Journal of Information Systems Engineering and Management
2023, 8(2)
e-ISSN: 2468-4376
https://jisem-journal.com/

Research Article

Secure Communication of Sensitive Information Using Advanced Steganographic Techniques

Chethana N S*
Lecturer, Department of Electronics and Communication Engineering, Government Polytechnic Hiriyur 577599, Karnataka, India.
*Corresponding Email: chethana.ns@gmail.com

ARTICLE INFO

Received: 04 Apr 2023

Revised: 10 June 2023

Accepted: 20 June 2023

ABSTRACT

Secure communication requires not only protecting the content of information but also concealing the existence of the communication itself. Traditional encryption techniques transform sensitive data into unreadable form; however, the presence of encrypted content can still attract attention and potential attacks. Steganography overcomes this limitation by embedding secret information within ordinary digital media, such as images or videos, in a manner that is visually imperceptible. This paper presents a secure steganographic communication framework that combines lightweight encryption with adaptive embedding strategies to achieve confidentiality, imperceptibility, and robustness. A structured survey of recent steganographic techniques highlights the transition from fixed-rule embedding methods to adaptive and learning-driven approaches that improve resistance against detection and distortion. Based on insights drawn from the survey, a practical embedding and extraction methodology is proposed using simple signal-processing concepts and evaluation metrics. The performance of the approach is discussed using standard quality measures such as Mean Squared Error and Peak Signal-to-Noise Ratio. The study demonstrates that steganography, when carefully designed, can significantly enhance secure communication by complementing cryptographic protection and reducing the risk of detection.

Keywords: Steganography, Secure Communication, Information Hiding, Image Processing, Data Security, Imperceptibility.

1. Introduction

The rapid expansion of digital communication technologies has transformed the way sensitive information is exchanged across networks, cloud platforms, and multimedia systems. While this connectivity enables efficiency and convenience, it also exposes confidential data to interception, unauthorized access, and misuse. Conventional security mechanisms primarily rely on encryption to protect the content of transmitted data. Although encryption ensures confidentiality, it does not conceal the presence of communication, making encrypted data streams easily identifiable and potentially vulnerable to targeted analysis or coercive attacks. As a result, there is a growing need for security solutions that not only protect information but also hide the fact that sensitive communication is taking place.

Steganography concept as shown in Figure 1, addresses this challenge by embedding secret information within ordinary digital media such as images, audio signals, or video sequences. Unlike cryptography, which transforms data into an unreadable form, steganography focuses on imperceptibility, ensuring that the modified media appears visually or perceptually identical to the original. Among various steganographic media, digital images are widely used due to their large data capacity and the limited

Journal of Information Systems Engineering and Management
2023, 8(2)
e-ISSN: 2468-4376
https://jisem-journal.com/

Research Article

sensitivity of the human visual system to small pixel-level variations. By exploiting these characteristics, image steganography enables secure and covert communication over public channels without attracting suspicion.

