REVISTA MULTIDISCIPLINARIA
DESARROLLO AGROPECUARIO, TECNOLOGICO, EMPRESARIAL Y HUMANISTA
UNIVERSIDAD TECNICA DE COTOPAXI - LA MANA. COTOPAXI. ECUADOR
ISSN: 2773-7527

Volumen 7. No. 2

Diciembre 2025

Metodologías de cifrado de datos para la seguridad de la información: Una revisión sistemática

Data encryption methodologies for information Security: A systematic review

Sebastian Alberto Espinoza Davalos[1], Alejandro Benjamín Quiroz Rodriguez[1], Alberto Carlos Mendoza de los Santos[1]

[1]Universidad Nacional de Trujillo, Trujillo - Perú

Correo de correspondencia: sespinozad@unitru.edu.pe, aquirozr@unitru.edu.pe, amendozad@unitru.edu.pe

Información del artículo

Tipo de artículo:
Artículo original

Recibido:
01/09/2025

Aceptado:
04/11/2025

Publicado:
15/12/2025

Revista:
DATEH

Resumen

En el contexto digital actual, el de datos se ha posicionado como una de las técnicas más efectivas para lograr garantizar la seguridad y privacidad de la información. En este trabajo se presenta una revisión sistemática en la que utilizamos la metodología PRISMA, realizando el análisis de distintas revistas publicadas entre los años 2021 y 2025, y después de una selección rigurosa nos quedamos con 15 publicaciones que fueron incluidas en este artículo para su revisión. Los resultados muestran que los algoritmos tradicionales, como AES, RSA y ECC, mantienen una alta efectividad en entornos estándar; sin embargo, nuevas propuestas como la criptografía de curva elíptica mejorada (EECC), el cifrado probabilístico y los esquemas híbridos ofrecen mejoras significativas en seguridad y adaptabilidad. Entre los aportes destacados, se identificaron variantes de AES que incrementan el efecto avalancha, esquemas híbridos en la nube que reducen los tiempos de recuperación de datos frente a métodos convencionales, y técnicas aplicadas al cifrado de imágenes que mejoran la robustez frente a ataques diferenciales. No obstante, estas soluciones emergentes presentan limitaciones relacionadas con el mayor consumo de recursos computacionales y el aumento de los tiempos de procesamiento, lo que restringe su aplicación en entornos con capacidades limitadas o de alta demanda en tiempo real. Este trabajo aporta una visión integral sobre los beneficios y las limitaciones del cifrado en la seguridad de la información digital.

Palabras clave: *cifrado, seguridad, información, innovación*

Abstract

In today's digital environment, data encryption has emerged as one of the most effective techniques for ensuring information security and privacy. This paper presents a systematic review using the PRISMA methodology, analyzing various journals published between 2021 and 2025. After a rigorous selection process, we selected 15 publications, which were included in this article for review. The results show that traditional algorithms such as AES, RSA, and ECC remain highly effective in standard environments; however, new proposals such as enhanced elliptic curve cryptography (EECC), probabilistic encryption, and hybrid schemes offer significant improvements in security and adaptability. Notable contributions included AES variants that enhance the avalanche effect, hybrid cloud schemes that reduce data recovery times compared to conventional methods, and techniques applied to image encryption that improve robustness against differential attacks. However, these emerging solutions present limitations related to increased computational resource consumption and increased processing times, which restricts their application in environments with limited capacities or high real-time demands. This work provides a comprehensive view of the benefits and limitations of encryption in digital information security.

Keywords: *encryption, security, information, innovation*

INTRODUCCIÓN

En la era digital actual, donde los datos fluyen constantemente entre sistemas y dispositivos, la protección de la información se ha convertido en algo prioritario para organizaciones y empresas. El progresivo aumento en el número de ciberataques y la creciente complejidad de las amenazas han intensificado la necesidad de garantizar la seguridad y la confidencialidad de la información. Bajo este contexto, las metodologías de cifrado de datos se han consolidado como una de las herramientas más eficaces para preservar privacidad e integridad de información sensible, tanto en tránsito como en reposo. El cifrado actúa como un mecanismo de defensa que transforma la información legible en texto cifrado incomprensible sin la clave de descifrado correspondiente,

ISSN: 2773-7527
Volumen 7. No. 2
Diciembre 2025

protegiendo credenciales, información financiera y secretos comerciales (Zafir et al., 2024).

