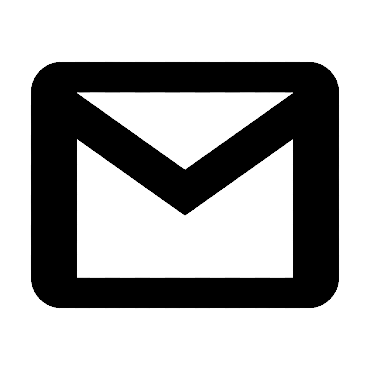
**Relevancia de la esteganografía en la seguridad de la red**

**Relevance of steganography in network security**

Maricielo Estefany Caciano Arroyo[](mailto:t513300120@unitru.edu.pe)[](file:///F:\Informes%202025%20MANP\Revista%20UNTELS%20VOL4%20-%20N3\0000-0001-7532-7604), Antony Fernando Vasquez Cabrera [[Logotipo

Descripción generada automáticamente con confianza media](https://orcid.org/0009-0001-3151-2936)](https://orcid.org/0009-0001-3151-2936), Alberto Carlos Mendoza de los Santos [[Logotipo

Descripción generada automáticamente con confianza media](https://orcid.org/0000-0002-0469-915X)](https://orcid.org/0000-0002-0469-915X)

Universidad Nacional de Trujillo, Trujillo, Perú

**RESUMEN**

La esteganografía, antigua práctica de ocultar información en medios habituales, ha ganado relevancia en la seguridad de las redes. Este estudio revisa trabajos de investigadores globales, destacando su aplicación en la creación de canales ocultos en protocolos como TCP/IP, la seguridad en Redes de Sensores Inalámbricos (WSN), y la combinación con criptografía para fortalecer la confidencialidad.

La metodología PRISMA guio la revisión sistemática, abordando la pregunta de investigación sobre la relevancia de la esteganografía en la seguridad de la red. La diversidad geográfica de estudios entre el 2020 a 2023, desde India hasta Polonia y China, resalta la importancia global de la esteganografía.

Los resultados evidencian la versatilidad de la esteganografía, desde propuestas innovadoras en detección de esteganografía hasta su aplicación en VoIP y cifrado homomórfico multiclave. La combinación de enfoques y la constante innovación subrayan la importancia continua de la esteganografía en la seguridad de la información en la era digital.

**Palabras clave:** Esteganografía, Seguridad de la red, Ocultamiento de información, Cifrado de datos

**ABSTRACT**

Steganography, the ancient practice of hiding information in common media, has gained relevance in network security. This study reviews work by global researchers, highlighting its application in the creation of hidden channels in protocols such as TCP/IP, security in Wireless Sensor Networks (WSN), and the combination with cryptography to strengthen confidentiality.

The PRISMA methodology guided the systematic review, addressing the research question of the relevance of steganography in network security. The geographic diversity of studies between 2020 to 2023, from India to Poland to China, highlights the global importance of steganography.

The results demonstrate the versatility of steganography, from innovative approaches in steganography detection to its application in VoIP and homomorphic multi-key encryption. The combination of approaches and constant innovation underline the continuing relevance of steganography in information security in the digital age.

**Keyboards:** Steganography, Network Security, Information Hiding, Data Encryption

1. **INTRODUCCIÓN**

La esteganografía, una disciplina antigua destinada a ocultar información dentro de medios aparentemente comunes, ha encontrado en el entorno de las redes un terreno fértil para desempeñar un papel crítico en la seguridad de la información. Cuando hablamos de redes, nos referimos a un conjunto de dispositivos electrónicos que son fundamentales en la actualidad para facilitar la comunicación, compartir recursos y acceder a servicios en línea.

Por lo tanto, la seguridad de la red se refiere a la implementación de medidas y estrategias para proteger la integridad, confidencialidad y disponibilidad de los datos y recursos dentro de una red informática. Este campo abarca la prevención y detección de accesos no autorizados, la gestión de amenazas y vulnerabilidades, así como la implementación de protocolos y políticas que resguarden la información que circula a través de los dispositivos interconectados en una red.

Para entender mejor el concepto de esteganografía, según Pérez (2020), nos menciona que la esteganografía se define como el acto de esconder información dentro de otro objeto o elemento de manera que pase inadvertida. Por otro lado, de acuerdo con Bejarano (2017), la seguridad de la red es asegurar la preservación de la integridad, confidencialidad, control, autenticación y disponibilidad de la información.