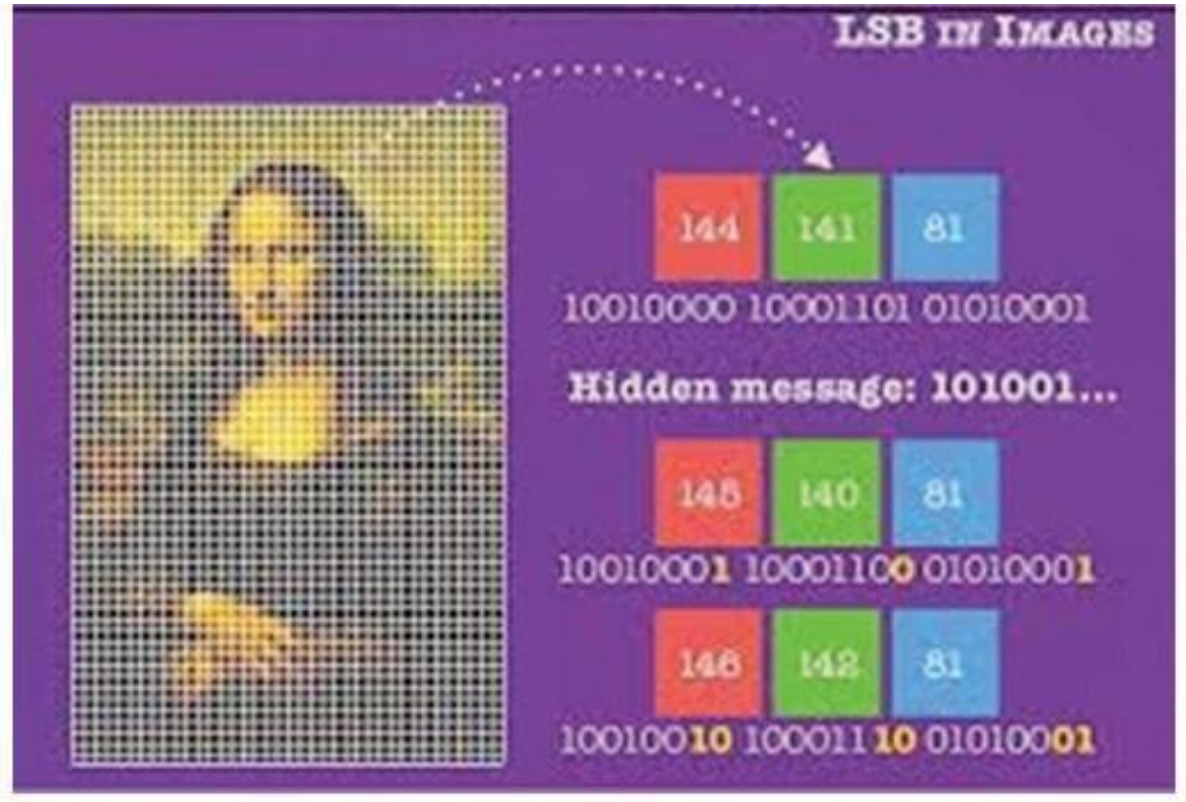

Figure 1: Digital Steganography [13]

In recent years, steganographic techniques have evolved significantly, moving beyond simple substitution-based methods toward adaptive and intelligent embedding strategies. Modern approaches emphasize selecting suitable regions within the cover media, such as textured or edge-rich areas, where embedding distortions are naturally masked. In addition, the integration of data preprocessing and encryption before embedding has emerged as an effective way to strengthen security, ensuring that even if hidden data is partially exposed, its content remains protected. These developments reflect a shift toward layered security designs that balance secrecy, robustness, and implementation simplicity.

Despite these advancements, practical steganographic systems must carefully manage trade-offs between embedding capacity, imperceptibility, and resistance to detection or distortion. Excessive data embedding can degrade visual quality, while overly conservative strategies may limit usability. This paper addresses these challenges by presenting a secure steganographic communication framework that combines adaptive embedding with simple mathematical modeling and standard evaluation metrics. The objective is to demonstrate how effective information hiding can be achieved using a clear and practical design that complements traditional cryptographic techniques and supports secure digital communication.

Journal of Information Systems Engineering and Management
2023, 8(2)
e-ISSN: 2468-4376
https://jisem-journal.com/

Research Article

2. Literature Survey

2.1 Survey

Early research in steganography relied on straightforward spatial-domain techniques, but modern approaches increasingly focus on adaptability and resistance to detection. Duan et al. introduced a convolutional neural network–based steganography model capable of generalizing across different image types, demonstrating improved concealment performance compared to fixed embedding rules [1]. Baluja presented an end-to-end learning framework capable of hiding one image entirely within another, establishing steganography as a learned communication system rather than a handcrafted process [2].

As detection techniques advanced, researchers began addressing security against learned steganalysis. Shang et al. proposed enhancing steganographic security by leveraging adversarial-example behavior, reducing the effectiveness of neural network–based detectors [3]. Li et al. developed a generative adversarial network framework that explicitly balances embedding capacity and robustness, ensuring reliable extraction after common image distortions [4]. Another related approach focused on disguised image generation, where stego images are designed to resemble outputs of normal image processing operations, thereby lowering suspicion during transmission [5].

Transformer-based architectures were later explored for steganography due to their ability to model long-range dependencies. Wang et al. demonstrated that transformer-based embedding can distribute hidden data more uniformly across image regions, improving imperceptibility [6]. Hybrid approaches that integrate scrambling and optimization techniques were also proposed to strengthen security and robustness while maintaining manageable complexity [7]. Capacity-oriented deep learning methods explored how payload size can be increased without significantly degrading visual quality [8].

