Journal of Computer Networks, Architecture and High Performance Computing
Volume 08, Number 2, April 2026
https://doi.org/10.47709/cnahpc.v8i2.7930

Submitted : 2026-01-30
Accepted : 2026-02-04
Published : 2026-04-30

THE DESIGN OF A HYBRID LSB STEGANOGRAPHY FRAMEWORK WITH ADAPTIVE PIXEL SELECTION AND CHAOS ENCRYPTION FOR SOCIAL MEDIA IMAGES

M Ardi Wiratama Putra[1)], Abdul Rahman[2)]
[1,2)] Universitas MDP, Palembang ,South Sumatera, Indonesia
[1)]mardiwiratamaputra_2426311007@mhs.mdp.ac.id , [2)]arahman@mdp.ac.id

ABSTRACT

The exchange of sensitive data via social media platforms faces dual challenges: the risk of third-party interception and distortion due to image compression. Conventional steganography methods based on Least Significant Bit (LSB) often fail to balance embedding capacity with visual quality and are vulnerable to statistical steganalysis attacks. This research proposes a hybrid steganography framework that integrates multidomain adaptive pixel selection and layered cryptographic security. The pixel selection method combines Canny Edge Detection, Local Binary Pattern (LBP), and Local Entropy to determine optimal Regions of Interest (ROI). Data security is reinforced through content encryption using Advanced Encryption Standard (AES-256) and pixel position scrambling using Arnold Cat Map (ACM). Validation was conducted on 100 images from the ALASKA2 and Dresden datasets. Experimental results demonstrate the system's superior performance in balancing quality and capacity under standard load, the system achieves an average Peak Signal-to-Noise Ratio (PSNR) of 77.85 dB and a Structural Similarity Index (SSIM) of 1.0000. Stress tests confirmed the system's scalability, accommodating a maximum capacity of 3.00 bpp while maintaining safe visual quality (PSNR 51.26 dB). Although the system is fragile against JPEG compression on public timelines, this characteristic is validated to function effectively as a tamper sensitivity feature to detect illegal manipulation. Therefore, this framework is recommended as a solution for secure covert communication via document transmission channels (file sharing) on social media, ensuring high confidentiality and data authenticity.

Keywords: Steganography, Adaptive LSB, Chaos Encryption, Arnold Cat Map, AES-256, Tamper Sensitivity, Social Media Security.

INTRODUCTION

In this era of digital transformation, information technology (IT). The Rapid development of social media platforms and the intensity of digital data exchange have created an urgent need for information protection mechanisms that are not only secure but also resistant to detection attempts. In this context, image steganography has become a crucial method that allows the insertion of secret messages into image pixels without arousing visual suspicion (Gutub & Al-Shaarani, 2020; Şener & Güney, 2024). Even so, modern steganography faces complex challenges in maintaining an optimal trade-off between three main parameters, namely payload capacity, visual quality (imperceptibility), and robustness against artificial intelligence-based steganalysis attacks (Bohra et al., 2024; Kheddar et al., 2024). Therefore, selecting the right basic method and developing it is key to addressing these security challenges.

The conventional Least Significant Bit (LSB) method, which has been popular due to its computational simplicity, has proven to have fundamental weaknesses. This method is vulnerable to advanced statistical analysis such as RS analysis and deep learning-based attacks such as SRNet, which are capable of detecting even the smallest anomalies in the bit structure of an image (Bohang et al., 2025; Rahman et al., 2025). Although recent research has proposed various LSB modifications through adaptive pixel selection and encryption approaches, the majority of these solutions are still limited to the use of one-dimensional selection criteria or validation conducted in overly controlled laboratory environments (Rustad et al., 2022; Sultana et al., 2024). These limitations indicate the need for a more holistic approach to address the remaining vulnerabilities.