El cifrado de datos ha demostrado ser un pilar fundamental de la seguridad de la información, siendo implementado en una amplia variedad de sistemas, desde aplicaciones móviles hasta plataformas de almacenamiento en la nube. Sin embargo, su ejecución presenta desafíos que deben considerarse cuidadosamente. Por un lado, el cifrado ofrece enormes beneficios en términos de protección de datos, pero por otro, introduce ciertos costos operativos, especialmente en términos de rendimiento del sistema. Estos costos pueden ser más evidentes en entornos con recursos limitados o donde se requiere un alto rendimiento en tiempo real. Como señala Meselhy et al., (2025), varios métodos de cifrado tienen dificultades para equilibrar la seguridad, la robustez y el procesamiento en tiempo real, lo que hace que la velocidad computacional sea particularmente crucial para las aplicaciones prácticas.

Además, seleccionar el algoritmo de cifrado adecuado no es tarea sencilla. Si bien algoritmos tradicionales como AES, RSA y ECC siguen siendo ampliamente utilizados, han surgido nuevos enfoques y variaciones que prometen una mayor eficiencia y una mayor resiliencia ante ataques. Sin embargo, estos avances no siempre son viables en todos los contextos. Por ejemplo, variantes como la criptografía de curva elíptica mejorada (EECC) han demostrado ser muy eficaces, pero su implementación puede ser computacionalmente costosa, lo que las hace menos atractivas para entornos que requieren tiempos de respuesta rápidos (Zhang & Zhao, 2024). Asimismo, el cifrado probabilístico se ha transformado en una elección interesante para mejorar la seguridad en los sistemas de comunicación, si bien introduce complejidades adicionales que pueden afectar la eficiencia y velocidad del proceso de cifrado y descifrado (Korchynskyi et al., 2023).

El propósito de esta investigación es explorar en detalle los beneficios que las metodologías de cifrado aportan a la seguridad de la información, así mismo establecer los principales desafíos que enfrentan las organizaciones al implementar estas soluciones. Con ello, se busca profundizar en la comprensión de cómo se pueden optimizar los diferentes métodos de cifrado para equilibrar la protección de datos con los requisitos operativos de rendimiento y eficiencia. Por lo tanto, la pregunta central que buscamos responder en esta investigación es: ¿Cuáles son los principales beneficios de las metodologías de cifrado de datos en la seguridad de la información y qué desafíos surgen al implementarlas en distintos entornos?

MATERIALES Y MÉTODOS

Para el desarrollo de esta investigación se comenzó evaluando diferentes enfoques metodológicos. El primero de ellos fue el SLR de Kitchenham, el cual tiene fortaleza en cuanto al campo de ingeniería de software se refiere, ya que trabaja con un marco adecuado para ello. Por otra parte, se evaluó también el Scoping Review de Arsksey y O'Malley, el cual funciona de manera flexible a través de cinco etapas. Esto permite explorar literatura con criterios de inclusión amplios.

Sin embargo, se optó finalmente por la metodología PRISMA. Se consideró más apropiada debido a que está diseñada especialmente para responder preguntas ya definidas con comparaciones concretas, pues define un marco ordenado que facilita la evaluación de los beneficios y desafíos del ámbito de investigación, viéndose en este caso, que se buscaba determinar estos aspectos de las distintas metodologías de cifrado de datos. Además, la familiaridad del equipo de investigación con esta metodología, permitió una aplicación más precisa en conjunto con un proceso más detallado.

Ya teniendo a PRISMA como la metodología a seguir, además de incluir los criterios de inclusión y los de exclusión, se realizó un filtrado de documentos repetidos y documentos que no coincidían con nuestro enfoque específico de investigación

Criterios de inclusión

- Se tuvo en consideración los artículos publicados en español e inglés.
- Se consideraron publicaciones en el rango de fechas del 2021 al 2025.
- Solo se consideraron documentos que son del tipo conference paper y los que son artículos.

Criterios de exclusión

- No se tuvieron en consideración las publicaciones que no sean de acceso público.
- Se filtraron los artículos duplicados.

