Revista de Gestión Empresarial y Sustentabilidad

http://rges.umich.mx

Diseño e implementación de una red de sustitución–permutación: análisis y resultados experimentales

Pedro Chávez Lugo [1]
Leticia Peña Morfín [2]

[1] Universidad Michoacana de San Nicolás de Hidalgo, pedro.chavez@umich.mx
[2] Universidad Michoacana de San Nicolás de Hidalgo, leticia.morfin@umich.mx

Revista de Gestión Empresarial y Sustentabilidad, Vol. 11, Núm. 1, Enero – Diciembre 2025, ISSN: 2448-6043,
pp. 1 – 17, Fecha de Recepción 20 de Junio de 2025, Fecha de Aceptación 2 de Octubre de 2025

Diseño e implementación de una red de sustitución–permutación: análisis y resultados experimentales

Resumen

Las redes de sustitución–permutación (SPN) constituyen una de las estructuras fundamentales en el diseño de algoritmos de cifrado por bloques dentro de la criptografía simétrica. Este artículo presenta el diseño e implementación de una red SPN propia, desarrollada bajo los principios de confusión y difusión propuestos por Claude Shannon. Se describe la arquitectura general del sistema, incluyendo la construcción de las cajas de sustitución (S-Box) y permutación (P-Box), la generación de subclaves. Posteriormente, se analiza el proceso de cifrado a través de pruebas experimentales orientadas a evaluar propiedades como el efecto avalancha, la no linealidad y la resistencia frente a ataques básicos de criptoanálisis diferencial y lineal.

Palabras clave: Criptografía simétrica, seguridad de la información, diseño criptográfico, análisis criptográfico.

Abstract

Substitution–permutation networks (SPNs) constitute one of the fundamental structures in the design of block cipher algorithms within symmetric cryptography. This article presents the design and implementation of a custom SPN, developed under the principles of confusion and diffusion proposed by Claude Shannon. The general architecture of the system is described, including the construction of substitution boxes (S-Boxes) and permutation boxes (P-Boxes), as well as the subkey generation process. Subsequently, the encryption process is analyzed through experimental tests aimed at evaluating properties such as the avalanche effect, nonlinearity, and resistance against basic differential and linear cryptanalysis attacks.

Keywords: Symmetric cryptography, information security, cryptographic design, cryptographic analysis.

Introducción

La necesidad de obtener y mantener protegida a la información sensible es y ha sido una de los retos constantes para las organizaciones. Conseguir esta protección en canales de comunicación o para el almacenamiento requiere de la aplicación de técnicas criptográficas como lo es la aplicación de la criptografía simétrica, asimétrica, curvas elípticas o incluso con la aplicación de técnicas esteganográficas o mediante la combinación de ambos tipos de técnicas. Este tipo de técnicas tienen una contraparte que busca romperlas con la finalidad de obtener la información sensible afectando al atributo de confidencialidad. Lo cual puede ocasionar al propietario de la información pérdida de credibilidad, confianza o en algunos casos económicas. Por estas razones se requiere de una correcta estrategia de seguridad que proteja a la información sensible en su transmisión en canales confidenciales de comunicación o para su almacenamiento y resguardo seguro.

Fundamentos de criptografía simétrica

La criptografía simétrica se basa en el principio del uso de una misma clave para los procesos de cifrado y descifrado (Stinson, D. R. (2005)). Esto implica un problema con la distribución de las claves. Cifrar la información mediante el uso de la criptografía simétrica resuelve el problema de la obtención de la confidencialidad más no el problema de compartir la clave utilizada. Existen técnicas que permiten el acuerdo de claves permitiendo solucionar el problema de la distribución de claves. La Figura 1, muestra el proceso de cifrado y descifrado mediante la criptografía simétrica. Como se puede observar una misma clave es utilizada en los procesos de cifrado y descifrado.

