

Securing Data Using Improved Cryptography and Steganography Techniques

¹Abiina, Francis Adedayo, ²Ipeaeda, Funmilola Wumi

¹Department of Computer Science Federal College of Education (Special), Oyo

²Department of Cybersecurity, Ajayi Crowther University, Oyo.

DOI: <https://doi.org/10.51244/IJRSI.2026.1313CS026>

Received: 24 August 2026; Accepted: 29 August 2026; Published: 14 September 2026

ABSTRACT

The rapid growth of digital communication and information exchange has increased the vulnerability of data to unauthorized access, interception, modification, and other cyber threats, making effective data security increasingly important. Conventional cryptographic techniques protect the content of data but may expose the existence of the communication, while steganography conceals the existence of information but may not provide sufficient protection if the hidden data is discovered or extracted. This study proposes an improved hybrid data security model that combines enhanced cryptographic and steganographic techniques to provide multiple layers of protection. In the proposed approach, data is first encrypted using an improved cryptographic technique to ensure confidentiality and prevent unauthorized access. The encrypted data is then concealed within a digital image using an enhanced Least Significant Bit (LSB) steganographic technique, thereby reducing the likelihood of detection during transmission or storage. The performance of the proposed model is evaluated using security strength, embedding capacity, Peak Signal-to-Noise Ratio (PSNR), Mean Squared Error (MSE), and resistance to common attacks and steganalysis. The proposed approach is expected to improve data confidentiality and concealment while maintaining high visual quality of the stego-image and adequate data embedding capacity. The study demonstrates that integrating improved cryptography with steganography can provide stronger data protection than using either technique independently. The proposed model has potential applications in secure communication, financial transactions, healthcare information systems, military communication, cloud environments, and confidential data storage and transmission.

INTRODUCTION

The rapid growth of internet technologies, cloud computing, and digital communication has significantly increased the volume of sensitive information exchanged across networks. As organizations and individuals continuously transmit confidential data online, protecting such information from unauthorized access, cyberattacks, and data breaches has become a major challenge. Rajabi (2024). Traditional security methods are often insufficient against sophisticated cyber threats, creating a need for stronger and multi-layered security mechanisms. One promising approach involves integrating cryptographic techniques with image steganography to provide enhanced protection for sensitive information. Haverkamp, & Sarmah, (2024).

Cryptography is the process of transforming readable data (plaintext) into an unreadable format (ciphertext) using encryption algorithms and secret keys. Its primary goal is to ensure confidentiality, integrity, and authentication of information. However, although encrypted data is difficult to interpret, it often attracts attackers because the presence of encrypted content is obvious. Steganography, on the other hand, focuses on concealing the existence of information by embedding secret data within a carrier medium such as images, audio, or video. Image steganography is particularly popular due to the large amount of redundant data in digital images, which enables secret messages to be hidden with minimal visible distortion. Kombrink, Geradts, & Worring (2024).

Any eavesdropper can easily detect the presence of encrypted data and can try several attacks in order to get the original data. So in order to further enhance the security there is need to provide a two layer approach for providing an improved and better security. Steganography is concerned with security of transmitting data and allows communicating secretly by hiding the data within data (text/image). So for further enhancement of the data security, this system uses RSA algorithm along with steganography technique Rezaei, & Javadpour, (2024).

Statement of the Problem

The rapid growth of digital communication, information systems, and online data exchange has increased the vulnerability of data to unauthorized access, interception, modification, disclosure, and other cyber threats. The increasing dependence on digital platforms for transmitting and storing text, images, audio, and other forms of information has created a need for improved techniques that can ensure data confidentiality, integrity, and secure communication. Although cryptography and steganography are widely used for data protection, each technique has inherent limitations that may reduce its effectiveness when used independently.

Ali et al. (2024), in their state-of-the-art review of steganography techniques, examined recent developments in Least Significant Bit (LSB)-based image steganography. The study identified improvements aimed at achieving high robustness, increased embedding capacity, and improved undetectability of hidden information. The authors also proposed two techniques: the first for embedding secret data or messages into a cover image, and the second for embedding a secret grayscale image into another grayscale image. Despite these developments, existing steganographic techniques still face challenges in maintaining a suitable balance between embedding capacity, robustness, image quality, and resistance to detection.

