Revista de Gestión Empresarial y Sustentabilidad

http://rges.umich.mx

Estudio comparativo de los modos de operación de cifrado ECB, CBC, OFB y CFB basado en una arquitectura de cifrado por bloques SPN-16

Rigoberto López Escalera[1]
Pedro Chavéz Lugo[2]

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

Revista de Gestión Empresarial y Sustentabilidad, Vol. 11, Núm. 1, Enero – Diciembre 2025, ISSN: 2448-6043, pp. 37 – 50, Fecha de Recepción 5 de Septiembre de 2025, Fecha de Aceptación 23 de Noviembre de 2025

Estudio comparativo de los modos de operación de cifrado ECB, CBC, OFB y CFB basado en una arquitectura de cifrado por bloques SPN-16

El avance de la tecnología y de los métodos de comunicación han ampliado las formas en que las personas intercambian información, desde idiomas tradicionales hasta sistemas especializados como braille o lengua de señas. En este contexto, garantizar la seguridad y confidencialidad de la información se vuelve fundamental, por lo que la criptografía juega un papel clave al transformar datos legibles en información cifrada accesible solo mediante una clave. Este estudio analiza métodos de cifrado aplicados a imágenes en formato BMP mediante un algoritmo de tipo SPN (Substitution Permutation Network) de 16 bit, el cual protege los datos utilizando procesos de sustitución y permutación. Se evaluaron cuatro modos de operación de cifrados por bloques: ECB (Electronic Code Book), CBC (Cipher Block Chaining), OFB (Output Feedback) y CFB (Cipher Feedback). La comparación se realizó considerando aspectos cuantitativos y cualitativos, como la calidad visual de las imágenes cifradas y la uniformidad en la distribución de los datos, con el objetivo de determinar la efectividad de cada modo en la protección de la información.

Palabras clave: Cifrado por bloques, SPN, ECB, CBC, OFB, criptografía simétrica.

Abstract

The advancement of technology and communication methods has expanded the ways in which people exchange information, ranging from traditional languages to specialized systems such as Braille and sign language. In this context, ensuring the security and confidentiality of information becomes essential, and cryptography plays a key role by transforming readable data into encrypted information that can only be accessed through a key. This study analyzes encryption methods applied to BMP images using a 16-bit SPN (Substitution Permutation Network) algorithm, which protects data through substitution and permutation processes. Four modes of operation for block ciphers were evaluated: ECB (Electronic Code Book), CBC (Cipher Block Chaining), OFB (Output Feedback), and CFB (Cipher Feedback). The comparison was conducted considering both quantitative and

qualitative aspects, such as the visual quality of the encrypted images and the uniformity of data distribution, with the aim of determining the effectiveness of each mode in protecting information.

Keywords: Block cipher, SPN, ECB, CBC, OFB, symmetric cryptography.

Introducción

En la actualidad, la interacción entre las personas y los sistemas de cómputo es cada vez mayor, abarcando ámbitos como el ocio, la educación, el trabajo y la salud. Este incremento del uso de tecnologías de la información hace indispensable garantizar la seguridad de la información, especialmente en términos de confidencialidad e integridad. Sin embargo, en muchos casos estos mecanismos de protección son ignorados por desconocimiento o descuido, lo que incrementa los riesgos asociados al manejo de datos.

Dentro de las estrategias para proteger la información destacan dos enfoques principales: la esteganografía, que busca ocultar la existencia del mensaje, y la criptografía, que transforma la información para hacerla ilegible a usuarios no autorizados. La criptografía, disciplina que estudia las técnicas de cifrado y descifrado de datos, se complementa con el criptoanálisis, encargado de analizar y romper sistemas criptográficos (William Stallings. (2017)) (Jonathan Katz, & Yehuda Lindell. (2020)). A lo largo de la historia, diferentes civilizaciones han utilizado métodos de cifrado, desde los jeroglíficos del antiguo Egipto hasta técnicas clásicas como la escítala griega y el cifrado de César en el Imperio romano.

En este contexto, el presente trabajo aborda los fundamentos del cifrado y descifrado de la información mediante el diseño e implementación de una red de sustitución-permutación (SPN) para cifrado simétrico. Asimismo, se analizan distintos modos de operación de cifrados por bloques aplicados al cifrado de imágenes en formato BMP, con el objetivo de realizar una comparación cuantitativa y cualitativa sobre la calidad y efectividad del proceso de cifrado.