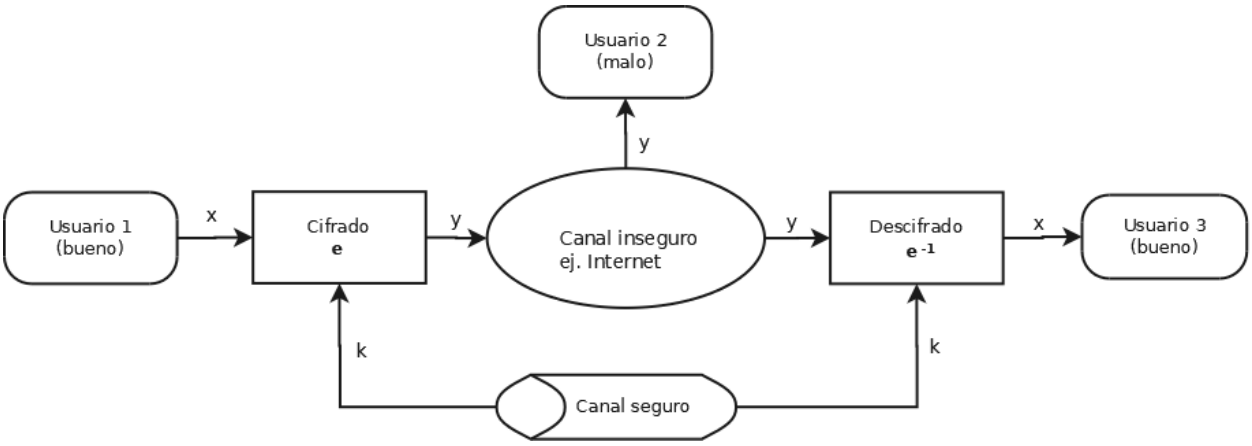

Figura 1. Proceso de cifrado y descifrado simétrico.

En el caso de la Figura 1 corresponde a la transmisión de la información cifrada por canal inseguro y seguro proporcionado por la aplicación del proceso de cifrado. Una alternativa similar se presenta en el almacenamiento de la información, en lugar de ser transmitida esta es almacenada. Es fundamental para el caso del uso de la criptografía simétrica el resguardo de la clave utilizada, el extravío de la clave es un escenario que se debe evitar ya que en este caso se estará imposibilitado de la aplicación del proceso de descifrado implicando con la aplicación de técnicas del criptoanálisis, las cuales demandan una gran cantidad de tiempo y recursos. Incluso una frustración al no ser posible romper con el algoritmo de cifrado simétrico, que es finalmente lo que se busca obtener en la aplicación de la criptografía (Swenson, C. (2008)).

Cifrado por bloques

En la criptografía simétrica el proceso de cifrado puede realizarse por flujo o bloque. En el caso del cifrado simétrico por flujo se transforma bit a bit utilizando una misma clave, mientras que por bloques se definen longitudes de bit de igual tamaño con una clave de igual o mayor. La Figura 2, muestra el cifrado simétrico por flujo o bloques.

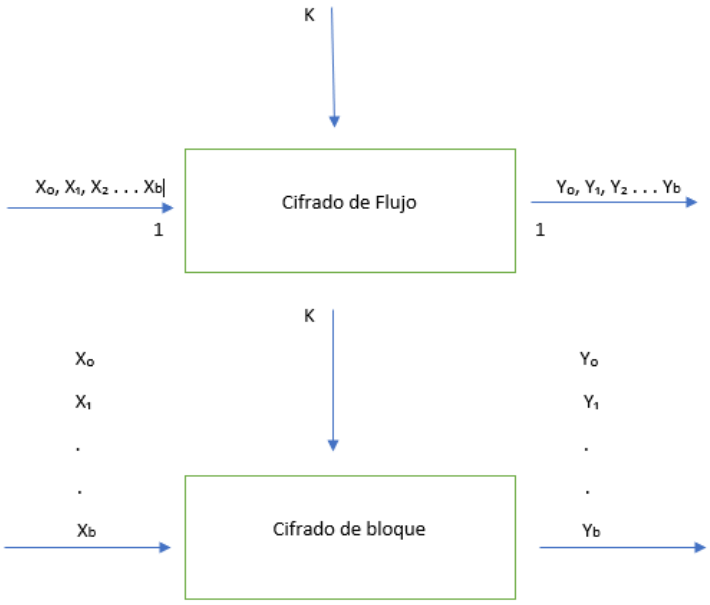

Figura 2. Cifrado de flujo y de bloque.

