingeniería sustentados en elementos de Álgebra Lineal” enmarcado en el Grupo de Investigación en la Enseñanza de la Matemática en Carreras de Ingeniería (GIEMCI). En la misma se busca que el contenido matemático desarrollado en la cátedra AyGA trascienda hacia una implementación práctica en la que los estudiantes tomen contacto con situaciones reales del campo de la ingeniería. Esto tiene como finalidad despertar el interés de éstos, a la vez que se los introduce en distintas ramas de la Ingeniería Electrónica logrando una articulación multidisciplinar y una mejora de sus desarrollos por competencias, que se definen según el Consejo Federal de Decanos de Ingeniería (CONFEDI) como “la capacidad de articular eficazmente un conjunto de esquemas (estructuras mentales) y valores, permitiendo movilizar (poner a disposición) distintos saberes, en un determinado contexto con el fin de resolver situaciones profesionales” (CONFEDI, 2008, p.6). Se propone el cifrado de datos a partir del método de Hill utilizando una matriz invertible clave, con la que a través de operaciones algebraicas se logra la encriptación. A fin de simplificar el desarrollo, la información que se procede a cifrar es una imagen en escala de grises. El cifrado se obtiene implementando una serie de comandos del software matemático MatLab.

Cifrado

El manejo de la información cumple un rol fundamental en la vida de cada ser humano. Una técnica que se ha desarrollado es la criptografía:

> La cual a lo largo de la historia del hombre ha jugado un papel fundamental, a partir de la necesidad de intercambiar información de forma confidencial. Actualmente, con la evolución de las tecnologías de la información y de la comunicación, esta necesidad se encuentra

> presente en aspectos de nuestra vida cotidiana “[…]”, con la finalidad de que información sensible “[…]”, no sea interceptada de forma fraudulenta. (Cancellieri et al., 2020, p.1)

En el desarrollo expuesto se recurre a utilizar el Cifrado de Hill, el mismo “fue inventado, basándose en el álgebra lineal, por el matemático norteamericano Lester S. Hill en 1929” (Ibáñez, 2017, p.2). Este método permite cifrar texto reemplazando cada letra del alfabeto por un valor numérico, fragmentando el mensaje en vectores de tamaño m y multiplicándolos por una matriz clave K_{mxm} invertible. Luego, al multiplicar los vectores de texto cifrado por la inversa de la matriz clave K, se recuperan los vectores que contienen el mensaje original por definición de matriz inversa. En esta ocasión el desarrollo consta de cifrar una imagen en escala de grises ya que se codifica de manera similar.

Desarrollo algebraico

En esta adaptación del Cifrado de Hill para encriptar imágenes en escala de grises, se representa el valor de gris de cada píxel de la imagen original (Fig.1) en una matriz O. En este caso la matriz O será de 486x486 debido a que ese es el tamaño original. El nivel de gris de cada píxel puede tomar valores entre 0 y 255, por lo que las operaciones se realizan en módulo 256 con la finalidad de trabajar siempre con niveles de gris válidos.

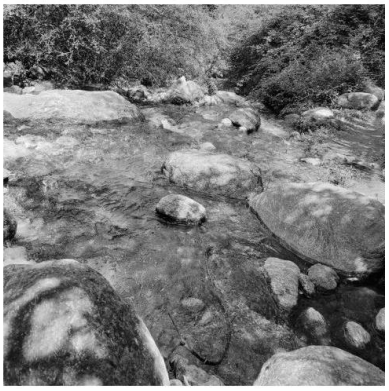

Figura 1: Imagen original.

Para realizar el cifrado se propone una matriz clave K de 3x3, la cual deberá cumplir las siguientes condiciones algebraicas (con $n=256$):

* K debe tener una matriz inversa K^{-1}.
* $mcd(|K|, n) = 1$, es decir el determinante de la matriz debe ser primo relativo con n.

(Arguello et al., 2015, p.61).