Criptografía simétrica

Los algoritmos de cifrado simétrico emplean una única clave compartida entre emisor y receptor para cifrar y descifrar la información. En este tipo de criptografía, la seguridad del sistema se basa principalmente en la confidencialidad y fortaleza de la clave, más que en el secreto del algoritmo, por lo que conocer el algoritmo no debería permitir descifrar el mensaje sin la clave correspondiente.

Existen diversos algoritmos de cifrado simétrico utilizados en la protección de la información deben ofrecer resistencia al criptoanálisis (Swenson, C. (2008)). Entre los más representativos se encuentran DES, desarrollado en la década de 1970 pero actualmente considerado débil por el tamaño de su clave; 3DES, una mejora de DES mediante su aplicación triple; AES, adoptado como estándar moderno de cifrado y ampliamente utilizado por su alto nivel de seguridad; Twofish, propuesto como candidato para AES.

Modos de operación

A lo largo del tiempo, la criptografía ha evolucionado con el desarrollo de nuevos algoritmos de cifrado y la creación de modos de operación diseñados para resolver problemas específicos y garantizar determinadas propiedades de seguridad. En la actualidad, existen diversos modos de operación estandarizados que permiten adaptar los sistemas criptográficos simétricos a distintos requisitos y escenarios de aplicación.

Los modos de operación surgieron junto con la necesidad de cifrar bloques de datos utilizando algoritmos de cifrado simétrico. De acuerdo con Paar y Pelzl (2009), los modos como ECB, CBC, CFB y OFB definen diferentes técnicas para procesar y cifrar bloques de información. Aunque existen otros modos de operación, en este trabajo únicamente se consideran los mencionados.

Electronic Code Book (ECB)

El modo de operación ECB es uno de los enfoques más directos en criptografía de bloques (Paar, C., & Pelzl, J. (2010)). Este modo consiste en cifrar cada bloque de forma

independiente utilizando una misma clave simétrica, lo que lo hace conceptualmente simple y fácil de implementar.

En el proceso de cifrado cada bloque del mensaje se procesa de manera secuencial y el resultado se concatena en el mismo orden para formar el texto cifrado final. El descifrado sigue el proceso inverso aplicando la función de descifrado a cada bloque. Debido a que los bloques se procesan de manera independiente, cualquier modificación en un bloque de texto plano solo afecta al bloque cifrado correspondiente, sin influir en los demás, como se puede observar en la Figura 1.

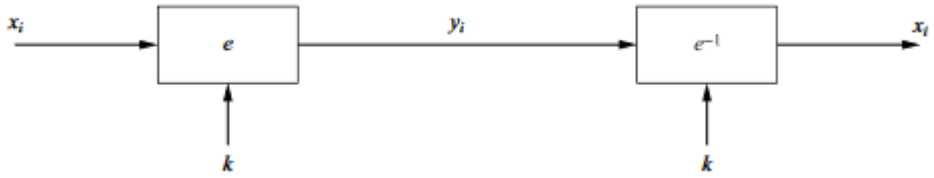

Figura 1. Modo de operación ECB.

Cipher Block Chaining (CBC)

El modo de operación CBC se basa en el principio fundamental que consiste en encadenar los bloques de cifrado mediante la operación XOR con el bloque cifrado anterior (Paar, C., & Pelzl, J. (2010)). A partir de este, los bloques siguientes se cifran combinando mediante XOR el bloque de texto plano con el bloque cifrado anterior, generando así una cadena de dependencia entre todos los bloques, como se puede observar en la Figura 2.

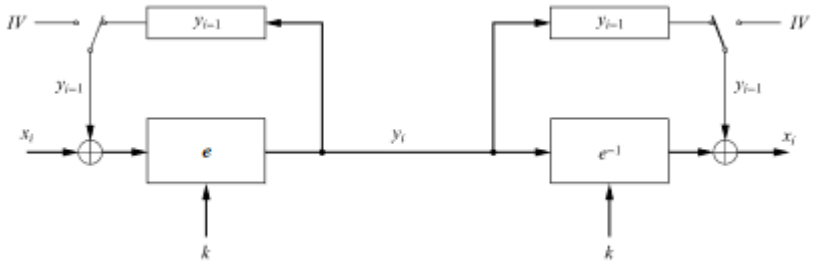

Figura 2. Modo de operación CBC.

Output Feedback (OFB)

El modo de operación OFB el algoritmo de cifrado se aplica inicialmente a un vector de inicialización (IV) para generar una secuencia pseudoaleatoria de bloques (Paar, C., & Pelzl, J. (2010)). Dicha secuencia se combina mediante una operación XOR con el texto plano para producir el texto cifrado. El proceso consiste en generar una secuencia pseudoaleatoria a partir del IV y la clave, reutilizar la retroalimentación en el cifrado del algoritmo y combinarlo con el texto plano mediante la operación XOR, como se puede observar en la Figura 3.