En el caso de esta propuesta de la SPN propia se utiliza el cifrado simétrico de bloque para una longitud 256 bit de bloque y clave (K). Lo cual permite generar un espacio de claves $2^{256} = 1.15\text{x}10^{77}$ posibles claves.

Modo de operación

El modo de operación es una selección fundamental el proceso de cifrado simétrico, una selección incorrecta por ejemplo el modo ECB (Electronic Code Book), refleja información en caso de la presencia de patrones repetidos. Para esta propuesta se utiliza el modo CBC (Cipher Block Chaining) (Paar, C., & Pelzl, J. (2010)).

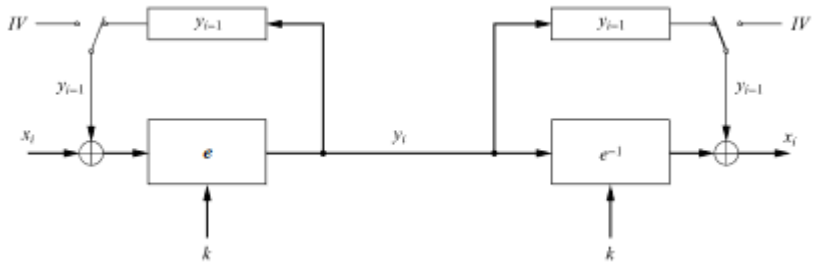

Figura 3. Modo de operación CBC.

La Figura 3, muestra el proceso de cifrado simétrico de bloques mediante el modo de operación CBC. Este modo de operación permite la correcta transformación de los bloque entrada repetidos considerados como patrones repetitivos. El algoritmo de cifrado se aplica posterior a una operación XOR que para el caso del primer bloque se realiza con un IV (Vector de Inicialización) y para los posteriores bloques la operación XOR se realiza con los bloques previamente cifrados. El modo CBC fue seleccionado para aplicarlo en la SPN propia.

Redes de sustitución–permutación

Para el cifrado simétrico se pueden utilizar las estructuras correspondientes a una red de Feistel y red de sustitución-permutación (William Stallings. (2017)) (Douglas C. Montgomery, George C. Runger. (2014)) (Jonathan Katz, & Yehuda Lindell. (2020)). Para el caso de esta propuesta se hace uso de una estructura correspondiente a una red de sustitución-permutación. La cual se basa en el principio de confusión y difusión (Claude Shannon. (1949)). La confusión se realiza mediante una caja de sustitución y la difusión mediante una caja de permutación, las cuales son aplicadas en un cierto número de rondas.

S-Box (Caja de Sustitución)

Una caja de sustitución S-Box, reemplaza en el proceso de cifrado un bloque de bit por otro bloque predefinido. Caja caja de sustitución debe tener asociada su respectiva caja de

sustitución inversa que será aplicada en el proceso de descifrado. La Figura 4, muestra un ejemplo de una caja de sustitución y su respectiva inversa. Si la entrada de una caja de sustitución es 0_{16} la salida corresponde a E_{16} y en la caja inversa el valor de entrada E_{16} corresponde a la salida 0_{16}.

Caja de Sustitución S-Box

Entrada	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
Salida	E	4	D	1	2	F	B	8	3	A	6	C	5	9	0	7

Caja de Sustitución Inversa S-Box^{-1}

Entrada	E	4	D	1	2	F	B	8	3	A	6	C	5	9	0	7
Salida	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F

Figura 4. Caja S-Box.

P-Box (Caja de Permutación)

Una caja de permutación P-Box, reordena los bit en una posición diferente en un bloque final. Caja de permutación debe tener asociada su respectiva caja de permutación inversa que será aplicada en el proceso de descifrado. La Figura 5, muestra un ejemplo de una caja de permutación de 16 bit y su respectiva inversa. Si la posición 6 de entrada corresponde a la posición de salida 9 y en la caja inversa la posición 9 corresponde a la posición 6 de salida.