In the perspective of Information Systems, this research offers an end-to-end solution to ensure the security and authenticity of data transmission within organizations. The urgency of this technology is reflected in the real challenges in national disaster management, where crowdsourcing platforms such as Peta Bencana.id, which rely on citizen reports via social media, often face data validity issues due to the circulation of hoax photos or recycled old

* Corresponding author

Journal of Computer Networks, Architecture and High Performance Computing
Volume 08, Number 2, April 2026
https://doi.org/10.47709/cnahpc.v8i2.7930

Submitted : 2026-01-30
Accepted : 2026-02-04
Published : 2026-04-30

photos. In this scenario, the hybrid steganography framework functions as an integrity verification mechanism, whereby the system can embed digital signatures containing time and location metadata into the pixels of the report image. Thanks to its tamper sensitivity characteristics, the system is able to detect even the slightest manipulation; if the message fails to be extracted, the authenticity of the image is questionable. This provides a crucial tool for decision makers such as BNPB to filter valid information from data noise on social media, while also supporting integration with modern architectures such as automated microservices. On the other hand, recognizing the potential for misuse of steganography technology for illegal activities, this research also emphasizes ethical aspects through recommendations for controlled implementation with strict verification mechanisms.

The overall aim of this study is to validate the system's performance, balancing quality and capacity, and demonstrating its function as a reliable method for covert communication in social media environments, specifically utilizing the integrity sensitivity characteristic to detect any manipulation

LITERATURE REVIEW

The literature review focuses on three main aspects that form the proposed steganography framework: adaptive LSB method for pixel selection, hybrid cryptography integration (AES and Chaos), and challenges posed by social media image compression.

LSB Steganography and Adaptive Enhancement

The Least Significant Bit (LSB) method is a popular spatial domain steganography technique due to its computational simplicity. However, conventional LSB is vulnerable to statistical steganalysis attacks, such as RS Analysis, due to random bit modifications in uniform pixels. To address this weakness, previous research has focused on modifying LSB through adaptive pixel selection (Adaptive LSB).

a. Integration of LSB with Cryptography: Several studies have proposed hybrid models that combine LSB with cryptographic algorithms such as AES-256 to ensure data confidentiality before the embedding process. Research by Jain et al. (2024) and Alanzy et al. (2023) shows that the combination of adaptive LSB and AES-256 can achieve high visual quality (PSNR >50 dB or even 80–85 dB) and resistance to statistical analysis.
b. Image Analysis-Based Pixel Selection: Efforts to increase capacity and imperceptibility are made by directing bit embedding only to areas with high complexity (edge pixels or textures). Research by Abdullah & Nawaf (2023) combines Discrete Wavelet Transform (DWT) with modified LSB for frequency subband selection, resulting in a significant PSNR improvement compared to traditional LSB.
c. Research Gap: Although many studies use adaptive LSB and encryption, there is a gap in simultaneously integrating various adaptive features. Previous studies have not sufficiently explored the combination of multidomain features such as edge detection (Canny Edge Detection), texture (LBP), and local entropy to determine the optimal Region of Interest (ROI), which is the main focus of this study.

The Modified LSB Model (Rustad et al., 2022) takes a different approach from the Inverted LSB method. This model focuses on minimizing error by finding the best insertion pattern, whether to flip bits or not, to maintain image quality. Although visual quality is maintained, in terms of security, this model only uses RC4 encryption, which is classified as a classic algorithm. An overview of this modified model can be seen in Figure 1

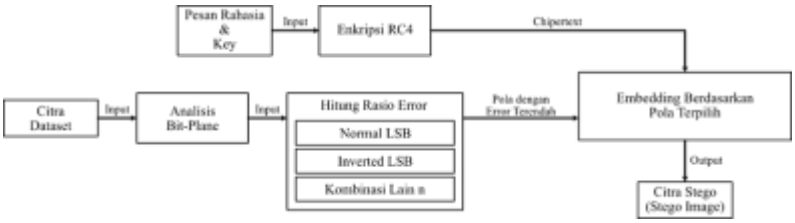

Fig. 1 Inverted LSB Modification Model

Hybrid Cryptography and Layered Security

To address modern steganalysis threats, steganography research has shifted to a hybrid approach that

* Corresponding author

Journal of Computer Networks, Architecture and High Performance Computing
Volume 08, Number 2, April 2026
https://doi.org/10.47709/cnahpc.v8i2.7930

Submitted : 2026-01-30
Accepted : 2026-02-04
Published : 2026-04-30

combines cryptography and steganography. This concept ensures confidentiality and layered security.