Un ejemplo de matriz clave es la siguiente:

$$K = \begin{pmatrix} 9 & 2 & 2 \\ 4 & 6 & 5 \\ 8 & 9 & 8 \end{pmatrix}$$

Se comprueba si la matriz cumple las condiciones necesarias para utilizarla en el cifrado calculando su determinante:

$$det\ K = \begin{vmatrix} 9 & 2 & 2 \\ 4 & 6 & 5 \\ 8 & 9 & 8 \end{vmatrix} = 9.6.8 + 2.5.8 + 4.9.2 - 2.6.8 - 2.4.8 - 5.9.9 = 19\ mod\ 256 = 19$$

Como $det\ K = 19 \neq 0$, la matriz K es invertible. Además, $det\ K$ es primo relativo del módulo ($mcd(19,256) = 1$), entonces posee inverso multiplicativo módulo 256.

El método adoptado para implementar el cifrado consta de recorrer la matriz O que contiene los valores de gris de la imagen original, agrupándolos en vectores V de 3x1, multiplicándolos matricialmente por la matriz clave K de 3x3 y guardándolos en una matriz vacía C que finalmente contendrá la imagen cifrada. Para la imagen seleccionada (Fig.1) los 3 primeros valores son 143, 107 y 131. A modo de ejemplo se expone el proceso de cifrado para los mismos:

$$K\,V = \begin{pmatrix} 9 & 2 & 2 \\ 4 & 6 & 5 \\ 8 & 9 & 8 \end{pmatrix} \begin{pmatrix} 143 \\ 107 \\ 131 \end{pmatrix} = \begin{pmatrix} 1763 \\ 1869 \\ 3155 \end{pmatrix} = \begin{pmatrix} 227 \\ 77 \\ 83 \end{pmatrix} (mod\ 256) = Y$$

Como se aprecia en la ecuación anterior, se reemplazan los valores de nivel de gris originales por nuevos valores módulo 256 correspondientes al cifrado de la imagen en el vector Y de 3x1.

Para realizar el descifrado se recorre la matriz C que contiene la imagen cifrada de la misma manera que anteriormente se recorrió la matriz O. Para recuperar la imagen original se multiplica matricialmente cada vector de C de 3x1 por la inversa de la matriz clave K^{-1}. Para ejemplificar descifraremos los 3 valores encriptados en la última ecuación. Primero se calcula la matriz K^{-1}:

$$K^{-1} = \frac{(adj\ (A))^t}{|A|} = \begin{pmatrix} \frac{3}{19} & \frac{2}{19} & \frac{-2}{19} \\ \frac{8}{19} & \frac{56}{19} & \frac{-37}{19} \\ \frac{-12}{19} & \frac{-65}{19} & \frac{46}{19} \end{pmatrix}$$

Siendo 27 el inverso multiplicativo de 19 módulo 256:

$$19\,.27 = 513\ mod\ 256 = 1$$

$$K^{-1} = \begin{pmatrix} \frac{3}{19} & \frac{2}{19} & \frac{-2}{19} \\ \frac{8}{19} & \frac{56}{19} & \frac{-37}{19} \\ \frac{-12}{19} & \frac{-65}{19} & \frac{46}{19} \end{pmatrix} = \begin{pmatrix} 3x27 & 2x27 & -2x27 \\ 8x27 & 56x27 & -37x27 \\ -12x27 & -65x27 & 46x27 \end{pmatrix} =$$

$$\begin{pmatrix} 81 & 54 & -54 \\ 216 & 1512 & -999 \\ -324 & -1755 & 1242 \end{pmatrix} = \begin{pmatrix} 81 & 54 & 202 \\ 216 & 232 & 25 \\ 188 & 37 & 218 \end{pmatrix} (mod\ 256)$$

Consecuentemente se recuperan los valores iniciales por multiplicación de matrices:

$$K^{-1}\,Y = \begin{pmatrix} 81 & 54 & 202 \\ 216 & 232 & 25 \\ 188 & 37 & 218 \end{pmatrix} \begin{pmatrix} 227 \\ 77 \\ 83 \end{pmatrix} = \begin{pmatrix} 39311 \\ 68971 \\ 63619 \end{pmatrix} = \begin{pmatrix} 143 \\ 107 \\ 131 \end{pmatrix} (mod\ 256)$$

Posterior a esta comprobación numérica y siguiendo la metodología expuesta, se procede a implementarla en un software de cálculo para concretar la prueba. Se utilizan los mismos valores correspondientes a la matriz K y K^{-1}.