Catálogos y bases de datos

Se realizó una búsqueda en distintos motores de base de datos, y ello derivó en un total de 256 publicaciones divididas en las siguientes fuentes: Scopus(68), ScienceDirect (103), IEEE Explore (85).

ISSN: 2773-7527
Volumen 7. No. 2
Diciembre 2025

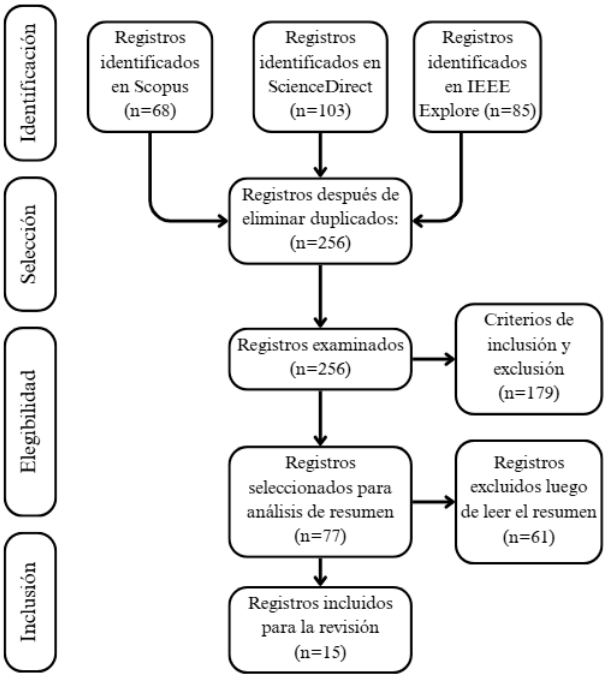

Figura 1. *Diagrama de flujo PRISMA*

Para poder obtener los resultados previos, fueron utilizadas las siguientes fórmulas que nos permitieron realizar el filtrado de publicaciones en cada una de las fuentes:

Scopus:

TITLE-ABS-KEY ("data" AND "Encryption" AND "methodology" AND "Information Security") AND PUBYEAR > 2020 AND PUBYEAR < 2026 AND (LIMIT-TO(LANGUAGE, "Spanish") OR LIMIT-TO(LANGUAGE "English")) AND (LIMIT-TO(DOCTYPE, "ar") OR LIMIT-TO(DOCTYPE, "cp"))

IEEE Xplore:

("All Metadata": data) AND ("All Metadata": Encryption) AND ("All Metadata": methodology) AND ("All Metadata": Information Security)
Filters Applied: 2021 - 2025
Show: Open Access Only

ScienceDirect:

"Data" AND "Encryption methodologies" AND "Information" AND "Security"
Years: 2025,2024,2023,2022,2021
Article type: Review articles, Research articles
Access type: Open access & Open archive

RESULTADOS Y DISCUSIÓN

En la Tabla 1 se puede observar un resumen detallado de los resultados provenientes del análisis de los artículos seleccionados mediante la metodología PRISMA.

Tabla 1
Resumen de publicaciones seleccionadas.