Use of AES-256: The Advanced Encryption Standard (AES) is universally used in hybrid steganography studies due to its high security and computational efficiency, ensuring that confidential content cannot be accessed without a key.
Role of Chaos Theory: Chaos theory, specifically using maps such as the Arnold Cat Map (ACM), is used to permute pixel positions. Chaos encryption aims to randomly distribute secret data across the carrier image, destroying statistical patterns that could be exploited by steganalysis.
Combination of Encryption and Permutation: The proposed framework adopts a layered security model: AES for content encryption, followed by ACM for randomizing the position of the encrypted payload before insertion. A literature review shows that although AES is common, the integration of ACM with multidomain adaptive pixel selection (Canny, LBP, Entropy) on spatial LSBs has not been explored in depth for the context of social media images.

Social Media Image Challenges and Integrity Sensitivity

The unique characteristics of images uploaded to social media platforms, such as the presence of destructive compression (JPEG/WebP) and EXIF metadata, create significant challenges for steganography.
Robustness vs. Fragility: Most steganography methods struggle to achieve robustness against social media compression, which can damage hidden data. However, this research utilizes this weakness as a feature.
Tamper Sensitivity (Integrity Verification): JPEG compression occurring on public timelines causes this steganography system to become fragile. This fragility is validated as a tamper sensitivity feature. If the stego image is modified, the hidden data cannot be extracted, which effectively detects illegal manipulation.
Research Focus: This research specifically uses the ALASKA2 dataset (representing social media compression and metadata) and Dresden (for sensor noise representation), which allows testing the system's response to social media channel distortion and validates its effectiveness as an integrity verification mechanism.

Overall, this research aims to fill the research gap by designing a hybrid framework that explicitly addresses the trade-off challenges between capacity, quality, and resistance to steganalysis, through the intelligent combination of multidomain adaptive pixel selection (LBP, Canny, Entropy) and layered cryptography (AES-256 and ACM) in the context of volatile social media compression environments.

METHOD

The research methodology applied in this study was designed to develop and validate a hybrid steganography framework. Broadly speaking, this methodology involves the following systematic steps:

1. Literature Review and Research Gap Identification
   The initial stage involved an in-depth literature review of 37 previous studies (2020–2025) to identify research gaps related to adaptive steganography and chaos encryption.
2. Data Collection and Pre-processing
   The test data was sourced from the ALASKA2 and Dresden standard datasets. These datasets were selected because they represent the characteristics of social media images containing variations in compression and real camera sensor noise. Image preprocessing was performed through format conversion and dimension normalization to ensure input consistency.
3. System Design and Implementation (Hybrid Framework)
   This stage focused on the development of two main modules that form the proposed system:
   - Adaptive Pixel Selection Module (Adaptive Pixel Selection Algorithm Design): This algorithm is multidomain, combining the following criteria:
   - Edge Detection (Canny Edge Detection)
   - Texture Feature Extraction (Local Binary Pattern/LBP)
   - Local Entropy Calculation
   - The goal is to determine the Region of Interest (ROI) or complex area on the image that is safe for message insertion. This process involves weighting and determining the ROI.
   - Hybrid Security Module (Chaos Encryption Module Design): Layered security in

This study was implemented through a series of systematic stages to ensure that each component of the framework

* Corresponding author

Journal of Computer Networks, Architecture and High Performance Computing
Volume 08, Number 2, April 2026
https://doi.org/10.47709/cnahpc.v8i2.7930

Submitted : 2026-01-30
Accepted : 2026-02-04
Published : 2026-04-30

was tested for validity. The general research flow is illustrated in fig.2.

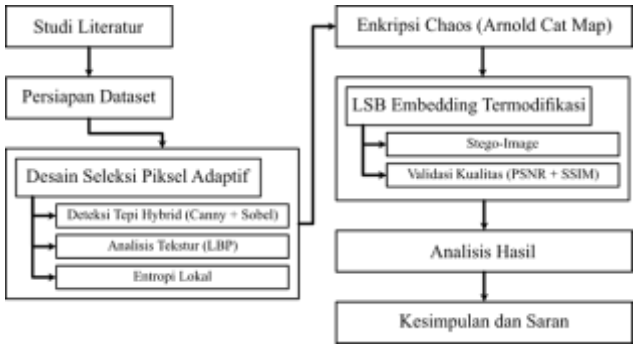

Fig. 2 Flowing Diagram of Research Methodology

The research methodology applied in this study was designed to develop and validate a hybrid steganography framework. Broadly speaking, this methodology involves the following systematic.
Security system designed using a hybrid approach to ensure confidentiality and randomness of data distribution, The performance evaluation is conducted comprehensively using three main testing categories that can be observed. as shown in Fig 3.