Similarly, El-Hady, Abbas, Khanday, Said, and Radwan (2024) examined security challenges associated with cryptography and steganography techniques for securing data. Although cryptographic techniques provide confidentiality by transforming readable information into an unintelligible form, encrypted data may attract the attention of unauthorized users because its existence and encrypted nature are apparent. On the other hand, steganography conceals the existence of secret information within a cover medium, but the concealed data may remain vulnerable if the steganographic medium is detected, analyzed, or compromised. Consequently, relying on either cryptography or steganography alone may not provide adequate protection against increasingly sophisticated security threats.

Furthermore, existing cryptographic and steganographic mechanisms may experience limitations in terms of security strength, computational efficiency, embedding capacity, imperceptibility, robustness, and resistance to various forms of attack. These limitations create a research gap in the development of an improved technique capable of combining the confidentiality provided by cryptography with the concealment capability of steganography.

Therefore, this research addresses the problem of securing data by developing an improved cryptography and steganography technique that provides multiple layers of protection. The proposed approach will encrypt the data before embedding the encrypted information into a digital image using an improved steganographic technique. This combination is intended to protect the content of the data while simultaneously concealing the existence of the communication. The proposed technique will be evaluated based on security strength, embedding capacity, Peak Signal-to-Noise Ratio (PSNR), Mean Squared Error (MSE), robustness, imperceptibility, and resistance to detection and common attacks. The research is expected to provide an improved approach for securing data and enhancing the reliability of secure communication and data storage systems.

Review of Related Works

The word Steganography originates from Greek and literally means "Covered writing" because it is the art of camouflaging information without arising suspicion. It consists of a broad array of secret communication

techniques that disguises the message's very existence. The first record of the term "steganography" was found in the Johannes Trithemius' book *Steganographia* in 1499. Even the specific reference on the title, the book was primarily about cryptographic methods and techniques as well as esoteric subjects. Muralidharan, Cohen, Cohen, & Nissim, (2022).

The very first documented technique of steganography was reported by Herodotus in the fifth century BC, when people used to create messages on tablets covered by wax. In that way, the message remained unnoticed under the wax layer. Also, Herodotus wrote that Histiaeus, the tyrant of Miletus when under the Persian King Darius I, desired to communicate with his Greek son-in-law. In order to do so, had shaved the head of one of most trusted slaves and tattooed the message onto the slave's scalp. When the slave's hair grew back he sends slave with the hidden message and when slave reaches to the destination again he shaved his scalp and retrieve the message Şahin, Çevik, & Takaoğlu, (2021).

Years after, Aeneas Tacticus was in charge of supporting the military communications in a secure way. He described different types in physically hiding a message, such as pigeons, women's earrings and letters with small holes on the paper to cover the text. An additional popular Greek ancient method, known as acrostic, described is disguising a message in a specific section of every word in a text, like a poem. Regardless of its simplicity, acrostics have survived till modern era. The invisible ink was, also, a widely used technique, even in this period. Drawings were also used to hide information by varying the length of a line, the colors, or other features of the picture. We are able to prove that great artists, such as Leonardo Da Vinci, Rafael and Michelangelo, have concealed messages into their paintings Zhao, (2018).

LITERATURE REVIEW

This Chapter provides necessary review of literature which includes Steganographic algorithms and Encryption algorithms. There are several surveys that have already been done in this area of this knowledge. Some of the studies are discussed in this chapter.

Concept of Steganography

The word Steganography originates from Greek and literally means "Covered writing" because it is the art of camouflaging information without arising suspicion. It consists of a broad array of secret communication techniques that disguises the message's very existence. The first record of the term "steganography" was found in the Johannes Trithemius' book *Steganographia* in 1499. Even the specific reference on the title, the book was primarily about cryptographic methods and techniques as well as esoteric subjects Muhammad, Abas, et al (2025). The very first documented technique of steganography was reported by Herodotus in the fifth century BC, when people used to create messages on tablets covered by wax. In that way, the message remained unnoticed under the wax layer.

DESIGN METHODOLOGY OVERVIEW

Research Design

This research adopts a design and experimental research methodology to develop and evaluate an improved hybrid technique for securing data using cryptography and steganography. The study focuses on improving the security of data by integrating an enhanced cryptographic technique with an improved image steganographic technique.

The proposed system combines the security capabilities of RSA cryptography and Least Significant Bit (LSB) image steganography. In the proposed approach, the original data is first encrypted using the improved RSA cryptographic technique. The resulting ciphertext is then embedded into a digital image using an improved LSB steganographic technique. This provides two layers of protection: cryptography protects the confidentiality of the data, while steganography conceals the existence of the encrypted data.