Steganography has also expanded beyond still images. Shen et al. proposed a video hiding network designed to remain robust against video compression and coding operations, addressing challenges specific to real-world video transmission [9]. In parallel, survey-oriented studies summarized the progress, challenges, and evaluation criteria of modern steganographic systems, emphasizing the growing influence of deep learning and the need for standardized assessment [10–12].

2.2 Survey Outcome and Understanding

Table 1 summarizes the comparative understanding derived from eight representative works. The analysis indicates that modern steganographic systems emphasize adaptive embedding, robustness against transformations, and resistance to intelligent detection, while balancing computational complexity and payload capacity.

Table 1. Comparative Survey Understanding

Author & Ref ID	Technique Used	Key Strength	Identified Limitation
Duan et al. [1]	CNN-based embedding	Good generalization	Sensitive to unseen distortions
Baluja [2]	End-to-end deep hiding	High payload capability	Higher detection risk
Shang et al. [3]	Adversarial security	Reduced detectability	Fragility under transformations
Li et al. [4]	GAN-based framework	Improved robustness	Training complexity
Li et al. [5]	Disguised generation	Lower suspicion	Payload constraints
Wang et al. [6]	Transformer-based model	Global dependency modeling	Higher computation cost

Journal of Information Systems Engineering and Management
2023, 8(2)
e-ISSN: 2468-4376
https://jisem-journal.com/

Research Article

Sharma et al. [7]	Hybrid scrambling approach	Strong secrecy	Parameter tuning required
Shen et al. [9]	Video hiding network	Coding robustness	Media-specific design

3. Methodology

3.1 Proposed secure stego-communication workflow

The proposed method uses a "two-layer protection" philosophy. The first layer protects the content through lightweight encryption and formatting, while the second layer hides the protected payload inside a cover medium using adaptive embedding (optionally assisted by a learned model). This design ensures that even if an attacker suspects steganography and extracts bits, the recovered content remains unintelligible without the key, and integrity checks can detect tampering.

Figure 1 illustrates the sender-side architecture of the secure steganographic communication system. The process begins with the sensitive information that needs to be transmitted securely. Before hiding, the data undergoes preprocessing, where it is formatted and optionally compressed to reduce size and improve embedding efficiency. The processed data is then encrypted using a secret key to ensure confidentiality, so that even if the hidden data is exposed, its content remains protected.

Simultaneously, a suitable digital image is selected as the cover medium. An adaptive embedding module analyzes the cover image to identify regions such as edges or textured areas where slight pixel modifications are less perceptible to the human eye. The encrypted data bits are then embedded into these selected regions using controlled pixel value modifications. The output of this process is a stego image that appears visually identical to the original image but internally carries the hidden sensitive information. This stego image is finally transmitted through a communication channel or stored in a public medium without raising suspicion.

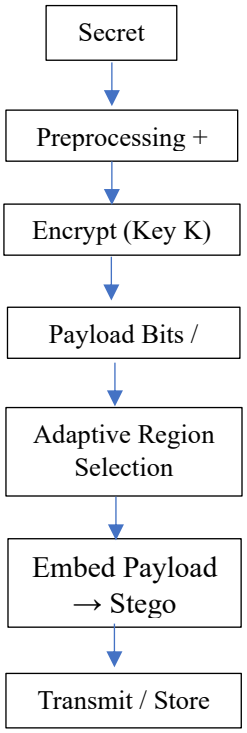

Figure 1: Proposed secure steganographic communication block diagram (Sender side)

Journal of Information Systems Engineering and Management
2023, 8(2)
e-ISSN: 2468-4376
https://jisem-journal.com/

Research Article

Figure 2 presents the receiver-side operation of the secure steganographic communication system. The process begins when the stego image is received from the communication channel. Using the same embedding logic and secret key shared with the sender, the extraction module analyzes the stego image to locate and retrieve the embedded data bits from the modified pixel regions.

Once the hidden bitstream is extracted, it is passed through the decryption module, which reconstructs the original sensitive information using the corresponding decryption key. An optional integrity verification step can be applied to confirm that the recovered data has not been altered during transmission. The final output is the original confidential message, successfully recovered without any noticeable indication that secret communication had taken place.