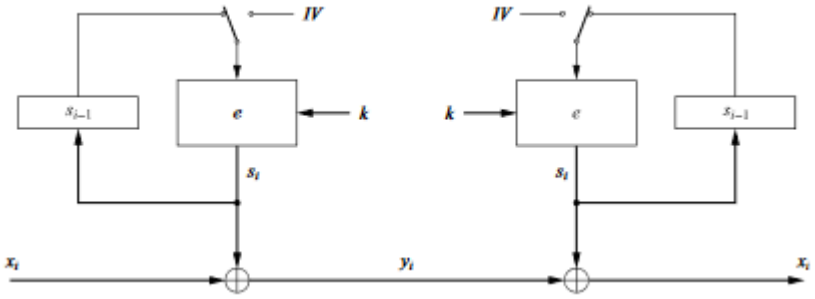

Figura 3. Modo de operación OFB.

Cipher Feedback (CFB)

El modo de operación CFB, inicialmente aplica el algoritmo de cifrado al vector de inicialización (IV), el resultado del algoritmo de cifrado lo combina con el bloque del texto plano mediante la operación XOR, el resultado se retroalimenta para ser cifrado (Paar, C.,

& Pelzl, J. (2010)). El resultado cifrado se combina de nuevo con el resto de los bloques del texto plano y la operación XOR, como se puede observar en la Figura 4.

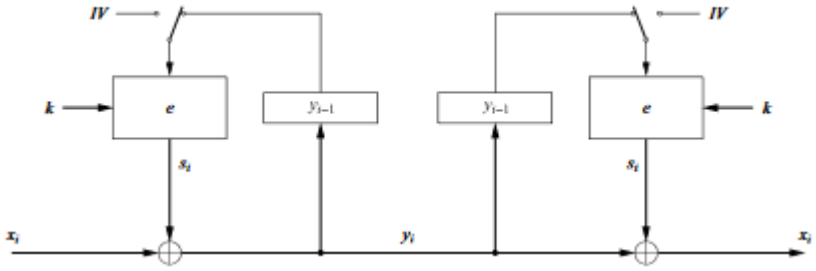

Figura 4. Modo de operación CFB.

Red de sustitución-permutación SPN-16

Para realizar las pruebas de cifrado simétrico de bloques y los modos de operación ECB, CBC, OFB y CFB se implementó la red de sustitución-permutación básica de 16 bits (SPN-16) propuesta por Stinson, D. R. (2005) para fines de estudio (Stinson, D. R. (2005)) (Youssef, A. M., Tavares, S. E., & Heys, H. M. (1996)) (Heys, H. M., & Tavares, S. E. (1996)). La Figura 5, muestra la estructura de la SPN-16 y como puede observarse consiste de cinco rondas, de las cuales las rondas 1, 2 y 3 tienen la misma configuración. Mientras que la ronda 4 difiere al no aplicarse la permutación y la ronda 5 consiste de la aplicación de la operación XOR con el resultado de la ronda 4 y la subclave 5.