La razón que impulsa este estudio es destacar la importancia de la esteganografía en la seguridad de las redes. A partir de lo mencionado anteriormente, surge la siguiente pregunta de investigación: ¿Cuál es la relevancia de la aplicación de la esteganografía en el ámbito de la seguridad de la red?

Para responder a este interrogante, se llevó a cabo una investigación minuciosa en reconocidas bases de datos que albergan publicaciones vinculadas al tema en cuestión, siendo pertinentes para alcanzar el objetivo establecido. Se aplicó el método PRISMA para la selección y evaluación de los resultados obtenidos de los estudios elegidos. Finalmente, se presentan de manera concisa las conclusiones que enfatizan la relevancia de la esteganografía en la seguridad de las redes.

**MATERIALES Y MÉTODOS**

**Tipo de Estudio**

En la realización de este análisis exhaustivo, se adoptó la metodología PRISMA. La pregunta de investigación formulada para obtener una respuesta objetiva es: ¿Cuál es la relevancia de la aplicación de la esteganografía en el ámbito de la seguridad de la red?

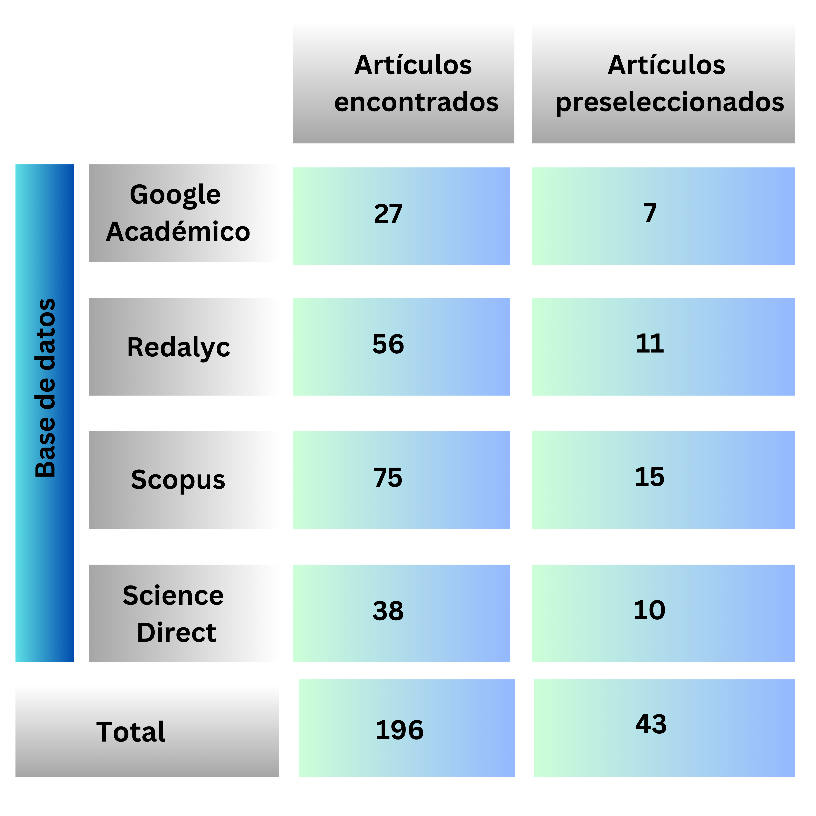
**Fundamentación de la Metodología**

Antes de profundizar en la explicación de la metodología PRISMA, es necesario definir qué es una revisión sistemática. Según Page et al. (2021), es un método de investigación que proporciona una síntesis estructurada y organizada del conocimiento disponible sobre un tema específico. Este enfoque busca recopilar, evaluar y resumir de manera exhaustiva la evidencia existente, permitiendo identificar patrones, tendencias, y lagunas en la investigación.

Teniendo en cuenta la definición de la metodología PRISMA, resulta evidente la importancia de su aplicación en una revisión sistemática. Para llevar a cabo este método, se seguirán los pasos sugeridos por Arnau y Sala (2020): Desarrollar la estrategia de búsqueda constituye el primer paso, seguido de la identificación y selección cuidadosa de la literatura pertinente. Los resultados obtenidos se registran y almacenan de manera sistemática. Luego, se procede a modelar y organizar las referencias seleccionadas, estableciendo una estructura coherente. Finalmente, se lleva a cabo un análisis detallado y la interpretación de los resultados obtenidos de los artículos seleccionados, permitiendo así extraer conclusiones significativas.