Caja de Permutación P-Box

Posición original	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Posición permutada	0	4	8	12	1	5	9	13	2	6	10	14	3	7	11	15

Caja de Permutación Inversa P-Box^{-1}

Posición original	0	4	8	12	1	5	9	13	2	6	10	14	3	7	11	15
Posición permutada	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15

Figura 5. Caja P-Box.

Estructura por rondas

Una red de sustitución-permutación requiere la aplicación de diferentes rondas que implican la confusión y difusión de los datos. Para esto se aplican las cajas de sustitución y permutación combinadas con la operación XOR. La Figura 6, muestra la constitución de una ronda para una SPN.

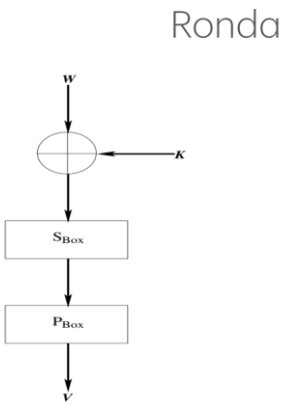

Figura 6. Ronda, combinación XOR, confusión y difusión.

Las rondas son aplicadas de manera repetitiva un cierto número de veces, como se puede observar en la Figura 7, en la SPN propia se definieron 13 rondas.

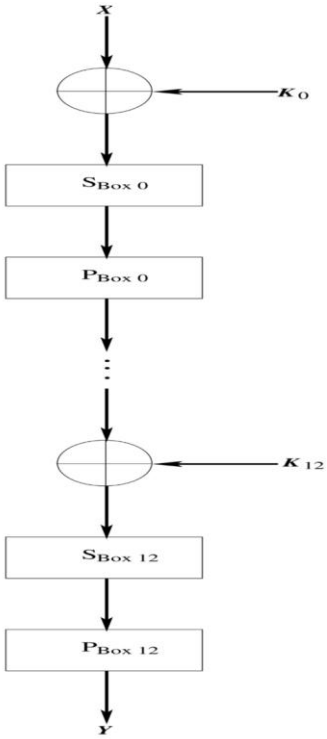

Figura 7. Rondas definidas en la SPN propia.

En el caso de trece rondas se requiere la generación de 12 claves o subclaves a utilizar en las diferentes rondas, lo cual demanda su generación o derivación a partir de la clave inicial proporcionada generalmente por un usuario.

SPN propia

En el diseño de la SPN propia se utilizó al generador de números aleatorios /dev/random del sistema operativo GNU/Linux. Dicho generador permitió generar trece diferentes cajas de sustitución y trece diferentes cajas permutación, en ambos casos con sus respectivas cajas inversas. La generación de subclaves también se realizó con el mencionado generador de números aleatorios.

Resultados

Para la aplicación del proceso de cifrado de la SPN propia se utilizaron dos diferentes imágenes que presentan patrones repetidos, correspondiente a una amplia presencia de algunos colores.

Primera imagen

La Figura 8, muestra la primera imagen seleccionada para el proceso de cifrado. Como puede observarse la imagen tiene patrones repetitivos, amplia presencia del color negro y tonalidades grises.