Autorías, título y año	Resultados	Tecnologías/Técnica
Kalaiselvi, R., Vennila, S, (2021). Security enhancement using custom-aes and its performance evaluation on avalanche effect-a new approach	En el artículo se propone realizar una modificación en el algoritmo AES para poder mejorar la seguridad en la transmisión de datos. Esta mejora se midió con el efecto avalancha y los resultados demuestran un mayor efecto avalancha en el algoritmo AES modificado, además es compatible con sistemas AES por lo que es práctico de implementar en estos. Sin embargo, algunas posibles dificultades que se puede observar es el incremento en el tiempo de cifrado/descifrado y que consume más recursos. Por lo que en entornos de sistemas con bajos recursos, no sería lo ideal.	Se utiliza la metodologia de cifrado simétrico (custom_AES)
Korchynskyi, V., Hordiichuk, V., Kildishev, V., Staikutsa, S., Riabukha, O., and Alfaiomi, K. (2023). Information protection method based on the integration of probabilistic encryption and noise-immune coding.	En este artículo se propone un método para proteger la información que consta de tres etapas, donde se implementa el cifrado probabilístico, la decodificación iterativa y la correlación de errores, este método mejora la inmunidad al ruido y la seguridad de la información. No obstante, al añadir más etapas de procesamiento, el rendimiento se puede ver afectado, además, al procesar en tantas etapas la información la velocidad de transmisión puede verse afectada.	Se utiliza el método de cifrado probabilístico
Khalid et al. (2023). Robust Color Image Encryption Scheme Based on RSA via DCT by Using an Advanced Logic Design Approach	En este artículo se propone un sistema para cifrar imágenes donde se combina RSA y la transformación discreta del coseno, con la ayuda de puertas lógicas reversibles, para poder crear claves secretas que varíen según las características de las imágenes, lo cual mejorará en gran medida la gestión de la seguridad y el rendimiento en cuanto al proceso de cifrado y descifrado de imágenes se refiere. Algunas dificultades que se pudieron identificar fueron que la complejidad del cifrado depende de la calidad de la imágen, por lo tanto en casos específicos donde la resolución sea muy baja puede ser vulnerable a ataques. Por otra parte, sería muy complicado de implementar en entornos donde se manejen gran cantidad de imágenes ya que se tendrían que guardar y gestionar todas las claves que se generen para cada una de ellas.	Se utiliza el método de cifrado RSA, DCT y RLG