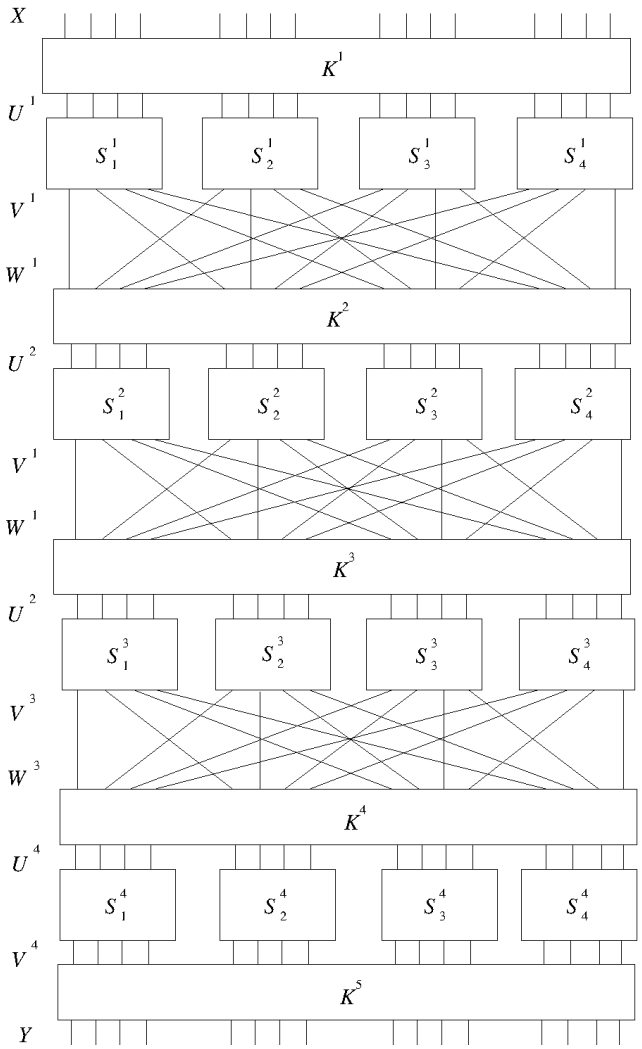

Figura 5. SPN-16.

La estructura requiere 5 subclaves utilizadas en las cinco rondas, se hace uso de una sola caja de sustitución (S-Box) utilizada en las rondas 1, 2, 3 y 4, de igual manera se tiene una sola caja de permutación (P-Box) utilizada en las rondas 1, 2, y 3. La Tabla 1, muestra el funcionamiento de la S-Box, Z corresponde a la entrada y la salida $\pi P(z)$. Si la entrada corresponde a 4_{16} la salida de la S-Box es 2_{16}. La finalidad de la S-Box es generar confusión. Las redes de sustitución-permutación se basan en el principio de la confusión y difusión (Claude Shannon. (1949)).

Z	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
$\pi S(z)$	E	4	D	1	2	F	B	8	3	A	6	C	5	9	0	7

Tabla 1. Caja de sustitución S-Box.

La Tabla 2, muestra el funcionamiento de la P-Box, Z corresponde a la entrada y la salida $\pi P(z)$. Dado que se realizan permutaciones, el bit de la posición 1 no es permutado manteniendo su posición, mientras que el bit 2 es permutado a la posición 5. La finalidad de la P-Box es generar la difusión.

Z	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$\pi P(z)$	1	5	9	13	2	6	10	14	3	7	11	15	4	8	12	16

Tabla 2. Caja de permutación P-Box.

Resultados

Para realizar las pruebas se utilizó una imagen con patrones dominantes que permiten apreciar los cambios de cifrado al aplicar los diferentes modos de operación y la red de sustitución-permutación SPN-16.

Imagen centauro

La Figura 6, muestra la imagen de un centauro en color blanco y fondo negro, estos colores corresponden a los patrones dominates de la imagen. La Figura 7, muestra el histograma de la imagen centauro, como puede observarse sólo tres valores tienen presencia. Claramente demuestra la presencia de patrones repetitivos.

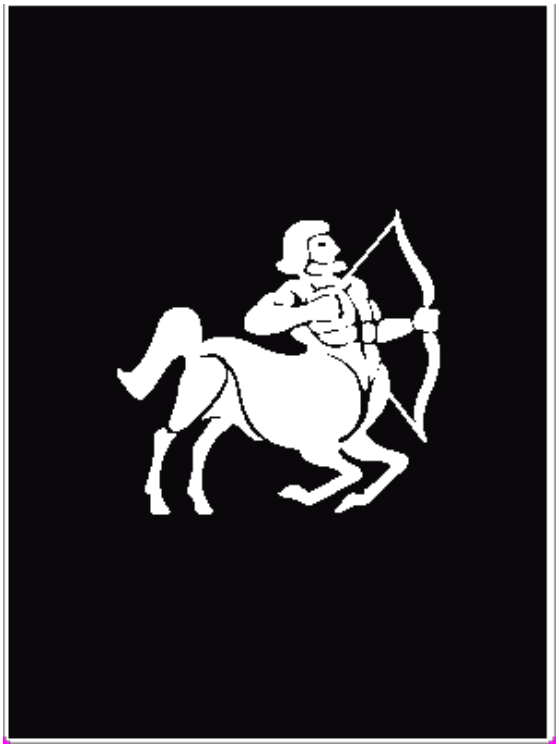

Figura 6. Imagen centauro.