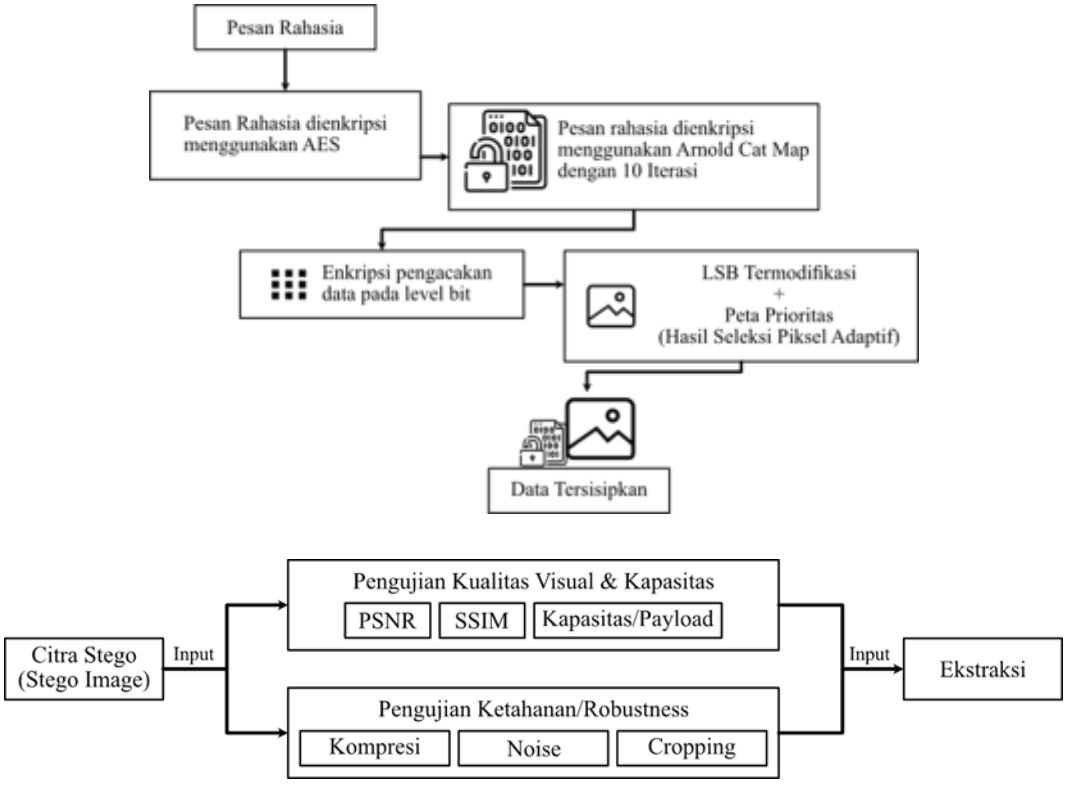

Fig. 3 Hybrid Encryption Scheme of AES and Chaos and Process of Testing and Evaluation

RESULT

The results of this study show that the proposed hybrid steganography framework is capable of achieving several key accomplishments, namely:

Increase in Insertion Capacity and Visual Quality: The system is capable of inserting data up to a maximum of 3.00 bpp (bits per pixel) without significantly compromising visual quality, with an average PSNR value of 77.85 dB and

* Corresponding author

Journal of Computer Networks, Architecture and High Performance Computing
Volume 08, Number 2, April 2026
https://doi.org/10.47709/cnahpc.v8i2.7930