Mustafa et al. (2022). Financial Information Security Using Hybrid Encryption Techniques in Multi-Cloud Architectures. Bulletin of Electrical and Computer Engineering	En este artículo se propone un sistema para gestionar la seguridad de datos en la nube, el sistema DDSPE divide los datos según su sensibilidad y utiliza diferentes métodos de cifrados como ECC, ARS, Y AES para asegurar la confidencialidad de los datos. Los resultados demostraron que DSSPE requiere menos tiempo para recuperar datos que otras técnicas y es más seguro. Sin embargo, una preocupación a tener en cuenta debería ser el procedimiento de clasificar la información en sus 3 distintos niveles, ya que si se clasifica mal o bien puede consumir más recursos de lo necesario, o podría volverse vulnerable información altamente sensible.	Se utilizaron métodos de cifrado híbrido (ECC, ARS y AES)
Zhengqi Zhang, Yan Zhao (2024). Enhanced Elliptic Curve Cryptography (EECC)	El artículo plantea una mejora en la criptografía de curvas elípticas (ECC), llamada EECC. Este algoritmo va a mejorar la seguridad significativamente, tratando de mantener una longitud de clave corta en relación al estándar ECC. Un dato a tener en cuenta, y se menciona en la propia investigación sería que no se ha sido aún probada en el mundo real, con las condiciones y desafíos que esta afronta, por lo que su funcionamiento en este ámbito aún es desconocido.	Se utiliza criptografía de curvas elípticas mejoradas (EECC)
Meselhy et al. (2025). Multiple image encryption techniques: Strategies, challenges, and future directions.	Este artículo se encarga de realizar un análisis de las distintas técnicas que se utilizan para el cifrado de múltiples imágenes como el basado en sistemas de caos, basado en dominios de transformación y técnicas híbridas. Comentan que aún hay desafíos críticos por resolverse, en especial en el ámbito de manejo de recursos y que se requiere una exploración continua para que esta área siga evolucionando.	Se utiliza Técnicas Hibridas
K. Priyadarsini, Arun Kumar Sivaraman, Abdul Quadir Md, Areej Malibari (2023) , Securing 3D Point and Mesh Fog Data Using Novel Chaotic Cat Map	En este artículo se propone un nuevo esquema para cifrar datos de puntos y mallas 3D, ya que los métodos tradicionales como RSA AES y DES no son suficientes para manejar la complejidad de los puntos adyacentes en datos 3D. Este algoritmo propuesto presenta un esquema de doble encriptación, por lo que los datos se encuentran protegidos ante ataques. Pero esto mismo implica dificultades de implementación en entornos donde se necesite un alto rendimiento.	Se propone un nuevo algoritmo de cifrado llamado “Chaotic cat”.
M. W. Hafiz, W. -K. Lee, SO Hwang, M. Khan y A. Latif, (2022), Discrete Logarithmic Factorial Problem and Einstein Crystal Model Based Public-Key Cryptosystem for Digital Content Confidentiality	En este artículo se propone un nuevo cifrado de clave pública usando criterios de anillo cercano y microestados para manejar de forma más segura la confidencialidad del contenido digital, ya que mencionan que las técnicas actuales como el RSA tienen debilidades en cuanto ataques CPA y CCA se refiere. Sin embargo, añadir la doble encriptación y las simulaciones de Monte Carlo significa una carga considerable al procesamiento de la información, lo que podría dar problemas en dispositivos de bajos recursos.	El artículo tiene como base el cifrado de clave pública (PKI)
F. ElAzzaby, K.H. Sabour, N. ELakkad, W. El-Shafai, A. Torki, S.R. Rajkumar (2023), Color image encryption using a Zigzag Transformation and sine–cosine maps	En este artículo se muestra un algoritmo de cifrado de imágenes que consta de dos partes. Codificación, donde se emplean transformaciones horizontales y verticales. Y Difusión donde se reemplazan individualmente los píxeles individuales de la imagen, así generando una capa extra de seguridad.	Se amalgama el Estándar de cifrado avanzado (AES) y el Estándar de cifrado de datos (DES)
Kazi Naimur Rahman, Monowar Wadud Hridoy, Md Mizanur Rahman, Md Rifatul Islam, Semonti Banik, (2024), Highly secured and effective management of app-based online voting system using RSA	En este artículo se muestra una problemática importante, la falta de interés o incapacidad de participar en los procesos electorales. Por lo que se propone un sistema de votación en línea usando el cifrado RSA para gestionar lo referente a la seguridad y asegurar que se mantenga la privacidad de los votos.	Se utiliza el método de cifrado RSA.
Muhammad Nadeem, Ali Arshad, Saman Riaz, Syeda Wajiha Zahra, Ashit Kumar Dutta, Moteeb Al Moteri, Sultan Almotairi, An Efficient Technique to Prevent Data Misuse with Matrix Cipher Encryption Algorithms,	En este artículo se propone el algoritmo de Matrix Hill mencionando las ventajas que tiene sobre otros algoritmos al tener una doble capa de protección por lo que es un gran aporte en cuanto a seguridad se refiere. Un gran aporte de este estudio es el uso de una tabla ASCII personalizada ya que es una muy buena idea para el reforzamiento de la seguridad. Sin embargo, se generan claves únicas para textos planos y manejar una gran cantidad de claves conlleva implementaciones complejas en entornos donde se manejen varios usuarios, por lo que se tendría que considerar en qué entorno aplicarla.	Se propone utilizar el algoritmo Matrix-Hill
Ehsanul Islam Zafir, Afifa Akter, M.N. Islam, Shahid A. Hasib, Touhid Islam, Subrata K. Sarker, S.M. Muyeen, Enhancing security of Internet of Robotic Things: A review of recent trends, practices, and	Este artículo se encarga de analizar qué tan efectivos son los mecanismos de cifrado en el IoRT y señala posibles mejoras que se podrían implementar, como la optimización de los algoritmos de cifrado y ampliar el alcance del cifrado de extremo a extremo.	Se analiza el cifrado simétrico y asimétrico. Además se menciona el cifrado de datos en reposo.