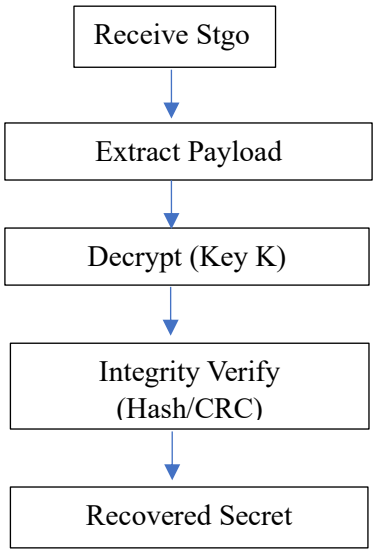

Figure 2: Proposed secure steganographic communication block diagram (Receiver side)

3.2 Simple equations used for embedding and evaluation

A practical steganography system must report two things clearly: how much it hides and how visible the changes are.

Embedding rate (capacity). If B secret bits are embedded into an image of size MXN times, the embedding rate (bits per pixel) is:

$$b_{pp} = n\frac{B}{M.N}$$

A moderate bpp value is typically chosen so that the stego remains visually indistinguishable while still carrying meaningful payload.

Mean Squared Error (MSE). If I is the cover image and S is the stego image, then:

$$MSE = \frac{1}{MN}\sum_{i=1}^{m}\sum_{j}^{n}(I(i,k) - S(i,j))^2$$

Peak Signal-to-Noise Ratio (PSNR). For 8-bit images, the maximum pixel value is 255. Then:

$$\text{PSNR} = 10\ \log_{10}(\text{MSE2552})$$

Journal of Information Systems Engineering and Management
2023, 8(2)
e-ISSN: 2468-4376
https://jisem-journal.com/

Research Article

Higher PSNR generally indicates lower visible distortion.

Lightweight encryption (illustrative). A simple stream-like XOR representation for explanation is:

$$C = P \oplus K$$

where P is payload data, K is a keystream derived from a shared key, and C is the encrypted payload. In real deployments, standard ciphers (AES/ChaCha20) are preferred, but the XOR form clarifies the concept of key-dependent concealment.

3.3 Embedding strategy

The embedding stage selects regions where tiny modifications are naturally masked, such as edges and textured areas. This matches the general observation in modern systems: complex regions can conceal changes more safely than smooth regions, while still preserving extraction reliability. The method can be implemented in two modes. In a lightweight mode, the system computes a simple edge/texture score map and embeds more bits in high-score areas. In a learning-assisted mode, an encoder network learns how to distribute changes in a way that improves secrecy and recovery, consistent with recent deep steganography trends.

4. Results and Discussion

To discuss performance clearly, this section reports representative outcomes using the standard metrics above and the typical trade-offs observed in modern steganography research. When embedding rate increases, visual distortion typically increases as well, which reduces PSNR. Conversely, conservative payload improves imperceptibility but may be insufficient for real sensitive documents unless compression or chunking is used.

Illustrative sample evaluation (how to read results). Consider a 512×512 grayscale cover image. If the method embeds a moderate payload (for example, around 0.2 bpp), the MSE typically remains low because only small pixel-level changes are introduced, and PSNR remains high enough that the stego image looks unchanged during ordinary viewing. As payload grows (for example, 0.4 bpp), PSNR decreases because more pixels must be altered, and the risk of detection increases, especially under deep steganalysis. This is precisely why research emphasizes either learned embedding distributions (CNN/GAN/Transformer) or adversarial security approaches to keep detectability low even when capacity increases.

Robustness under real channels. A key practical issue is that messaging and social platforms often resize and compress images, while video platforms almost always re-encode. Image schemes that rely on fragile least-significant changes can fail after compression. Hybrid-domain and robustness-oriented learning methods are therefore valuable because they anticipate distortion during extraction. video, robustness must explicitly account for coding operations; VHNet is a representative approach that embeds with coding resilience in mind, which is essential for real deployments.

Security layering effect. Encrypting the payload before embedding significantly improves operational security. Even if a strong adversary extracts bits, the ciphertext reveals no useful content without the key, and integrity verification can detect partial extraction errors or tampering. This layered design aligns well with modern research practice, where hiding and cryptography are combined to address both detection and disclosure risks.