Submitted : 2026-01-30
Accepted : 2026-02-04
Published : 2026-04-30

SSIM of 1.0000. This proves that the multidomain adaptive LSB method is able to overcome the trade-off between capacity and quality that is usually a constraint in conventional steganography. High data security: The integration of AES-256 encryption with chaos encryption (Arnold Cat Map) provides a strong level of security for the embedded data and increases resistance to statistical and brute-force attacks. Test results show that hidden data remains safe from detection and manipulation, and enables detection of illegal manipulation through fragility characteristics against lossy compression such as JPEG. Scalability and Attack Resistance: The system can accommodate capacities of up to 3.00 bpp and maintain high visual quality (PSNR above 51 dB) when tested under maximum load. However, the system is fragile to JPEG compression in the public timeline, which can be used as a sensitivity feature to detect data manipulation.

Risk Profile Analysis and IT Issues. Emprical Validation on the ALASKA2 and Dresden Datasets: The system has been well validated through experiments on social media image datasets containing metadata and sensor noise. The test results show its effectiveness in maintaining visual quality, making it suitable for confidential communication and reporting in social media environments. Operational Efficiency: This framework is capable of securing the transmission of large amounts of sensitive data (up to 425 KB per 1080p image) through public platforms with high confidentiality and guaranteed data authenticity, making it potential for use in cybersecurity applications and confidential organizational communications.

Overall, this research proves that the combined approach of multidomain adaptive pixel selection, AES encryption, and chaos can overcome the limitations of conventional steganography methods while maintaining security, capacity, and visual quality simultaneously.

Compare with Previous Research To position this research, a comparison of features with similar studies is presented in Table 1.

Table 1Comparison with Previous Research

Fitur / Metrik	Penelitian Ini (Proposed)	Sultana dkk. (2024)	Rustad dkk. (2022)
Metode Dasar	Hybrid LSB (Edge+LBP+Entropy)	Hybrid Edge LSB	Inverted LSB
Keamanan	AES-256 + Chaos (ACM)	Tanpa Enkripsi	RC4 (Lemah)
Kualitas (PSNR)	~51,26dB (3,0 bpp) ~77,85 dB (0,006 bpp)	~50 dB	~55 dB
Kapasitas	3,00 bpp	~1,5 bpp	~1,0 bpp
Sifat Sistem	Fragile / Tamper Sensitive	Semi-Robust	Fragile
Validasi Dataset	ALASKA2 & Dresden (100 Sampel)	Standard Images	Standard Images
Kesimpulan	Unggul di Kapasitas Tinggi	Seimbang di Kapasitas Rendah	Baik di Kapasistas Rendah

DISCUSSIONS

This research presents a comprehensive framework integrating adaptive pixel selection, cryptography, and steganography techniques to enhance the security and imperceptibility of hidden data within social media images. The key contributions lie in the development and validation of a hybrid system that optimizes payload capacity while maintaining visual quality and security robustness.

Effectiveness of Adaptive Pixel Selection The proposed adaptive pixel selection mechanism, which combines edge detection, Local Binary Pattern (LBP), and local entropies, effectively identifies optimal regions for data embedding. Tempahasizing the importance of context-aware embedding to balance capacity and visual fidelity.

Security Through Hybrid Encryption The integration of AES-256 encryption with Arnold Cat Map (ACM) permutation introduces a layered security approach. The encryption effectively resists brute-force and statistical analysis attacks, as evidenced by key space analysis and histogram uniformity tests, which show increased resistance to steganalysis. Resilience Against Media Distortion and Attack Robustness tests against JPEG/WebP lossy compression, resizing, cropping, and noise addition exhibit the system's resilience, maintaining payload integrity up to moderate distortion levels. Trade-Offs and Limitations While the system demonstrates high capacity (up to 3 bits per pixel) and maintained visual quality, trade-offs exist in computational complexity due to the multi-step adaptive selection and encryption processes. Practical Implications and Applications The proposed framework's integration into social media platforms aligns with the need for secure and covert communication channels, supporting organizational and social privacy policies. Future Directions Building upon this work, future research should explore the extension to dynamic media, incorporate machine learning-driven adaptive algorithms for improved selection, and evaluate performance under real-world social media workflows.