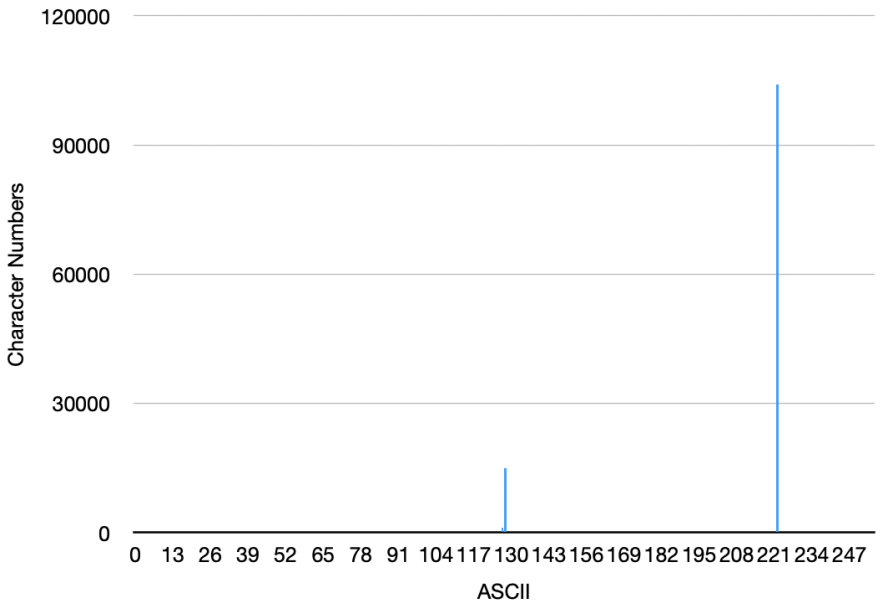

Figura 7. Histograma de la imagen centauro.

Imagen cifrada con SPN-16 y ECB

La Figura 8, muestra la imagen cifrada con la SPN-16 y el modo de operación ECB. Como se puede observar los patrones repetidos se transformaron en nuevos patrones producidos por la SPN-16.

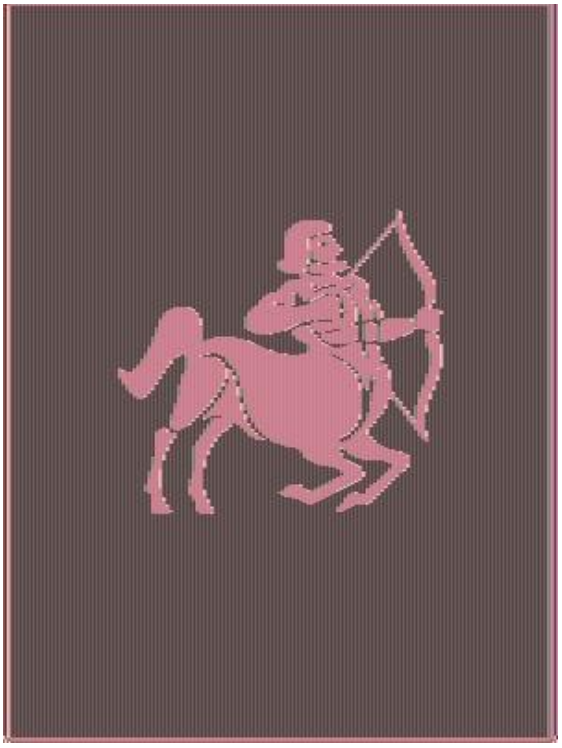

Figura 8. Imagen cifrada con SPN-16 y ECB.

La Figura 9, revela la presencia de patrones repetitivos, en el histograma de la imagen original se aprecian solo tres valores y en el histograma de la imagen cifrada se presentan más de tres valores de los cuales dos tienen mayor presencia.