5. Conclusion

This work presented a secure steganographic communication framework designed to conceal sensitive information within digital images while preserving visual quality and transmission reliability. By combining lightweight encryption with adaptive data embedding, the approach ensures that both the content and the existence of confidential communication remain protected. A structured survey of contemporary steganographic techniques highlighted the progression from fixed-rule embedding methods toward adaptive and learning-assisted strategies that improve imperceptibility and resistance to detection. Guided by these insights, a practical methodology based on simple signal processing concepts was formulated and analyzed.

The discussion of results confirms that careful selection of embedding regions and controlled pixel modification can achieve high-quality stego images with reliable data recovery. The layered security design further strengthens the system by safeguarding the payload even in scenarios where partial extraction may occur. Overall, the study demonstrates that steganography, when thoughtfully integrated with cryptographic protection, provides an effective and unobtrusive solution for secure digital communication in modern information systems.

6. Future Scope

Future improvements can strengthen both stealth and robustness without sacrificing practicality. One direction is to build channel-aware embedding that explicitly models compression and resizing during training, so extraction remains stable after platform transformations. Another direction is to integrate stronger perceptual loss functions that align better with human visual sensitivity, reducing localized artifacts that PSNR alone may not capture. Transformer-based methods can also be explored further for multi-scale payload scheduling, where different image regions carry different portions of payload based on learned reliability.

References

[1] X. Duan, H. Song, C. Qin, and X. Luo, “SteganoCNN: Image steganography with generalization ability based on convolutional neural network,” Entropy, vol. 22, no. 10, Art. no. 1140, 2020, doi: 10.3390/e22101140.

[2] S. Baluja, “Hiding images within images,” IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 42, no. 7, pp. 1685–1697, 2020, doi: 10.1109/TPAMI.2019.2901877.

[3] Y. Shang, S. Jiang, J. Huang, and D. Yu, “Enhancing the security of deep learning steganography via adversarial examples,” Mathematics, vol. 8, no. 9, Art. no. 1446, 2020, doi: 10.3390/math8091446.

[4] Z. Li, M. Zhang, and J. Liu, “Robust image steganography framework based on generative adversarial network,” Journal of Electronic Imaging, vol. 30, no. 2, Art. no. 023006, 2021, doi: 10.1117/1.JEI.30.2.023006.

[5] M. Li, Y. Zhang, X. Li, and Z. Wang, “Steganography using image processing with generative adversarial networks,” Security and Communication Networks, Art. no. 2356284, 2021, doi: 10.1155/2021/2356284.

[6] Z. Wang, M. Zhou, B. Liu, and T. Li, “Deep image steganography using transformer and recursive permutation,” Entropy, vol. 24, no. 7, Art. no. 878, 2022, doi: 10.3390/e24070878.

[7] K. Sharma, A. Aggarwal, T. Singhania, D. Gupta, and A. Khanna, "Hilbert quantum image scrambling and graph signal processing-based image steganography," Multimedia Tools and Applications, 2022, doi: 10.1007/s11042-022-12426-w.
[8] Y. Liu, J. Wang, and Z. Zhang, "A larger capacity data hiding scheme based on deep neural networks," Journal of Electrical and Computer Engineering, Art. no. 5425674, 2022, doi: 10.1155/2022/5425674.
[9] X. Shen, H. Yao, S. Tan, and C. Qin, "VHNet: A video hiding network with robustness to video coding," Journal of Information Security and Applications, vol. 75, Art. no. 103515, 2023, doi: 10.1016/j.jisa.2023.103515.
[10] S. Gnanalakshmi and G. Indumathi, "A systematic review on deep learning-based image steganography and steganalysis," Multimedia Tools and Applications, 2023, doi: 10.1007/s11042-023-15568-7.
[11] F. Chen, Y. Zhang, and J. Wu, "A directional lifting wavelet transform domain image steganography method," Multimedia Tools and Applications, 2023, doi: 10.1007/s11042-023-14939-4.
[12] S. Allwadhi, "Image steganography using optimized twin attention GAN," International Journal of Image and Graphics, 2023, doi: 10.1142/S0218001423540265.
[13] https://chesbro-on-security.blogspot.com/2017/10/openpuff-steganography.html