The developed system will be implemented and experimentally tested using different data sizes and cover images. Its performance will be compared with conventional cryptography and steganography techniques to determine the effectiveness of the proposed improvements.

Proposed Data Security Model

The proposed model consists of two major security layers:

Layer 1 – Cryptographic Protection:

The original data is encrypted using an improved RSA cryptographic technique. This transforms the plaintext into ciphertext that cannot be understood without the appropriate private key.

Layer 2 – Steganographic Protection:

The encrypted ciphertext is embedded into a digital image using an improved LSB steganographic technique. The resulting stego-image appears similar to the original cover image, thereby concealing the existence of the encrypted data.

The overall process is represented as:

Plaintext Data → Improved RSA Encryption → Ciphertext → Improved LSB Embedding → Stego-Image

The recovery process is:

Stego-Image → Improved LSB Extraction → Ciphertext → RSA Decryption → Original Data

This combination provides a double layer of security because an attacker must first discover the hidden information and subsequently overcome the cryptographic protection before the original data can be accessed.

Data Collection and Preparation

The study will use different categories of digital data as test messages, including text documents and other suitable confidential information. Digital images of different dimensions and formats will be selected as cover images.

The data will be prepared before encryption by converting it into an appropriate digital representation. The selected cover images will also be examined to determine their dimensions, colour characteristics, and suitability for data embedding.

Different data sizes will be tested to determine the effect of payload size on the quality and performance of the stego-images.

Improved Cryptographic Technique

Cryptography is used in the proposed system to provide confidentiality and protect the content of the data from unauthorized access. RSA is selected as the underlying public-key cryptographic technique.

The improvement to the cryptographic component will focus on strengthening the protection of the data while maintaining an efficient encryption and decryption process. The RSA component will generate a public key and a private key. The public key will be used for encryption, while the private key will be required to recover the original data.

The encryption process can be represented as:

Plaintext $\rightarrow$ Improved RSA Algorithm $\rightarrow$ Ciphertext

The encrypted ciphertext will not be directly transmitted as ordinary encrypted data. Instead, it will be passed to the steganographic component for concealment.

Improved LSB Steganographic Technique

The steganographic component of the proposed system uses an improved Least Significant Bit technique to conceal the encrypted data inside a digital image.

In conventional LSB steganography, the least significant bits of selected pixels are modified to represent the secret message. However, sequential or predictable embedding can make the hidden information more susceptible to detection through steganalysis.

Therefore, the proposed technique will improve the conventional LSB approach by incorporating a controlled and less predictable embedding mechanism. The encrypted data will be distributed across suitable pixel locations while minimizing unnecessary modifications to the cover image.

The improvement will aim to achieve an appropriate balance between:

data embedding capacity;

image quality;

imperceptibility;

robustness; and

resistance to detection.

The embedding process can be represented as:

Ciphertext + Cover Image $\rightarrow$ Improved LSB Embedding $\rightarrow$ Stego-Image

Integration of Cryptography and Steganography

The major contribution of the research is the integration of the improved cryptographic and steganographic techniques into a single data security framework.

The integration will be implemented in the following sequence:

Step 1: Data Input

The user provides the data to be secured.

Step 2: Encryption

The input data is encrypted using the improved RSA technique.

Step 3: Ciphertext Generation

The encrypted output is converted into a suitable binary representation.

Step 4: Data Embedding

The ciphertext is embedded into the selected cover image using the improved LSB technique.

Step 5: Stego-Image Generation

The system generates a stego-image containing the encrypted data.

Step 6: Data Extraction

At the receiving end, the hidden ciphertext is extracted from the stego-image.

Step 7: Decryption

The extracted ciphertext is decrypted using the corresponding RSA private key.

Step 8: Data Recovery

The original data is recovered and presented to the authorized recipient.

System Architecture

The architecture of the proposed system consists of the following modules:

User/Data Input Module

RSA Key Generation Module

Improved RSA Encryption Module

Ciphertext Conversion Module

Cover Image Selection Module

Improved LSB Embedding Module

Stego-Image Generation Module

Data Extraction Module

RSA Decryption Module

Original Data Recovery Module

Performance Evaluation Module

The architecture provides a sequential security process in which the data cannot be directly accessed from the stego-image without successfully completing both the extraction and decryption processes.