Implementación en Matlab

Para la aplicación en software se recurre a utilizar un programa especializado en cálculo: Matlab (Laboratorio Matricial), el cual “es un sistema interactivo, cuyo ‘dato básico’ es un arreglo que no requiere dimensionamiento. Permite resolver problemas técnicos, especialmente aquellos con formulaciones de matriz y vector, en menos tiempo del que demandan otros lenguajes como C o Fortran” (Giner, 2008, p.10).

La ventaja de utilizar Matlab es su “parecido a lenguajes de alto nivel como BASIC o C. Esto permite que el usuario pueda agrupar sentencias que utiliza frecuentemente dentro de un programa que puede ser invocado posteriormente” (Arahal, 2008, p.113).
Al programar en Matlab se utilizan recursos básicos de programación como bifurcaciones, bucles, funciones y manejo de datos del tipo: cadena de caracteres, vectores y matrices. Esto nos permite incorporar conocimientos que pertenecen a la asignatura Informática I. Además, la selección de esta herramienta informática se fundamenta a partir de reconocerse muy utilizada en materias del ciclo superior de Ingeniería Electrónica como Análisis de Señales y Sistemas, Sistemas de Comunicaciones, Técnicas Digitales III y la materia electiva Procesamiento Digital de Imágenes.

Para la implementación, es necesario recurrir a algunas instrucciones que posee MatLab vinculadas al Procesamiento Digital de Imágenes, las cuales se encuentran resumidas en la Fig.2:

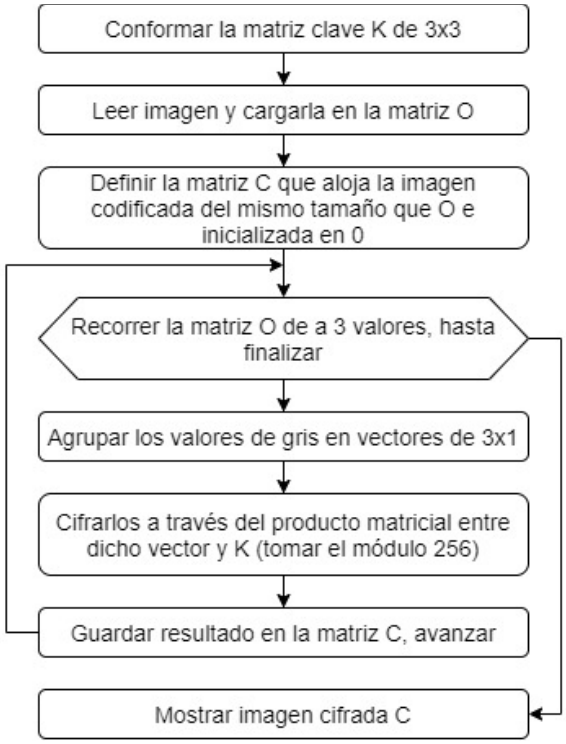

Figura 2: Algoritmo de Cifrado

En la Fig.3, se tiene a la izquierda la imagen original (Fig. 1), y a la derecha se grafica la imagen encriptada luego de que se le aplica el procesamiento descripto en Fig. 2. Se concluye en una imagen cifrada en la que a simple vista no es posible reconocer su contenido inicial.