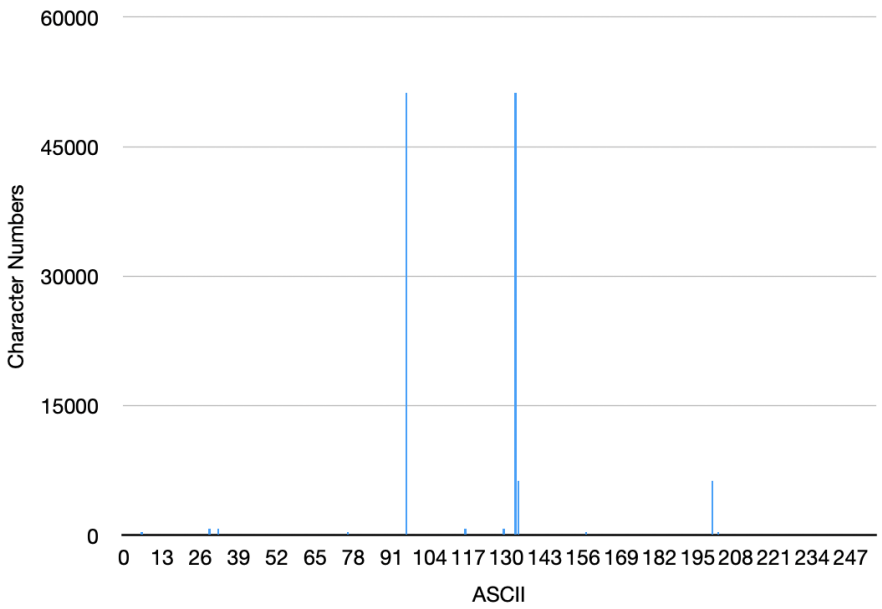

Figura 9. Histograma de la imagen cifrada SPN-16 y ECB.

Imagen cifrada con SPN-16 y CBC

La Figura 10, muestra la imagen cifrada con la SPN-16 y el modo de operación CBC. Como se puede observar los patrones repetidos se transformaron perdiéndose en el cifrado resultante. El cifrado obtenido no revela información de la imagen original, los patrones repetitivos se transformaron en datos que no revelan su presencia. La Figura 11, muestra el histograma de la imagen cifrada empleando el modo de operación CBC. Se obtiene una distribución homogénea con una variación mínima entre el máximo y el mínimo.

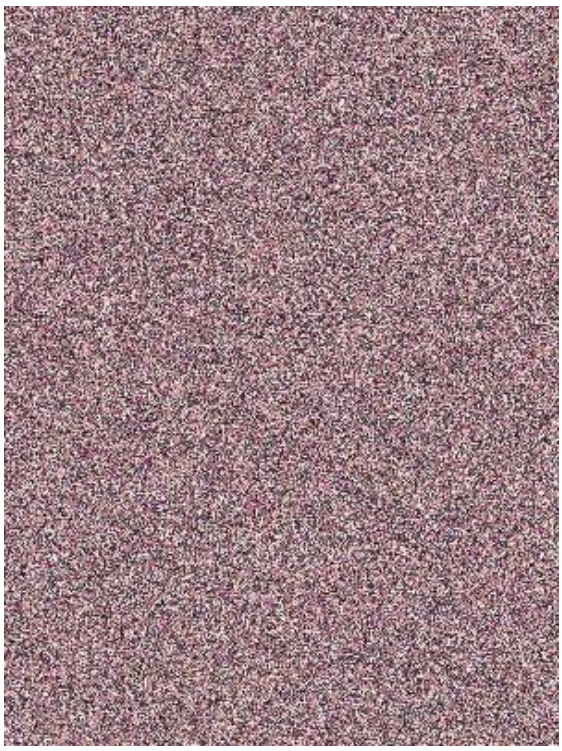

Figura 10. Imagen cifrada con SPN-16 y CBC.

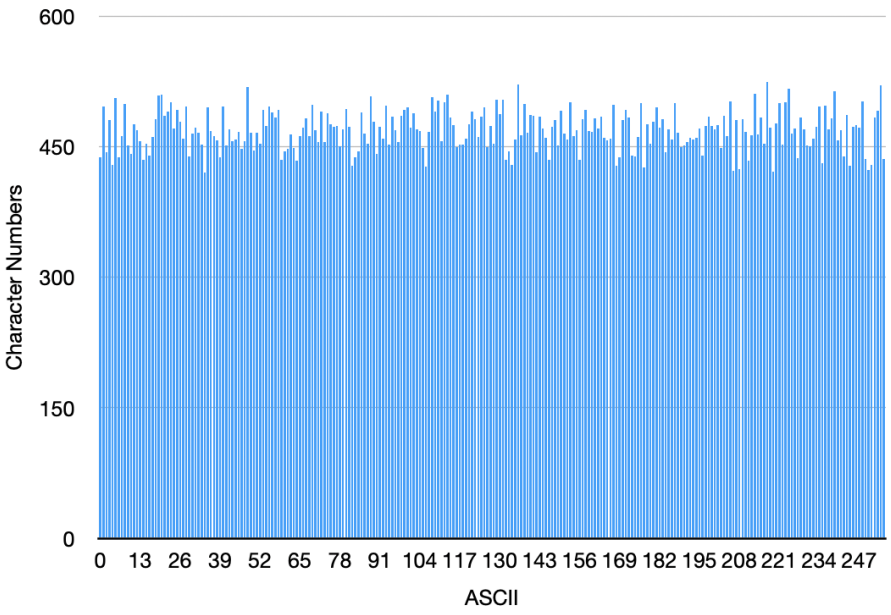

Figura 11. Histograma de la imagen cifrada SPN-16 y CBC.