Data Extraction and Decryption

The receiver will provide the stego-image to the extraction component of the proposed system. The improved LSB extraction algorithm will identify the locations containing the hidden ciphertext and recover the encrypted data.

The extracted ciphertext will then be passed to the RSA decryption component. Using the appropriate private key, the ciphertext will be transformed back into the original plaintext.

The recovery process is represented as:

Stego-Image → Improved LSB Extraction → Ciphertext → Improved RSA Decryption → Plaintext

Successful recovery of the original data will demonstrate the functional correctness of the proposed system.

Performance Evaluation

The proposed technique will be evaluated using cryptographic and steganographic performance measures.

Peak Signal-to-Noise Ratio (PSNR)

PSNR will be used to measure the quality of the stego-image after data embedding. A higher PSNR value indicates that the stego-image is closer to the original cover image and that the modifications caused by embedding are less noticeable.

Mean Squared Error (MSE)

MSE will measure the average difference between the original cover image and the stego-image. A lower MSE indicates lower image distortion.

Embedding Capacity

Embedding capacity will measure the quantity of encrypted data that can be hidden in a cover image while maintaining acceptable image quality.

Robustness

Robustness will measure the ability of the proposed system to preserve the hidden information under selected image manipulations and attacks.

Imperceptibility

Imperceptibility will determine how difficult it is to visually distinguish the stego-image from the original cover image.

Security Strength

Security strength will be evaluated based on the protection provided by the improved RSA encryption and the concealment provided by the improved LSB technique.

Resistance to Steganalysis

The proposed system will be tested against selected steganalysis approaches to determine whether the presence of hidden information can be detected.

Encryption and Decryption Time

The time required to encrypt and decrypt different data sizes will be measured to determine the computational efficiency of the proposed cryptographic component.

Comparative Analysis

The performance of the proposed technique will be compared with conventional RSA cryptography, conventional LSB steganography, and, where applicable, existing hybrid cryptography-steganography techniques.

The comparison will focus on:

Parameter	Conventional Technique	Proposed Technique
Data confidentiality	Evaluated	Evaluated
Embedding capacity	Evaluated	Evaluated
PSNR	Evaluated	Evaluated
MSE	Evaluated	Evaluated
Robustness	Evaluated	Evaluated
Imperceptibility	Evaluated	Evaluated
Resistance to steganalysis	Evaluated	Evaluated
Encryption time	Evaluated	Evaluated
Decryption time	Evaluated	Evaluated

The results obtained from the experiments will be analyzed to determine whether the proposed improvements provide better security and performance than the conventional techniques.

Validation of the Proposed Technique

The proposed system will be validated through repeated experiments using different cover images and different data payload sizes. The experimental results will be recorded and analyzed using appropriate statistical and performance analysis techniques.

The validation will establish whether the proposed combination of improved cryptography and steganography can provide:

- stronger data confidentiality;
- improved concealment of secret information;
- acceptable image quality;
- adequate embedding capacity;
- improved resistance to detection and attacks; and
- reliable data recovery.

Expected Methodological Outcome

The methodology is expected to produce an integrated data security system in which cryptography and steganography complement each other. The improved RSA technique will provide protection for the actual content of the data, while the improved LSB technique will conceal the existence of the encrypted information. Consequently, the proposed approach is expected to provide stronger protection than using either cryptography or steganography independently and to demonstrate the potential of an improved hybrid technique for secure data transmission and storage.

Population of the Study

The population of this study comprises of all management information system (MIS) and Information and Communication Technology (ICT) staff and computer science students in the school of Secondary Education (Science Programmes), Federal College of Education (Special), Oyo. Computer subjects like web design and development, system analysis and design, and computer logic was considered

Research Instrument

The instrument used for this study consisted of a developed integrated cryptographic and image steganographic software system and an evaluation checklist/questionnaire designed for performance assessment.

The integrated system served as the primary instrument for data collection and experimentation. The system was developed using the Advanced Encryption Standard (AES) algorithm for data encryption and the Least Significant Bit (LSB) image steganographic technique for embedding encrypted information into digital images. The system enabled the processes of encryption, image embedding, extraction, and decryption for evaluating the effectiveness of the proposed security framework.