**Estrategia de Búsqueda**

Con el fin de obtener la información necesaria sobre el tema de investigación, se emplearon términos clave específicos durante la búsqueda en las bases de datos seleccionadas. Estos términos incluyeron: "esteganografía", "seguridad de red", "ocultamiento de información", *"steganography", "network security", "hide information".* Para recopilar información y lograr resultados más precisos y actualizados en la investigación (ver Figura 1), se emplearon diversas fuentes: SCOPUS, GOOGLE ACADÉMICO, REDALYC, SCIENCE DIRECT. La incorporación de estas fuentes garantiza la calidad y relevancia de los datos recolectados y examinados en el estudio.



**Figura 1.** Bases de datos y artículos encontrados

Diagrama

Descripción generada automáticamente

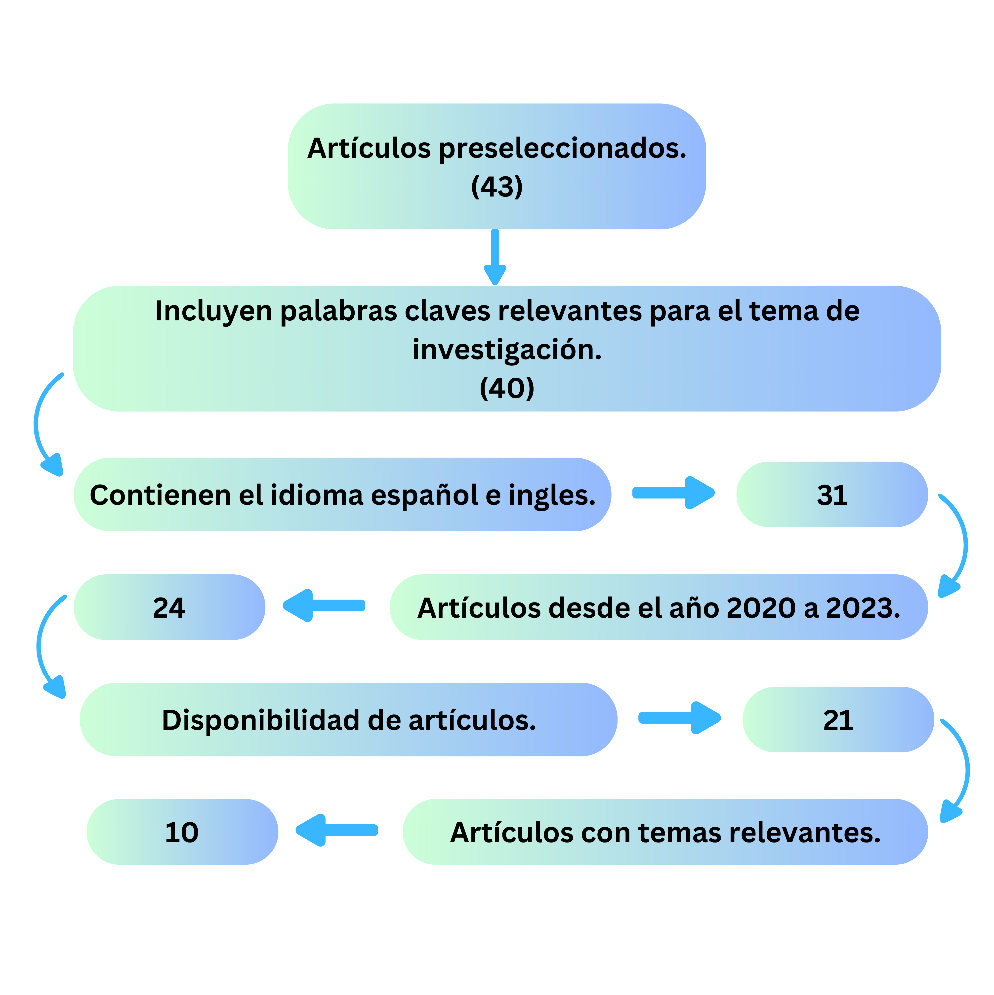
**Figura 2.** Análisis de bibliografía

**Criterios de inclusión y de exclusión**

En la elección de documentos para este estudio, se consideraron artículos de investigación redactados tanto en inglés como en español, utilizando diversas bases de datos para ampliar la búsqueda y obtener una muestra representativa. Se delimitaron los años de investigación en el intervalo desde 2020 hasta 2023 con el propósito de incorporar documentos actualizados y pertinentes para la investigación en cuestión.