Imagen cifrada con SPN-16 y CFB

La Figura 12, muestra la imagen cifrada con la SPN-16 y el modo de operación CFB. Como se puede observar los patrones repetidos se transformaron perdiéndose en el cifrado resultante. El cifrado obtenido no revela información de la imagen original, los patrones repetitivos se transformaron en datos que no revelan su presencia. La Figura 13, muestra el histograma de la imagen cifrada empleando el modo de operación CFB. Se obtiene una distribución homogénea con una variación mínima entre el máximo y el mínimo.

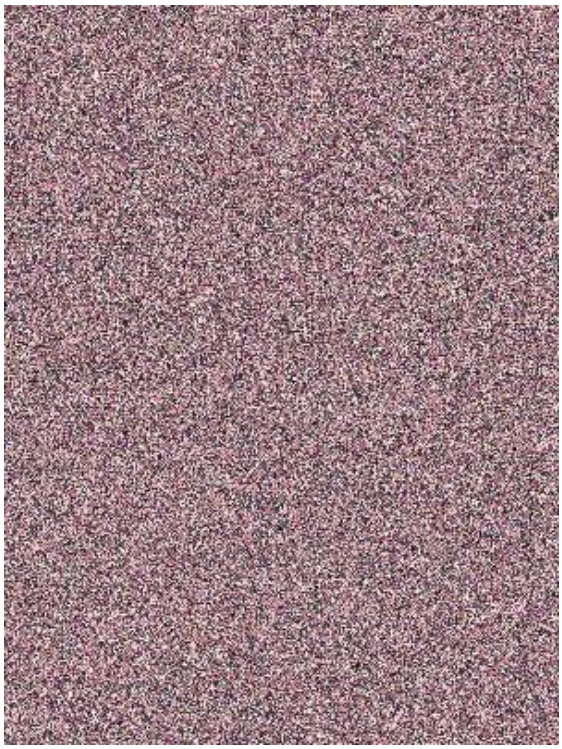

Figura 12. Imagen cifrada con SPN-16 y CFB.

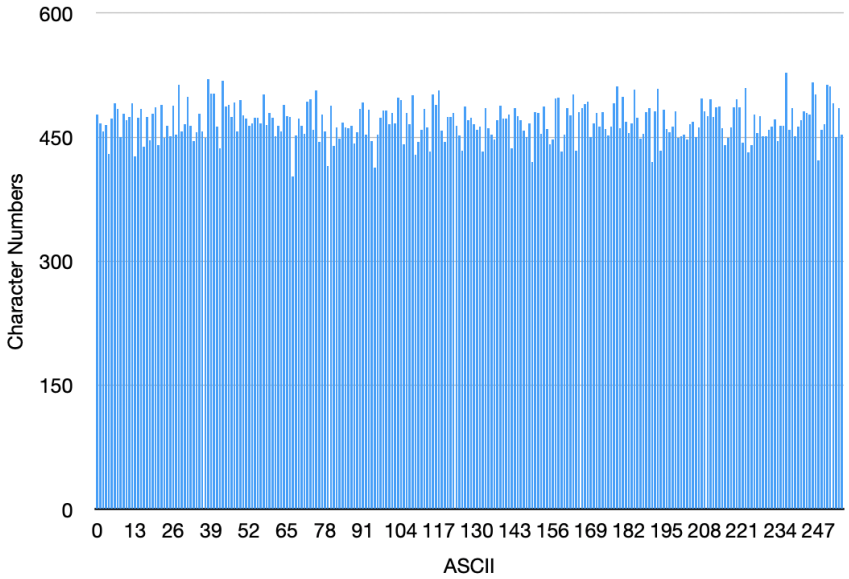

Figura 13. Histograma de la imagen cifrada SPN-16 y CFB.

Imagen cifrada con SPN-16 y OFB

La Figura 14, muestra la imagen cifrada con la SPN-16 y el modo de operación OFB. Como se puede observar los patrones repetidos se transformaron perdiéndose en el cifrado resultante. El cifrado obtenido no revela información de la imagen original, los patrones repetitivos se transformaron en datos que no revelan su presencia. La Figura 15, muestra el histograma de la imagen cifrada empleando el modo de operación OFB. Se obtiene una distribución homogénea con una variación mínima entre el máximo y el mínimo.