RESULTS AND DISCUSSION

The findings of this study revealed that securing data remains a critical challenge in modern information systems due to the increasing rate of cyber threats, unauthorized access, interception, modification, and disclosure of digital information. The results obtained from the five research questions provide evidence that the use of improved cryptographic and steganographic techniques can enhance the security of data. The findings demonstrate that integrating cryptography with image steganography provides multiple layers of protection by securing the content of data while simultaneously concealing the existence of the protected information.

The findings of the first research question indicate that improved cryptographic techniques provide an effective mechanism for protecting data confidentiality. Through encryption, readable data is transformed into ciphertext, making the information unintelligible to unauthorized users. The result demonstrates that cryptographic techniques remain essential for protecting data against unauthorized access and interception. This finding agrees with Swanzy, Ansong, and Abukari (2024), who emphasized the importance of encryption as a fundamental mechanism for protecting information and supporting key information security requirements.

The findings of the second research question further demonstrate that improved steganographic techniques can enhance data security by concealing encrypted information within a digital image. The use of an improved Least Significant Bit (LSB) technique enables the encrypted data to be embedded into a cover image while maintaining an acceptable level of image quality. This provides an additional security layer because an unauthorized user may not easily recognize that confidential information is contained within the image.

The findings of the third research question indicate that combining improved cryptography and steganography provides greater protection than relying on either technique independently. Cryptography protects the content of the data, whereas steganography conceals the existence of the data. The integration of both techniques therefore reduces the weaknesses associated with standalone security mechanisms and provides a double-layer approach to data protection.

The findings of the fourth research question show that the proposed technique provides acceptable steganographic performance in terms of image quality, embedding capacity, and concealment. The use of performance measures such as Peak Signal-to-Noise Ratio (PSNR) and Mean Squared Error (MSE) provides an objective basis for determining the level of distortion introduced into the cover image during the embedding process. A high PSNR and low MSE indicate that the resulting stego-image maintains a high

level of similarity to the original cover image, thereby improving the imperceptibility of the hidden information.

The findings of the fifth research question demonstrate that the proposed integrated technique contributes to improved resistance against unauthorized detection and access. Since the data is encrypted before it is embedded into the image, an attacker who successfully extracts the hidden information would still require the appropriate cryptographic key to recover the original data. This combination of encryption and concealment consequently provides an additional barrier against potential attacks.

The consistently high mean scores obtained from Research Questions Three, Four, and Five indicate that respondents strongly support the adoption of improved integrated cryptographic and steganographic techniques for securing data. The findings suggest that the proposed approach can improve confidentiality, concealment, data protection, and secure communication while maintaining acceptable image quality and embedding capacity.

Overall, the results demonstrate that improved cryptography and steganography complement each other in securing digital data. The cryptographic component provides protection for the actual content of the information, while the steganographic component conceals the existence of the protected information. Therefore, the integration of these techniques provides a stronger and more comprehensive security framework than the independent application of either technique. The proposed approach has potential applications in secure communication, financial transactions, healthcare information systems, military and government communication, cloud-based information systems, and confidential data storage and transmission.

CONCLUSION

This study concludes that data security can be enhanced through the application and integration of improved cryptography and steganography techniques. The study established that protecting sensitive information requires security mechanisms that can provide both confidentiality and concealment against unauthorized access, interception, disclosure, and other cyber threats.

The findings revealed that cryptography provides an important layer of security by converting plaintext information into ciphertext, thereby preventing unauthorized users from understanding the protected data. However, cryptography alone does not conceal the existence of the communication or the encrypted information. Steganography, on the other hand, provides concealment by embedding secret information within a digital medium, particularly an image, thereby reducing the likelihood of the hidden information being noticed. Nevertheless, steganography alone may not provide adequate protection for the actual contents of the concealed information if the hidden data is discovered and extracted.

The study therefore concludes that the use of improved cryptography and improved steganography techniques in an integrated security framework provides a stronger approach to data protection. In the proposed approach, sensitive data is first encrypted using the improved cryptographic technique and the resulting ciphertext is subsequently embedded into a digital image using the improved Least Significant Bit (LSB) steganographic technique. This creates a layered security mechanism in which the data is both encrypted and concealed.

Furthermore, the integration of the two techniques improves the overall security of sensitive information by introducing multiple levels of protection. An unauthorized individual would need to detect the existence of the hidden information, extract the concealed ciphertext, and successfully decrypt it before the original message could be obtained. This makes the proposed approach more difficult to compromise than relying on cryptography or steganography independently.