recommendations with encryption and blockchain techniques,		
Yousheng Zhou, Rundong Peng, Yuanni Liu, Pandi Vijayakumar, Brij Gupta, TRE-DSP: A traceable and revocable CP-ABE based data sharing scheme for IoV with partially hidden policy	En este artículo se muestra una mejora a la política de texto cifrado utilizada en el Iov, (CP-ABE) que sería el TRE-DSP. Este no solo se encargaría de mejorar la cobertura de cifrado de datos, sino que también invalidaría claves de descifrado de usuarios malintencionados. El único punto a señalar sería que al trasladar todas las tareas computacionales a la nube, implicaría dependencias de infraestructura interna y externa, lo que a su vez ocasiona un aumento de latencia.	Se utiliza la técnica de cifrado basada en atributos con política de texto cifrado (CP-ABE)
O. F. A. Wahab, A. A. M. Khalaf, A. I. Hussein and H. F. A. Hamed, Hiding Data Using Efficient Combination of RSA Cryptography, and Compression Steganography Techniques	En este artículo se propone usar un algoritmo híbrido de compresión de datos. Esto con la finalidad de poder aumentar la seguridad mandando más datos de entrada hacia el método de encriptación RSA pero optimizando el espacio que ocupa la imagen. Es decir, se logra mayor seguridad y menor tamaño, así beneficiando de igual manera a la transmisión eficiente.	Se usa el método de encriptación RSA (Rivest-Shamir-adleman)
Fauziyah, Zhaoshun Wang, Mujahid Tabassum. A Holistic Secure Communication Mechanism Using a Multilayered Cryptographic Protocol to Enhanced Security,	En este artículo se nos plantea el problema de la inseguridad de los tradicionales mecanismos de encriptación frente a una constante evolución de la tecnología. Por lo que proponen integrar los aspectos del algoritmo ECDH, el AES-GCM y el ECDSA. Se llegó a la conclusión de que si se analiza detenidamente las relaciones entre estos, podrían suplantar a los algoritmos de encriptación actuales.	Se usa el estándar de cifrado avanzado en modo Galois/Contador (AES-GCM)

Luego de haber revisado todos estos artículos, podemos ver la gran importancia que conlleva el cifrado de datos, ya que como menciona (Cumpa Vila & Huachaca Urbina, 2024) “En términos de seguridad, si se implementan tecnologías de cifrado y autenticación se puede llegar a reforzar en gran medida la información sensible de los clientes”.

Y es que no se puede negar ello, en estos tiempos donde mucha información se maneja de manera digital es una necesidad mantener segura información sensible. Esta fuga de información puede causar serios problemas si se maneja con malas intenciones como afirma (Benussi Diaz, 2020). Esta información puede ser usada para actividades indeseables para los titulares, como por suplantación de identidad.

En relación con las distintas técnicas que existen para el cifrado de datos podemos afirmar que es necesario separar cada cual para el ámbito donde pueda ser más eficiente, ya que en algunos casos unas mínimas modificaciones o alteraciones que se basan en otro algoritmo, pueden hacer la diferencia, tanto como para gestionar de mejor manera la seguridad, como también, para lograr una mejora en el rendimiento del procesamiento.

Un ejemplo de ello podría ser el EECC, si bien otorga una mayor capa de protección, estos cálculos adicionales que realiza van de la mano con el tiempo que se demora en hacerlos, tiempo que en algunos casos puede ser depreciado, pero, en otros no. Siendo uno de estos casos, entornos donde los tiempos de respuesta esperados sean extremadamente cortos.

En vista de ello, encontramos que se puede justificar la creciente variedad de métodos de cifrado, ya que actualmente se está viendo mucho la digitalización de la información y como tal, hay muchos ámbitos en los que se requiere un guardado de información en la red y no se puede asegurar la similitud entre tantos. Por lo que, de cierta manera, es un avance importante comenzar a desarrollar y aplicar estas distintas metodologías a casos específicos para mejorar el rendimiento de las operaciones sin afectar la seguridad de información sensible.

Por lo tanto, el cifrado de datos no solo se puede tomar como un pilar fundamental de la seguridad digital. Por el contrario, se debe considerar como un factor clave para asegurar la protección de datos en esta creciente digitalización de los procesos y servicios.

CONCLUSIONES

Según el análisis de los artículos realizados, se demuestra que el cifrado de datos es una metodología muy importante para garantizar que la información que pueda ser de carácter sensible en el ámbito digital se mantenga segura. Los resultados nos muestran que el cifrado ayuda en gran medida a la protección de los datos, tal como se pudo ver en las evaluaciones de rendimiento de algoritmos como AES, RSA y ECC en sus respectivos contextos.

Sin embargo, no solo se debe tener en cuenta implementarlos, sino que se debe hacer una evaluación para determinar cuál de estos es el adecuado para su respectivo entorno, ya que, si bien pueden tener múltiples beneficios de seguridad, de la mano de estos va el procesamiento adicional que se le cargarán a los sistemas.

Una muestra de ello son los resultados que se pudieron observar en distintos artículos, ya que nos muestran que combinando algoritmos de cifrado, como AES y RSA se

ISSN: 2773-7527
Volumen 7. No. 2
Diciembre 2025

puede llegar a mantener una relación estable y eficaz entre seguridad y rendimiento.