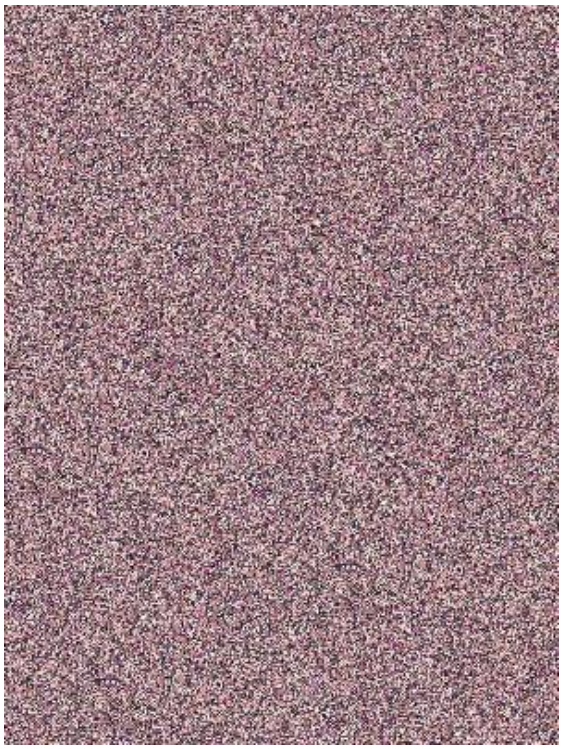

Figura 14. Imagen cifrada con SPN-16 y OFB.

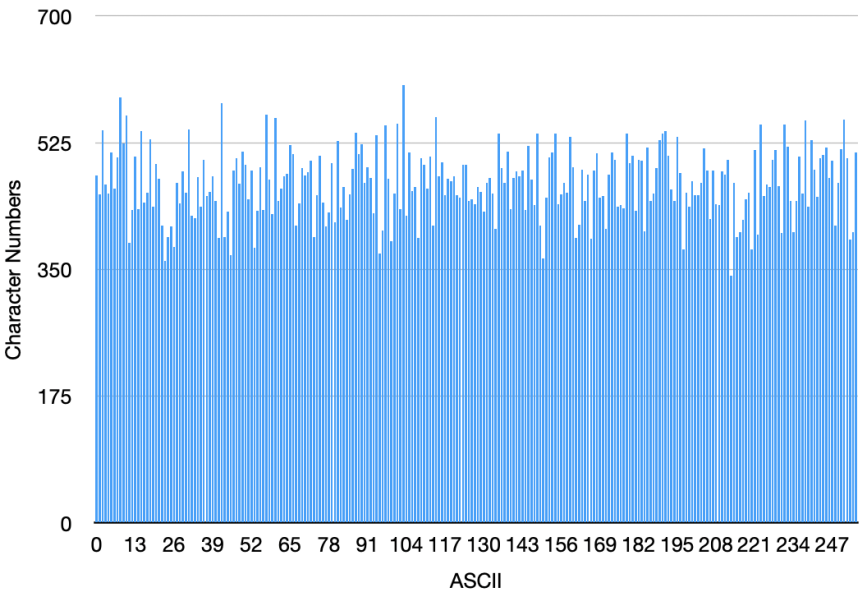

Figura 15. Histograma de la imagen cifrada SPN-16 y OFB.

Conclusiones

Se concluye que los modos de operación ECB, CBC, CFB y OFB, implementados mediante una SPN-16, presentan comportamientos de cifrado distintos. El modo ECB destaca por su simplicidad y rapidez debido a la independencia entre bloques; sin embargo, esta característica constituye también su principal debilidad, ya que los patrones repetitivos del texto plano pueden mantenerse en el texto cifrado, facilitando la posible inferencia de información. Por su parte, el modo CBC, CFB y OFB introducen dependencia entre bloques al encadenar cada bloque cifrado con el anterior, lo que transforma patrones repetidos en distribuciones más homogéneas y mejora la seguridad del cifrado. En general, los resultados indican que el uso del modo ECB debe evitarse debido a su incapacidad para ocultar adecuadamente patrones repetitivos, mientras que CBC, CFB y OFB ofrecen mejores propiedades de seguridad al generar distribuciones más homogéneas y con menores diferenciales.

Referencias Bibliográficas

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

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

Heys, H. M., & Tavares, S. E. (1996). Substitution-permutation networks resistant to differential and linear cryptanalysis. Journal of cryptology, 9(1), 1-19.

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

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

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

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

Youssef, A. M., Tavares, S. E., & Heys, H. M. (1996). A new class of substitution-permutation networks. In Workshop on Selected Areas in Cryptography, SAC (Vol. 96, pp. 132-147).