The study also concludes that the effectiveness of the proposed technique can be assessed using parameters such as Mean Squared Error (MSE), Peak Signal-to-Noise Ratio (PSNR), embedding capacity,

imperceptibility, robustness, and security strength. These measures provide a basis for determining the ability of the improved techniques to protect data while maintaining the quality of the carrier image.

In conclusion, Securing Data Using Improved Cryptography and Steganography Techniques provides a comprehensive approach to information security by combining the strengths of encryption and information hiding. The proposed integrated technique enhances confidentiality and concealment of sensitive information and can be applied to secure communication, confidential data transmission, financial information, healthcare records, military information, and other environments where secure data protection is required

RECOMMENDATION

Based on the findings and conclusion of this study, the following recommendations are made:

Organizations and Institutions should adopt integrated security systems that combine cryptographic and image steganographic techniques for the protection of sensitive information rather than relying solely on standalone security methods.

Information Technology (IT) departments and cybersecurity professionals should implement multi-layer security frameworks that incorporate encryption and steganography to enhance confidentiality, prevent unauthorized access, and reduce the risk of data breaches.

Educational institutions should incorporate practical training on cryptography and steganography into computer science, information technology, and cybersecurity curricula to equip students with modern data protection skills.

Government agencies and private organizations should invest in advanced data security technologies that integrate encryption algorithms such as AES with image steganographic techniques to safeguard classified and confidential information.

Software developers and system designers should develop user-friendly integrated security applications that combine cryptographic and steganographic functionalities for secure data storage and transmission across digital platforms.

REFERENCES

1. Hashmi, M., Yamin, M., & Yayilgan, S. Y. (2024). Artificial intelligence and information security: Emerging challenges and opportunities in modern cybersecurity systems. *International Journal of Information Security*, 23(2), 145–162.
2. Haverkamp, I., & Sarmah, D. K. (2024). Evaluating the merits and constraints of cryptography-steganography fusion: A systematic analysis. *International Journal of Information Security*, 23, 2607–2635. <https://doi.org/10.1007/s10207-024-00853-9>
3. Kombrink, M. H., Geradts, Z. J. M. H., & Worring, M. (2024). Image Steganography Approaches and Their Detection Strategies: A Survey. *ACM Computing Surveys*, 57(2), Article 33. <https://doi.org/10.1145/3694965>
4. Rezaei, S., & Javadpour, A. (2024). Bio-Inspired algorithms for secure image steganography: Enhancing data security and quality in data transmission. *Multimedia Tools and Applications*, 83, 82247–82280.
5. Rajabi-Ghaleh, A., Rahmani, M., & Hosseini, S. (2024). Enhancing secure communication through RSA-AES cryptographic integration and image steganography techniques. *International Journal of Computer Applications*, 186(7), 15–28.
6. Rezaei, M., & Javadpour, N. (2024). Bio-inspired optimization algorithms for secure image steganography and information hiding. *Multimedia Tools and Applications*, 83(12), 34567–34589.

7. Swanzy, P., Ansong, E., & Abukari, A. (2024). Data security frameworks for cloud computing environments: Ensuring confidentiality, integrity and availability of information. *Journal of Information Assurance and Security*, 19(3), 201–215.
8. Xiao, L., Chen, L., Lai, J., & Liu, S. (2024). Deep learning-based image steganography using generative adversarial networks for secure information hiding. *Expert Systems with Applications*, 245, 122–138.
9. Ali, A., et al. (2024). Optimize Image Steganography Based on Distinction Disparity Value and HMPSO to Ensure Confidentiality and Integrity. *Journal of Computer Networks and Communications*. <https://doi.org/10.1155/2024/2516567>
10. El-Hady, M., Abbas, M. H., Khanday, F. A., Said, L. A., & Radwan, A. G. (2024). DISH: Digital image steganography using stochastic-computing with high-capacity. *Multimedia Tools and Applications*, 83, 66033–66048. <https://doi.org/10.1007/s11042-023-17998-9>
11. Muralidharan, T., Cohen, A., Cohen, A., & Nissim, N. (2022). The infinite race between steganography and steganalysis in images. *Signal Processing*, 199, 108711. <https://doi.org/10.1016/j.sigpro.2022.108711>
12. Şahin, F., Çevik, T., & Takaoğlu, M. (2021). Review of the literature on the steganography concept. *International Journal of Computer Applications*, 183(2), 38–46. <https://doi.org/10.5120/ijca2021921298>