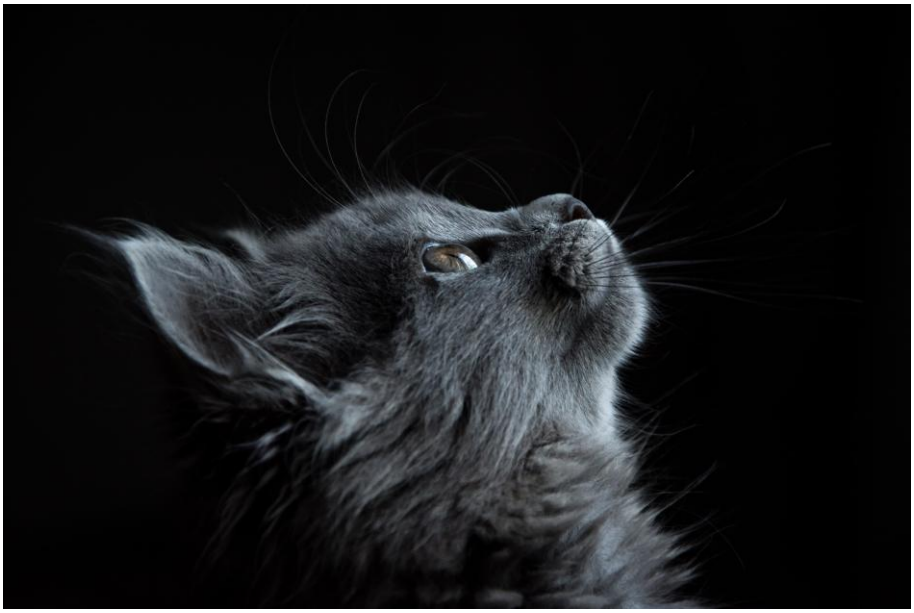

Figura 8. Primera imagen.

La Figura 9, muestra el histograma de la primera imagen, en el cual se revela la presencia de patrones predominantes, concentrados en los primeros valores del rango de 0 a 255 y con mayor predominancia en uno de estos.

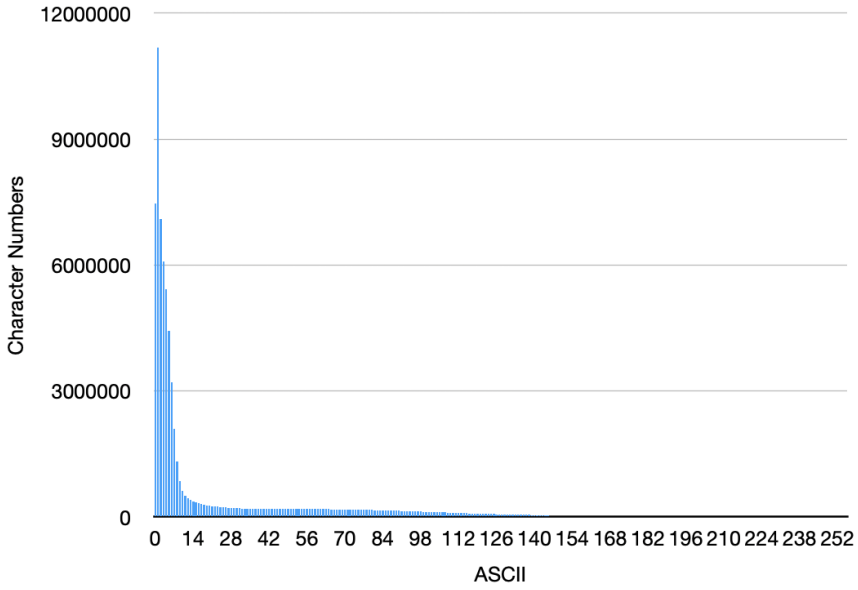

Figura 9. Histograma de la primera imagen.

Primera imagen cifrada

El resultado de la primera imagen cifrada con la SPN propia se muestra en la Figura 10.