Asimismo, se identificaron distintos tipos de documentos académicos para su inclusión en el análisis, abarcando artículos y revisiones. Es crucial señalar que, como criterio de inclusión, se estableció la condición de que estos documentos estén disponibles en línea para asegurar su accesibilidad.

En cuanto al criterio de exclusión, se excluyeron publicaciones que abordan temáticas no relevantes para la investigación. Este enfoque garantiza que la selección de documentos sea pertinente y se alinee con los objetivos de la investigación, contribuyendo así a la mejora de la calidad y confiabilidad de los resultados obtenidos (ver Figura 3).



**Figura 3.** Criterios de inclusión y exclusión.

**RESULTADOS Y DISCUSIÓN**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Nro** | **Autor** | **Título** | **Año** | **País** | **Importancia** |
| 1 | Punam Bedia, Arti Dua | Network Steganography using the Overflow Field of Timestamp Option in an IPv4 Packet | 2020 | India | La esteganografía en redes es esencial para ocultar mensajes secretos mediante protocolos comunes como TCP/IP, utilizando campos como el encabezado o la carga útil. Esto posibilita la creación de canales ocultos, siendo muy significativo en entornos de redes debido a sus amplias posibilidades para establecer comunicación encubierta. |
| 2 | Ambika, Virupakshappa, Sachinkumar Veerashetty | Secure communication over wireless sensor network using image steganography with generative adversarial networks | 2022 | India | La esteganografía es fundamental para la seguridad en Redes de Sensores Inalámbricos (WSN) y se considera una de las técnicas de cifrado más seguras. Facilita la comunicación secreta al esconder mensajes dentro de datos aparentemente normales, como imágenes, siendo esencial para reforzar la seguridad en entornos de redes no confiables en WSN. |
| 3 | Milosz Smolarczyk, Krzysztof Szczypiorski, Jakub Pawluk | Multilayer Detection of Network Steganography | 2020 | Polonia | Este estudio destaca la importancia de la esteganografía en redes al presentar un nuevo método de detección que utiliza algoritmos de aprendizaje automático para analizar métricas en protocolos de red, buscando capacidad de estegoanálisis en entornos con muchos dispositivos y conexiones. |
| 4 | Rohit Kumar, Kamaldeep Joshi | Enhancing Network Security for Image Steganography by Splitting Graphical Matrix | 2020 | India | Se propone un mecanismo divisor gráfico para transferir contenido seguro en imágenes voluminosas, con el objetivo de prevenir el pirateo o la lectura no autorizada. En conjunto, subraya la relevancia de la esteganografía en la seguridad de la información en entornos de redes. |
| 5 | Madhur, Ajay, Vijay, Pranjali y Sunita | Cryptography & Network Security | 2022 | India | Utilizando una combinación de la esteganografía con la criptografía, se puede lograr un nivel aún mayor de seguridad y confidencialidad para los datos sensibles aumentado la seguridad de red al hacer que sea más difícil detectar y extraer la información confidencial que se transmite a través de la red. |
| 6 | Beijing Chen, Jiaxin Wang, Yingyue Chen, Zilong Jin, Hiuk Jae Shim y Yun-Qing Shi. | High-Capacity Robust Image Steganography via Adversarial Network | 2020 | China | Se introduce una red de estegoanálisis para mejorar la seguridad contra la detección de la información oculta, y una red de ataque para mejorar la robustez contra algunos tipos de alteraciones, como el ruido, el filtrado y el recorte. |
| 7 | Xintao Duan, Zhiqiang Shao, Wenxin Wang, En Zhang, Dongli Yue, Chuan Qin y Haewoon Nam. | A Steganography Model Data Protection Method Based on Scrambling Encryption | 2022 | China | Proponen una idea basada en la codificación de parámetros del modelo de red. Su importancia destaca en que cuando se utilizan parámetros codificados para la extracción de imágenes secretas, se extrae una imagen sin sentido independiente de la imagen secreta, lo que demuestra que este método puede proteger bien la seguridad del modelo de red de esteganografía. |
| 8 | Wu, Z.; Guo, J.; Zhang, C.; Li, C | Steganography and Steganalysis in Voice over IP: A Review | 2021 | China | La esteganografía es relevante para la seguridad de la red porque puede proporcionar una capa adicional de protección para la transmisión de datos sensibles como la esteganografía basada en VoIP (Voz sobre IP), esto se refiere al uso de la voz como portador de información secreta. |
| 9 | Ibrahi Abunad, Hana Abdullah, Saud S., MashaelM., Manar Ahmed Haza, Abu Sarwa Zaani, Abdelwahed y Ishfaq Yaseen | Optimal Multikey Homomorphic Encryption with Steganography Approach for Multimedia Security in Internet of Everything Environment | 2022 | Arabia Saudita | Establecen que la importancia de la esteganografía en la red se basa en el cifrado homomórfico multiclave y la esteganografía de imágenes para proteger la transmisión de datos multimedia en el entorno de Internet de todo (IoE). |
| 10 | Gyimah, S. | Security During Transmission Of Data Using Web Steganography | 2022 | Ghana | La relevancia que destacan es que la esteganografía se puede combinar con métodos criptográficos. La combinación de esteganografía y criptografía para la transmisión de datos ocultos es el mejor método sugerido para proteger los datos transferidos a través de Internet. |