Por último, a través de esta revisión se pudo corroborar que debido a la digitalización de la información que se está generando debido a los avances tecnológicos, se ha generado una mayor demanda de métodos de cifrado, ya que se deben adaptar a diferentes situaciones en distintos ámbitos.

CONTRIBUCIÓN DE LOS AUTORES

Sebastian Alberto Espinoza Davalos: Conceptualización, metodología, investigación y escritura.

Alejandro Benjamín Quiroz Rodriguez: Investigación, metodología, análisis y escritura.

Alberto Carlos Mendoza de los Santos: Validación, análisis, revisión y supervisión.

REFERENCIAS BIBLIOGRÁFICAS

ElAzzaby et al. 2023, Color image encryption using a Zigzag Transformation and sine–cosine maps, Scientific African, vol 22. https://doi.org/10.1016/j.sciaf.2023.e01955

Hafiz et al., 2022, Discrete Logarithmic Factorial Problem and Einstein Crystal Model Based Public-Key Cryptosystem for Digital Content Confidentiality, IEEE Access, vol. 10. https://ieeexplore.ieee.org/document/9895258

Kalaiselvi R,Vennila S, 2021, Security enhancement using custom-aes and its performance evaluation on avalanche effect-a new approach, Indian Journal of Computer Science and Engineering, 12(3), 591-597 https://doi.org/10.21817/indjcse/2021/v12i3/211203092

Khalid et al.,2023, Robust Color Image Encryption Scheme Based on RSA via DCT by Using an Advanced Logic Design Approach, Baghdad Science Journal, vol 20, 2593-2607. https://doi.org/10.21123/bsj.2023.8715

Korchynskyi et al., 2023, Method of information protection based on the integration of probabilistic encryption and noise immune coding, Radioelectronic and Computer Systems, 4(108), 184-196 https://doi.org/10.32620/REKS.2023.4.13

Meselhy et al., 2025, Multiple image encryption techniques: Strategies, challenges, and potential future directions, Alexandria Engineering Journal, vol 125. https://doi.org/10.1016/j.aej.2025.04.006

Mustafa et al., 2022, Financial information security using hybrid encryption technique on multi-cloud architecture, Bulletin of Electrical Engineering and Informatics, 11(6), 3450-3461. https://doi.org/10.11591/eei.v11i6.3967

Nadeem et al. 2022, An Efficient Technique to Prevent Data Misuse with Matrix Cipher Encryption Algorithms, Computers, Materials and Continua, 74(2). https://doi.org/10.32604/cmc.2023.032882

Naimur et al. 2024, Highly secured and effective management of app-based online voting system using RSA encryption and decryption, Heliyon, 10(3). https://doi.org/10.1016/j.heliyon.2024.e25373

Priyadarsini et al.,2023. Securing 3D Point and Mesh Fog Data Using Novel Chaotic Cat Map, Computers, Materials and Continua, 74(3) https://doi.org/10.32604/cmc.2023.030648

Wahab et al.,2021 , Hiding Data Using Efficient Combination of RSA Cryptography, and Compression Steganography Techniques, IEEE Access, vol. 9, pp. 31805-31815. https://ieeexplore.ieee.org/document/9356603/authors#authors

Fauziyah et al., (2024, enero 17), A Holistic Secure Communication Mechanism Using a Multilayered Cryptographic Protocol to Enhanced Security. Computers, Materials & Continua, 78(3), 4417-4452. https://doi.org/10.32604/cmc.2024.046797

Yousheng et al. 2024, TRE-DSP: A traceable and revocable CP-ABE based data sharing scheme for IoV with partially hidden policy, Digital Communications and Networks. https://doi.org/10.1016/j.dcan.2024.03.005

Zafir et al. 2024, Enhancing security of Internet of Robotic Things: A review of recent trends, practices, and recommendations with encryption and blockchain techniques, Internet of Things, vol. 28. https://doi.org/10.1016/j.iot.2024.101357

Zhengqi Zhang, Yan Zhao, Enhanced Elliptic Curve, 2024, Cryptography (EECC), Procedia Computer Science, vol 247. https://doi.org/10.1016/j.procs.2024.10.158