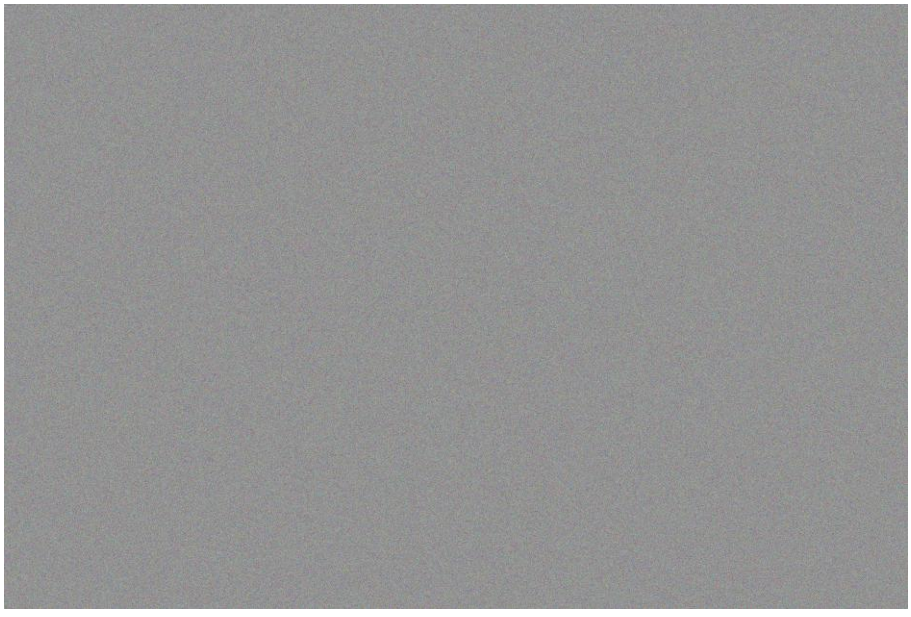

Figura 10. Primera imagen cifrada.

La Figura 11, muestra el histograma de la primera imagen cifrada, en el cual se revela la eliminación de patrones predominantes o repetidos, reflejando la presencia de todos los valores del rango de 0 a 255 correspondiente a una distribución homogénea.

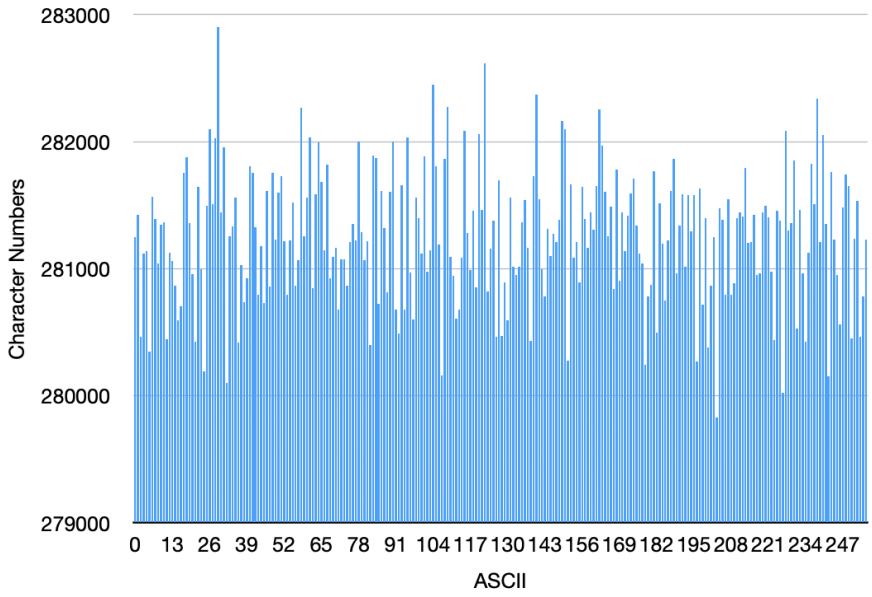

Figura 11. Histograma de la primera imagen cifrada.

Segunda imagen

La Figura 12, muestra la segunda imagen seleccionada para el proceso de cifrado. Como puede observarse la imagen tiene patrones repetitivos, amplia presencia del color blanco y algunas tonalidades como lo son el gris, verde y café.

Figura 12. Segunda imagen.

La Figura 13, muestra el histograma de la segunda imagen, en el cual se revela la presencia de patrones predominantes, concentrados en los últimos valores del rango de 0 a 255 y con mayor predominancia en uno de estos.