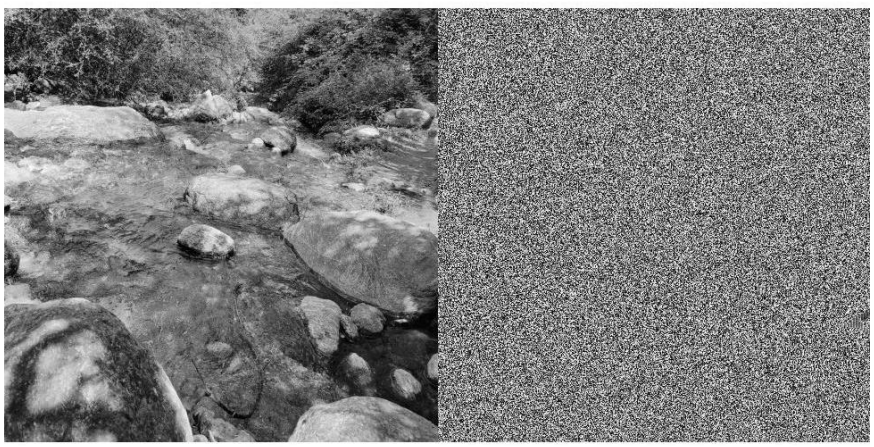
Figura 3: Original (izquierda) Encriptada (derecha).

Una vez que se obtiene la imagen correctamente cifrada, se procede a utilizar el método algebraico para el descifrado en Matlab con el algoritmo ilustrado en la Fig.4.

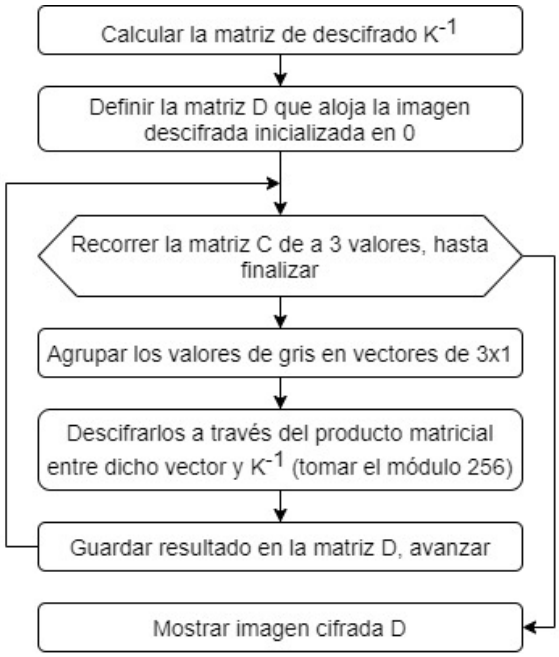

Figura 4: Algoritmo de Descifrado.

Finalmente se observa la imagen recuperada satisfactoriamente con el descifrado ejecutado en Fig.5.

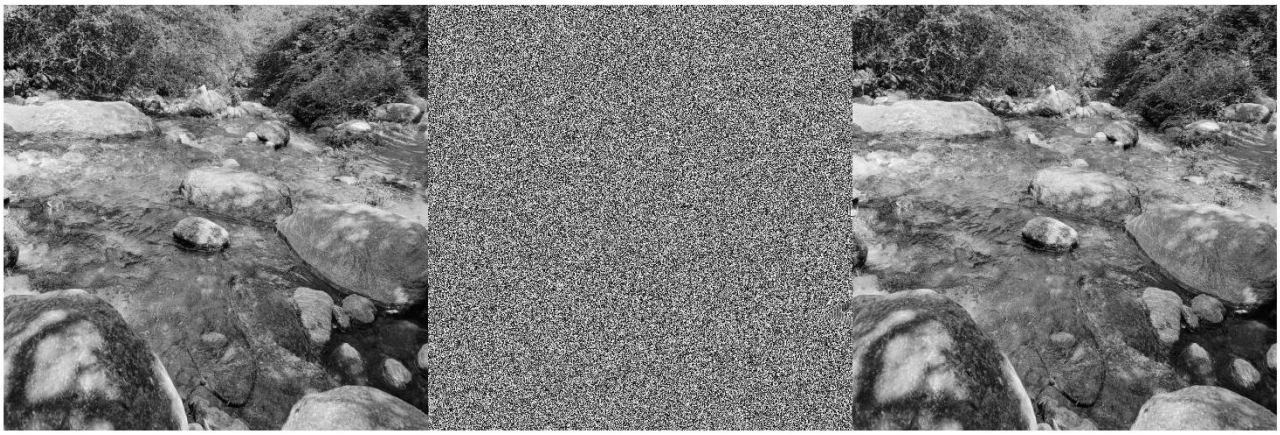

Figura 5: Imagen Original (izquierda) Imagen Cifrada (centro) Imagen Descifrada (Derecha).