* Corresponding author

Journal of Computer Networks, Architecture and High Performance Computing
Volume 08, Number 2, April 2026
https://doi.org/10.47709/cnahpc.v8i2.7930

Submitted : 2026-01-30
Accepted : 2026-02-04
Published : 2026-04-30

CONCLUSION

The adaptive pixel selection mechanism designed by integrating edge detection, Local Binary Pattern (LBP), and local entropy has proven to successfully balance the classic trade-offs of steganography. The implementation of integration between the Advanced Encryption Standard (AES-256) and the chaos scheme using the Arnold Cat Map (ACM) successfully created a complementary dual defense system, where AES guarantees high entropy values, while the Arnold Cat Map (ACM) plays a crucial role in eliminating spatial correlations between pixels to prevent visual detection in concentrated insertion areas. Architecturally, this hybrid steganography framework has proven to be feasible for integration into organizational information systems as a covert communication solution, provided that lossless data transmission infrastructure is used.

REFERENCES

Abdelhakm, M., Salah, A., Askar, S., Abouhawwash, M., & Karawia, A. A. (2024). An image steganography algorithm via a compression and chaotic maps. *AIP Advances*, *14*(4). https://doi.org/10.1063/5.0202343

Abdelrazik, H. F., & Mahmoud, A. M. (2024). *International Journal of Intelligent IMAGE STEGANOGRAPHY : A COMPARATIVE AND PRACTICAL STUDY*. *24*(2), 41–57.

Abdullah, S. F., & Nawaf, S. F. (2023). Optimizing Data Security with Hybrid Scheme Based on LSB and DWT. *Tikrit Journal of Engineering Sciences*, *30*(3), 190–199. https://doi.org/10.25130/tjes.30.3.17

Abuali, M. S., Rashidi, C. B. M., Raof, R. A. A., Azir, K. N. F. K., Hussein, S. S., & Abd-Alhasan, A. Q. (2024). Enhancing Security with Multi-level Steganography: A Dynamic Least Significant Bit and Wavelet-Based Approach. *Mathematical Modelling of Engineering Problems*, *11*(6), 1403–1416. https://doi.org/10.18280/mmep.110602

Abuzanouneh, K. I. M., & Hadwan, M. (2021). Multi-Stage Protection using Pixel Selection Technique for Enhancing Steganography. *International Journal of Communication Networks and Information Security*, *13*(1), 55–61. https://doi.org/10.17762/ijcnis.v13i1.4907

Alanzy, M., Alomrani, R., Alqarni, B., & Almutairi, S. (2023). Image Steganography Using LSB and Hybrid Encryption Algorithms. *Applied Sciences (Switzerland)*, *13*(21). https://doi.org/10.3390/app132111771

Alenizi, A., Mohammadi, M. S., Al-Hajji, A. A., & Ansari, A. S. (2024). A Review of Image Steganography Based on Multiple Hashing Algorithm. *Computers, Materials and Continua*, *80*(2), 2463–2494. https://doi.org/10.32604/cmc.2024.051826

Apau, R., Asante, M., Twum, F., Ben Hayfron-Acquah, J., & Peasah, K. O. (2024). Image steganography techniques for resisting statistical steganalysis attacks: A systematic literature review. In *PloS one* (Vol. 19, Nomor 9). https://doi.org/10.1371/journal.pone.0308807

Avantika Bisht, Annu Singla, & Kamaldeep Joshi. (2024). A Review on Image Steganography Techniques. *International Research Journal on Advanced Engineering Hub (IRJAEH)*, *2*(07), 1986–1996. https://doi.org/10.47392/irjaeh.2024.0271

Awadh, W. A., Alasady, A. S., & Hamoud, A. K. (2022). Hybrid information security system via combination of compression, cryptography, and image steganography. *International Journal of Electrical and Computer Engineering*, *12*(6), 6574–6584. https://doi.org/10.11591/ijece.v12i6.pp6574-6584

BHATT, D. P., PARGI, B., & KUMAR, R. (2024). Enhancing Security through Advanced Image Steganography Techniques. *OPSearch: American Journal of Open Research*, *3*(3), 921–927. https://doi.org/10.58811/opsearch.v3i3.97