**Esteganografía**

La esteganografía desciende de las palabras griegas "steganos" y "graphein", que significa "escritura" y "dibujo", respectivamente. Steganos implica "cubierto", "secreto" u "oculto". Los datos escondidos en un material de cobertura para que sean invisibles para los demás son el objetivo básico de la esteganografía (Abdulazeez, et al., 2023). La esteganografía es el concepto de un algoritmo de cobertura que intenta cifrar el mensaje secreto dentro de algunos objetos/medios de cobertura transmitidos por internet que ningún atacante puede detectar (Rahman et al., 2023).

Según Buin et al. (2023) menciona que el ocultamiento de datos, como la esteganografía, tiene aplicaciones importantes en la protección de los derechos de autor, la comunicación preservada de la privacidad y la procedencia del contenido. Para Rahman et al., 2023 menciona además que la importancia de la esteganografía es que a simple vista los atacantes no puedan sospechar el mensaje oculto en ningún medio de cobertura.

**Seguridad en la red con esteganografía**

Seguridad de redes, criptografía y esteganografía es el concepto de datos del producto mientras se transmite a través del Internet y red inalámbrica. Se ocupa del desarrollo y analizando protocolos que previenen a terceros maliciosos de recuperar información compartida entre dos entidades. La comunicación segura se refiere al escenario donde el mensaje o los datos compartidos entre dos partes no pueden ser accedidos por una entidad maliciosa. La esteganografía es un intento de lograr una seguridad y comunicación indetectable.

**Relevancia de la esteganografía en la seguridad de las redes informáticas**

La esteganografía en redes ha evolucionado como un componente esencial para salvaguardar la confidencialidad de la información en entornos de comunicación. Este arte milenario de ocultar mensajes dentro de datos aparentemente normales encuentra una nueva dimensión en el mundo digital, donde destacados expertos de diversas partes del mundo han explorado y propuesto innovadoras técnicas. Desde India hasta Polonia, China hasta Ghana, estos estudios reflejan la creciente importancia de la esteganografía en la seguridad de redes, abordando desafíos específicos y resaltando su aplicación en diversos contextos.

En el corazón de este fascinante campo se encuentra el estudio de Punam Bedia y Arti Dua, quienes, en 2020 desde la India, destacaron la esencia de la esteganografía en la creación de canales ocultos en protocolos como TCP/IP, permitiendo una comunicación encubierta en entornos de redes. Este enfoque ha sido continuado por investigadores indios como Ambika, Virupakshappa y Sachinkumar Veerashetty, quienes en 2022 exploraron la esteganografía como una técnica fundamental para reforzar la seguridad en Redes de Sensores Inalámbricos (WSN).

El panorama internacional también se destaca con trabajos como el de Milosz Smolarczyk y su equipo en Polonia, quienes presentaron en 2020 un novedoso método de detección de esteganografía en redes, subrayando la necesidad de abordar la ocultación de información para garantizar la seguridad de las comunicaciones en entornos complejos. Desde India, Rohit Kumar y Kamaldeep Joshi propusieron en el mismo año un mecanismo divisor gráfico para transferir contenido seguro en imágenes, resaltando la relevancia de la esteganografía en la seguridad de la información en entornos de redes.