Conclusiones

Se obtuvo una aplicación práctica didáctica de matrices invertibles y producto matricial que les permite a los estudiantes tomar noción de la utilidad de estos temas, a la vez que se mejoran sus competencias y se incorporan conocimientos introductorios a distintas asignaturas y ramas de Ingeniería Electrónica.

El recurso logrado muestra de forma gráfica y llamativa los resultados tanto parciales como totales que se obtienen al valerse de los algoritmos desarrollados en una aplicación de software, invitando a los estudiantes a tomar la iniciativa de familiarizarse con los distintos tópicos tratados.
La tarea desarrollada posee un gran potencial para la propuesta de actividades asíncronas complementarias al desarrollo del dictado de clases. Dicho esto, la propuesta toma aún mayor relevancia en el contexto de actualidad, donde producto de la pandemia de COVID-19 prevalecen

las clases virtuales y todas las herramientas que despierten el interés en el estudiantado son de gran utilidad a fines de evitar la deserción o dificultades de atención en el aprendizaje durante el transcurso de los años iniciales de las carreras universitarias.

Trabajo futuro

Como mejora y ampliación de la metodología se plantea realizar el cifrado a través de una matriz clave K dinámica, es decir, que varíe con cada encriptación que se realiza, reduciendo así la probabilidad que la clave sea descubierta. Una variante que mejora la seguridad del sistema, a la vez que incrementa la complejidad algebraica, es aumentar el tamaño de la matriz clave. Otra opción es la utilización de algoritmos de cifrado más complejos, donde se permite un mayor desarrollo tanto del contenido matemático como el referido a la encriptación. Como última alternativa se propone utilizar imágenes en color u otro tipo de dato codificable con el objetivo de diversificar las aplicaciones de la metodología.

Referencias

Arahal M.R. (2008). Fundamentos de informática para Ingeniería Aeronáutica. Escuela Técnica Superior de Ingeniería, Sevilla. Recuperado de: http://www.esi2.us.es/~jaar/Datos/FIA/FIA.pdf.

Arguello, N., Molano, T., Rojas, V & Medina, I. (agosto de 2015). Encriptación de imágenes aplicando el método de Hill. III Encuentro Internacional de Matemáticas, Estadística y Educación Matemática. Conferencia llevada a cabo en el congreso Universidad Pedagógica y Tecnológica de Colombia, Duitama, Colombia.

Cancellieri, L., Savoie, L., Klimovsky, E., y Gaitán, M. (septiembre de 2020). Criptografía: una aplicación sustentada en álgebra lineal para la educación matemática en ingeniería. Comunicación presentada en XLIII Reunión de Educación Matemática, virtUMA 2020, Reunión Anual Unión Matemática Argentina.

Consejo Federal de Decanos de Ingeniería. (2008). Resumen XLI plenario CONFEDI. Recuperado de https://www.utn.edu.ar/images/Secretarias/SGral/ReformaAcademica/B1-Competencias-Genericas-de-Egreso-del-Ingeniero-Iberoamericano.pdf

Giner, S. (2008). Curso de Matlab Entorno interactivo de cálculo y visualización vinculado a un lenguaje de programación de alto nivel. Área Departamental Ingeniería Química Facultad de Ingeniería-UNLP. Recuperado de: http://sedici.unlp.edu.ar/bitstream/handle/10915/15919/Documento_completo.pdf?sequence=1#:~:text=MATLAB%20es%20un%20sistema%20interactivo,lenguajes%20como%20C%20o%20Fortran

Ibáñez, R. (2017). Criptografía con matrices, el cifrado de Hill. Cuaderno de cultura científica. Recuperado de: https://culturacientifica.com/2017/01/11/criptografia-matrices-cifrado-hill/.