Bohang, L., Li, N., Yang, J., Alfarraj, O., Albelhai, F., Tolba, A., Shaikh, Z. A., Alizadehsani, R., Pławiak, P., & Yee, P. L. (2025). Image steganalysis using active learning and hyperparameter optimization. *Scientific Reports*, *15*(1), 1–32. https://doi.org/10.1038/s41598-025-92082-w

Bohra, S., Naik, C., Batra, R., Popat, K., & Kaur, H. (2024). Advancements in Modern Steganography Techniques for Enhanced Data Security: A Comprehensive Review. *2024 11th International Conference on Computing for Sustainable Global Development (INDIACom)*, 941–944. https://doi.org/10.23919/INDIACom61295.2024.10498587

Das, D., Durafe, A., & Patidar, V. (2023). An Efficient Lightweight LSB Steganography with Deep Learning Steganalysis. *Computational Intelligence in Image and Video Processing*, 131–154. https://doi.org/10.1201/9781003218111-7

* Corresponding author

Journal of Computer Networks, Architecture and High Performance Computing
Volume 08, Number 2, April 2026
https://doi.org/10.47709/cnahpc.v8i2.7930

Submitted : 2026-01-30
Accepted : 2026-02-04
Published : 2026-04-30

Din, R., Shakir, A. H., Ali, S. H., Qasim Almaliki, A. J., Utama, S., & Almaliki, J. Q. (2024). Exploring Steganographic Techniques for Enhanced Data Protection in Digital Files. *International Journal of Computational Thinking and Data Science*, *1*(1), 1–9. https://doi.org/10.37934/ctds.1.1.19

G, V., & Sargunam, B. (2023). *An Empirical Study for Image Steganography and Steganalysis: A Challenging Overview*. *January*, 1–7. https://papers.ssrn.com/abstract=4518073

Gloe, T., & Böhme, R. (2010). The Dresden Image Database for Benchmarking Digital Image Forensics. *Journal of Digital Forensic Practice*, *3*, 1584–1590. https://doi.org/10.1080/15567281.2010.531500

Gutub, A., & Al-Shaarani, F. (2020). Efficient Implementation of Multi-image Secret Hiding Based on LSB and DWT Steganography Comparisons. *Arabian Journal for Science and Engineering*, *45*(4), 2631–2644. https://doi.org/10.1007/s13369-020-04413-w

Howard, A., Quentin, G., PatrickFrenchie, Cogranne, R., & Cukierski, W. (2020). *ALASKA2 Image Steganalysis*.

Hussain, M., Riaz, Q., Saleem, S., Ghafoor, A., & Jung, K.-H. (2021). Enhanced adaptive data hiding method using LSB and pixel value differencing. *Multimedia Tools and Applications*, *80*(13), 20381–20401. https://doi.org/10.1007/s11042-021-10652-2

Jain, P., Saini, A., Singh, A., & Shreya, S. (2024). Secure Data Transmission with Steganography. *2024 11th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO)*, 1–4. https://doi.org/10.1109/ICRITO61523.2024.10522274

Jamatia, R., & Bhuyan, B. (2023). Comparative Analysis and Performance Metrics Evaluation of Image Steganography Embedding Algorithms. *2023 International Conference on Evolutionary Algorithms and Soft Computing Techniques (EASCT)*, 1–7. https://doi.org/10.1109/EASCT59475.2023.10393229

Jasim, Z. K. J., & Kurnaz, S. (2024). An Improved Image Steganography Security and Capacity Using Ant Colony Algorithm Optimization. *Computers, Materials and Continua*, *80*(3), 4643–4662. https://doi.org/10.32604/cmc.2024.055195

Kataria, M., Jain, K., & Subramanian, N. (2023). Exploring Advanced Encryption and Steganography Techniques for Image Security. *2023 11th International Symposium on Digital Forensics and Security (ISDFS)*, 1–6. https://doi.org/10.1109/ISDFS58141.2023.10131890

Kheddar, H., Hemis, M., Himeur, Y., Megías, D., & Amira, A. (2024). Deep learning for steganalysis of diverse data types: A review of methods, taxonomy, challenges and future directions. *Neurocomputing*, *581*, 127528. https://doi.org/https://doi.org/10.1016/j.neucom.2024.127528

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). https://doi.org/10.1145/3694965