Algunos estudios específicos, como el análisis de esteganografía basada en VoIP en China, subrayan la aplicabilidad de esta técnica en contextos particulares, como la seguridad en la transmisión de datos de voz sobre IP. Además, la fusión de esteganografía con cifrado homomórfico multiclave en Arabia Saudita destaca la versatilidad de esta disciplina en el emergente entorno de Internet de Todo (IoE).

Por otro lado, el panorama asiático se amplía con la contribución china de Beijing Chen y su equipo en 2020, quienes introdujeron una red de estegoanálisis y una red de ataque para mejorar la seguridad contra la detección de información oculta en imágenes. Xintao Duan y colaboradores, también de China, propusieron en 2022 una innovadora idea basada en la codificación de parámetros del modelo de red, protegiendo la seguridad del modelo de red de esteganografía.

En conjunto, estas investigaciones reflejan la riqueza y diversidad de la esteganografía en redes, destacando su papel crucial en la seguridad de la información a nivel global, desde la creación de canales ocultos hasta la combinación con la criptografía para garantizar la confidencialidad en la transmisión de datos sensibles.

**CONCLUSIONES**

Después de un análisis a la literatura sobre la relevancia de la esteganografía en la seguridad de la red, se puede concluir que esta disciplina se posiciona como un componente crucial en la preservación de la confidencialidad y la integridad de la información en entornos de comunicación.

En este escenario, donde la ciberdelincuencia busca aprovechar las vulnerabilidades de los sistemas para acceder a información confidencial, la esteganografía se revela como una herramienta estratégica para establecer canales ocultos y proteger la comunicación encubierta. La diversidad de enfoques y técnicas presentadas en los estudios revisados resalta la adaptabilidad de la esteganografía a diversos contextos, desde Redes de Sensores Inalámbricos (WSN) hasta aplicaciones específicas como la transmisión segura de datos de voz sobre IP.

La revisión sistemática ha permitido identificar que la esteganografía no solo se limita a ocultar información, sino que también se integra eficazmente con la criptografía y otras técnicas de seguridad para ofrecer un nivel superior de protección de la red.

Al proyectar hacia el futuro, se vislumbra un continuo desarrollo en las técnicas y modelos de esteganografía, enfocándose en la creación de métodos más precisos y confiables para la ocultación de información. En este sentido, se insta a los entornos de redes a implementar activamente la esteganografía como una herramienta esencial para optimizar la seguridad de la red y mitigar riesgos potenciales.

**REFERENCIAS BIBLIOGRÁFICAS**

Abdulazeez, Sabah & Nawar, Abbas & Lubna, Emad & Jahefer, Mothefer. (2023). Hiding Information in Digital Images Using LSB Steganography Technique. International Journal of Interactive Mobile Technologies (iJIM). 17. 167-178. <https://doi.org/10.3991/ijim.v17i07.38737>

Abunadi, I., Mengash, HA, Alotaibi, SS, Asiri, MM, Hamza, MA, Zamani, AS, … Yaseen, I. (2022). Cifrado homomórfico multiclave óptimo con enfoque de esteganografía para seguridad multimedia en entornos de Internet de todo. *Ciencias Aplicadas (Suiza)*, *12* (8). <https://doi.org/10.3390/app12084026>

Ambika, Virupakshappa, & Veerashetty, S. (2022). Secure communication over wireless sensor network using image steganography with generative adversarial networks. *Meas*u*rement: Sensors*, *24*. <https://doi.org/10.1016/j.measen.2022.100452>

Bedi, P., & Dua, A. (2020). Network Steganography using the Overflow Field of Timestamp Option in an IPv4 Packet. \*Procedia Computer Science, 171\*, 1810-1818. <https://doi.org/10.1016/j.procs.2020.04.194>

Bejarano Forero, E. (2017). AREANDINA Fundación Universitaria del Area Andina Repositorio Institucional. Recuperado de <https://digitk.areandina.edu.co/handle/areandina/1419>

Borato, MA, Panhale, AN, Panhale, VN, Gade, P. y Jadhav, Dr. S. (2022). Criptografía y seguridad de redes. *Revista internacional de investigación en ciencias aplicadas y tecnología de ingeniería*, *10* (12), 819–826. <https://doi.org/10.22214/ijraset.2022.48057>

Bui, T., Agarwal, S., Yu, N., & Collomosse, J. (2023). RoSteALS: Robust Steganography using Autoencoder Latent Space. [Preprint]. arXiv. <https://doi.org/10.48550/arXiv.2304.03400>