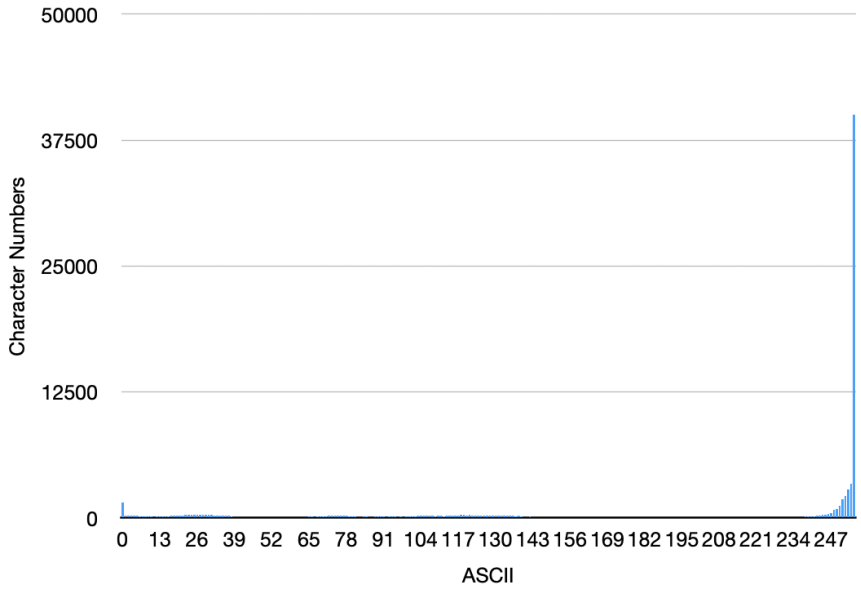

Figura 13. Histograma de la segunda imagen.

Segunda imagen cifrada

El resultado de la segunda imagen cifrada con la SPN propia se muestra en la Figura 14.

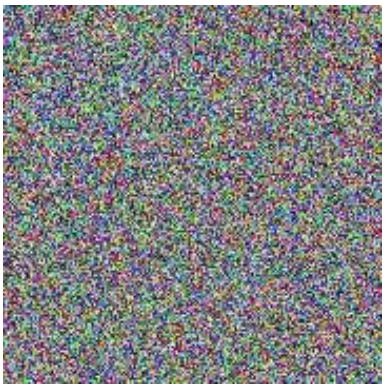

Figura 14. Segunda imagen cifrada.

La Figura 15, muestra el histograma de la segunda imagen cifrada, en el cual se revela la eliminación de patrones predominantes o repetidos, reflejando la presencia de todos los valores del rango de 0 a 255 correspondiente a una distribución homogénea.

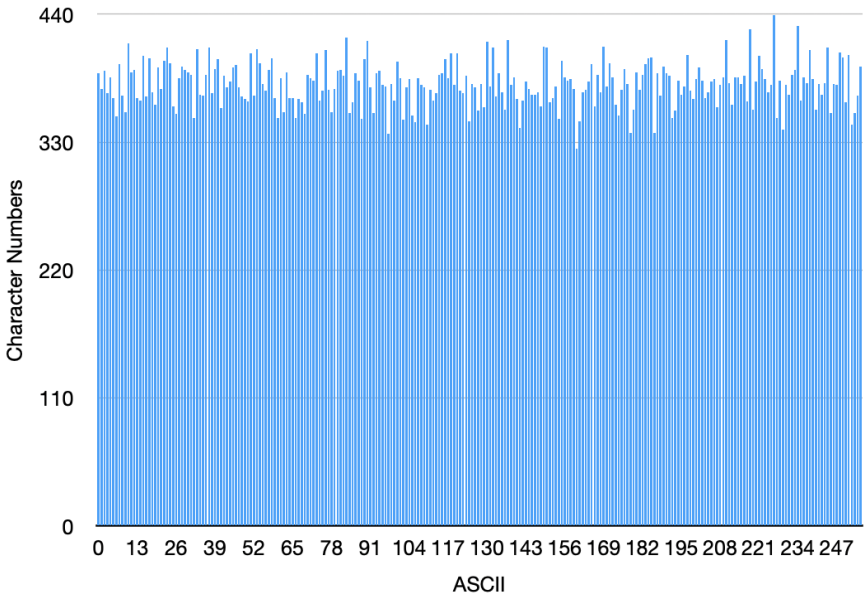

Figura 15. Histograma de la segunda imagen cifrada.