Kumar, M., Soni, A., Shekhawat, A. R. S., & Rawat, A. (2022). Enhanced Digital Image and Text Data Security Using Hybrid Model of LSB Steganography and AES Cryptography Technique. *2022 Second International Conference on Artificial Intelligence and Smart Energy (ICAIS)*, 1453–1457. https://doi.org/10.1109/ICAIS53314.2022.9742942

Madaan, R., Zudock, K. K., & Brown, N. L. (2024). Comparison of Steganography Exploits. *2024 IEEE Integrated STEM Education Conference (ISEC)*, 1. https://doi.org/10.1109/ISEC61299.2024.10665283

Nath, A., Mondal, S., Deb, R., & Das, A. (2021). Data Hiding and Retrieval Method Using LSB Substitution Algorithm. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, *3307*, 267–279. https://doi.org/10.32628/cseit217352

Njoum, M., Sulaiman, R., Shukur, Z., & Qamar, F. (2024). High-Secured Image LSB Steganography Using AVL-Tree with Random RGB Channel Substitution. *Computers, Materials and Continua*, *81*(1), 183–211. https://doi.org/10.32604/cmc.2024.050090

Nourah Alamri, E. al. (2023). New Algorithm to Enhance the Accuracy of Extracting Steganography Hidden Data. *International Journal on Recent and Innovation Trends in Computing and Communication*, *11*(9), 4483–4489. https://doi.org/10.17762/ijritcc.v11i9.9943

Rahman, S., uddin, J., Hussain, H., Shah, S., Salam, A., Amin, F., de la Torre Díez, I., Vargas, D. L. R., & Espinosa, J. C. M. (2025). A novel and efficient digital image steganography technique using least significant bit substitution. *Scientific Reports*, *15*(1), 1–16. https://doi.org/10.1038/s41598-024-83147-3

* Corresponding author

Journal of Computer Networks, Architecture and High Performance Computing
Volume 08, Number 2, April 2026
https://doi.org/10.47709/cnahpc.v8i2.7930

Submitted : 2026-01-30
Accepted : 2026-02-04
Published : 2026-04-30

Rustad, S., Setiadi, D. R. I. M., Syukur, A., & Andono, P. N. (2022). Inverted LSB image steganography using adaptive pattern to improve imperceptibility. *Journal of King Saud University - Computer and Information Sciences*, *34*(6), 3559–3568. https://doi.org/10.1016/j.jksuci.2020.12.017

Selvamani, R., Binti Yusoff, Y., Fatin Liyana Binti Mohd Rosely, N., & BintiMd Siraj, M. (2022). Comparative Analysis on the Image Steganographic Algorithms. *2022 2nd International Conference on Emerging Smart Technologies and Applications (eSmarTA)*, 1–7. https://doi.org/10.1109/eSmarTA56775.2022.9935396

Şener, D., & Güney, S. (2024). Enhancing Steganography in 256×256 Colored Images with U-Net: A Study on PSNR and SSIM Metrics with Variable-Sized Hidden Images. *Review of Computer Engineering Studies*, *11*(2), 13–29. https://doi.org/10.18280/rces.110202

Setiadi, D. R. I. M. (2021). PSNR vs SSIM: imperceptibility quality assessment for image steganography. *Multimedia Tools and Applications*, *80*(6), 8423–8444. https://doi.org/10.1007/s11042-020-10035-z

Sharma, A., Chauhan, R., Bhatt, C., Devliyal, S., & Kumar, R. R. (2024). Securing Data: Cryptography and Steganography. *2024 Asia Pacific Conference on Innovation in Technology (APCIT)*, 1–6. https://doi.org/10.1109/APCIT62007.2024.10673714

Soman, V. K., & Natarajan, V. (2025). Crayfish optimization based pixel selection using block scrambling based encryption for secure cloud computing environment. *Scientific reports*, *15*(1), 2406. https://doi.org/10.1038/s41598-025-86956-2

Sultana, H., Kamal, A. H. M., Apon, T. S., & Alam, M. G. R. (2024). Increasing embedding capacity of stego images by exploiting edge pixels in prediction error space. *Cyber Security and Applications*, *2*(May 2023). https://doi.org/10.1016/j.csa.2023.100028

* Corresponding author