Chen, B., Wang, J., Chen, Y., Jin, Z., Shim, HJ y Shi, YQ (2020). Esteganografía de imagen robusta de alta capacidad a través de una red adversaria. *Transacciones KSII en Internet y sistemas de información*, *14* (1), 366–381. <https://doi.org/10.3837/tiis.2020.01.020>

Chinniyan, K., Samiyappan, TV, Gopu, A. y Ramasamy, N. (2022). Esteganografía de imágenes utilizando redes neuronales profundas. *Automatización inteligente y informática suave*, *34* (3), 1877–1891. <https://doi.org/10.32604/iasc.2022.027274>

Dar, Sun, Raja, N., Sreenivas, Nune, Mishra, Manish, Pattanaik, Balachandra, & P, Karthika. (2021). RSA Algorithm Using Performance Analysis of Steganography Techniques in Network Security. <https://doi.org/10.1007/978-981-33-4909-4_56>

Ding, Y., Wang, Z., Qin, Z., Zhou, E., Zhu, G., Qin, Z., & Choo, K.-K.R. (2024). Backdoor Attack on Deep Learning-Based Medical Image Encryption and Decryption Network. IEEE Transactions on Information Forensics and Security, 19, 280-292. <https://doi.org/10.1109/TIFS.2023.3322315>

Duan, X., Shao, Z., Wang, W., Zhang, E., Yue, D., Qin, C., & Nam, H. (2022). A Steganography Model Data Protection Method Based on Scrambling Encryption. *Computers, Materials and Continua*, *72*(3), 5363–5375. <https://doi.org/10.32604/cmc.2022.027807>

Fu, Z., Wang, F. y Cheng, X. (2020). La esteganografía segura para ocultar imágenes a través de GAN. *Revista Eurasip sobre Procesamiento de Imágenes y Vídeo*, *2020* (1). <https://doi.org/10.1186/s13640-020-00534-2>

Gyimah, S. A. (2022). Security During Transmission Of Data Using Web Steganography. *Advances in Multidisciplinary and Scientific Research Journal Publication*, *34*, 37–42. <https://doi.org/10.22624/aims/accrabespoke2022/v34p3>

Kumar, R., & Joshī, K. (2020). Enhancing Network Security for Image Steganography by Splitting Graphical Matrix. \*International Journal of Information Security Science\*, 9(1), 13–23. <https://dergipark.org.tr/en/pub/ijiss/issue/67165/1048731#article_cite>

Mrs. N. Dhivya, Mrs S. Banupriya, 2020, Network Security with Cryptography and Steganography, INTERNATIONAL JOURNAL OF ENGINEERING RESEARCH & TECHNOLOGY (IJERT) ICATCT – 2020 (Volume 8 – Issue 03). [https://](about:blank)doi.org/[10.17577/IJERTCONV8IS03010](about:blank)

Page, M. J., et al. (2021). Declaración PRISMA 2020: una guía actualizada para la publicación de revisiones sistemáticas. Revista Española de Cardiología, 74(9), 790-799. <https://doi.org/10.1016/j.recesp.2021.06.016>

Pérez Beristain, M. A. (2020). "Esteganografía de la información en nuestra vida." *Logos Boletín Científico De La Escuela Preparatoria No. 2, 7*(14), 7-8. Recuperado de: <https://repository.uaeh.edu.mx/revistas/index.php/prepa2/article/view/6088>

Rahman, S.; Uddin, J.; Hussain, H.; Jan, S.; Khan, I.; Shabir, M.; Musa, S. Multi Perspectives Steganography Algorithm for Color Images on Multiple-Formats. Sustainability 2023, 15, 4252. <https://doi.org/10.3390/su15054252>

Smolarczyk, M., Szczypiorski, K. y Pawluk, J. (2020). Detección multicapa de esteganografía de red. *Electrónica (Suiza)*, *9* (12), 1–14. <https://doi.org/10.3390/electronics9122128>

Wu, Z., Guo, J., Zhang, C. y Li, C. (2 de febrero de 2021). Esteganografía y esteganálisis en voz sobre ip: una revisión. *Sensores (Suiza)*. MDPI AG. <https://doi.org/10.3390/s21041032>

Zhang, XG, Yang, GH y Ren, XX (2022). Marco de seguridad basado en esteganografía de red para sistemas ciberfísicos. Ciencias de la Información, 609, 963–983. <https://doi.org/10.1016/j.ins.2022.07.081>