Medidas estadísticas utilizadas

Error Absoluto Medio - MAE

El Error Absoluto Medio es utilizado para calcular el cambio de cada dato de la imagen con el dato cifrado respectivo, esperando para el caso del cifrado resultante que los datos obtenidos no se parezcan a los datos originales. La Ecuación 1 define al Error Absoluto Medio (Kotz, S., Read, C. B., Balakrishnan, N., & Vidakovic, B. (2006)).

$$\boldsymbol{MAE} = \frac{\mathbf{1}}{\boldsymbol{n}}|\boldsymbol{x_i} - \boldsymbol{y_i}|$$

Ecuación 1. Error Absoluto Medio - MAE

El Coeficiente de Correlación Lineal de Pearson es utilizado para determinar qué tan parecidos son los datos de la imagen y los datos de su respectivo cifrado. La Ecuación 2 se utiliza para determinar el Coeficiente de Correlación Lineal, el cual puede variar en el rango de $-1 \leq r \leq +1$. En donde el valor -1 corresponde a una correlación lineal negativa fuerte, +1 es una correlación lineal positiva fuerte y 0 denota que no existe correlación (Douglas C. Montgomery, George C. Runger. (2014)). Para obtener una buena calidad de cifrado el coeficiente de correlación lineal ideal es r = 0, dicho valor denotara que los datos cifrados no guardan relación alguna con los datos originales.

$$\boldsymbol{r} = \frac{\boldsymbol{n}\sum_1^n \boldsymbol{x_i y_i} - \sum_1^n \boldsymbol{x_i} \sum_1^n \boldsymbol{y_i}}{\sqrt{[\boldsymbol{n}\sum_1^n \boldsymbol{x_i}^2 - (\sum_1^n \boldsymbol{x_i})^2][\boldsymbol{n}\sum_1^n \boldsymbol{y_i}^2 - (\sum_1^n \boldsymbol{y_i})^2]}}$$

Ecuación 3. Coeficiente de Correlación Lineal.

Resultados obtenidos

La Tabla 1, muestra las medidas estadísticas obtenidas entre la primera, segunda imagen y su respectivo cifrado con la SPN propia.

Imagen	MAE	Coeficiente de Correlación
Primera imagen cifrada con SPN propia	112.73 (44%)	-1.9308×10^{-5}
Segunda imagen cifrada con SPN propia	108.88 (42%)	-0.0066

Tabla 1. Tabla de valores MAE y Coeficiente de Correlación entre imágenes originales e imágenes cifradas.

Conclusiones

Las imágenes cifradas demuestran una distribución homogénea, en la cual se tiene presencia de todos los valores de 0 a 255, esta homogeneidad en la frecuencia de los valores impide la formación de patrones repetidos presentes en las primera y segunda imagen. El valor de error absoluto medio MAE obtenido varió en el rango de un 42 a 44 % lo cual denota que se tiene una calidad de cifrado buena. Para el caso del coeficiente de correlación lineal se obtuvo el valor de 0, lo cual indica que se tiene una correlación nula entre la primera y segunda imagen y sus respectivos cifrados. La implementación demuestra una capacidad efectiva para transformaciones sin relación con los datos originales. El cifrado generó estructuras visibles sin repeticiones perceptibles, lo cual es crucial para la protección de contenidos digitales.

Trabajos Futuros

Como trabajos futuros se considera realizar un criptoanálisis diferencial y lineal, optimizar el código para realizar una comparación de tiempo de ejecución y calidad de cifrado de otros algoritmos de cifrado simétrico como AES, TwoFish, entre otros.

Referencias Bibliográficas

Swenson, C. (2008). Modern cryptanalysis: techniques for advanced code breaking. John Wiley & Sons.

Stinson, D. R. (2005). Cryptography: theory and practice. Chapman and Hall/CRC.

Paar, C., & Pelzl, J. (2010). Understanding cryptography (Vol. 1). Springer-Verlag Berlin Heidelberg.

Kotz, S., Read, C. B., Balakrishnan, N., & Vidakovic, B. (2006). Encyclopedia of Statistical Sciences (2nd ed.). Wiley.

Douglas C. Montgomery, George C. Runger. (2014). Applied Statistics and Probability for Engineers (6th ed.). John Wiley & Sons.

Claude Shannon. (1949). Communication theory of secrecy systems. Bell System Technical Journal, 28(4), 656–715.

William Stallings. (2017). Cryptography and Network Security: Principles and Practice (7th ed.). Pearson.

Jonathan Katz, & Yehuda Lindell. (2020). Introduction to Modern Cryptography (3rd ed.). CRC