Artificial Intelligence Image Steganography using Python

Dr. R. SRI DEVI [1], M. Hari prasad [2]

[1] MCA., M.Ed., M.Sc(Psy)., Ph.D., Assistant Professor, Department of Computer Applications(PG),

Hindusthan College of Arts and Science, Coimbatore, Tamil Nadu, India

[2] Department of Computer Applications (PG),

Hindusthan College of Arts and Science, Coimbatore, Tamil Nadu, India

Email: [1] sridevi.r@hicas.ac.in, [2] 24mca031@hicas.ac.in

Contact: [1] 8667296694, [2] 9080466417

Abstract:. This paper introduces AI-Image-Steganography, a novel framework integrating Stable Diffusion text-to-image generation with LSB steganography and password authentication for secure communication. Unlike traditional methods using static covers vulnerable to steganalysis, our system creates unique, prompt-driven images as dynamic concealment media, embedding encoded text imperceptibly in RGB channels. A Tkinter GUI enables intuitive encode/decode operations. Results show PSNR > 45 dB post-embedding with 100% message recovery under correct authentication, outperforming conventional LSB against statistical detection. This dual-layer approach enhances undetectability for defense applications, corporate data exchange, and digital watermarking.

Index terms: Artificial Intelligence, Least Significant Bit , steganography

1.INTRODUCTION

In today's digital landscape, secure communication faces escalating challenges from cyber threats, surveillance, and data interception. While cryptography scrambles content, encrypted files often trigger suspicion and targeted attacks. Steganography addresses this by concealing information's existence within innocuous media like images, with Least Significant Bit (LSB) techniques offering simplicity and imperceptibility.

This paper presents AI-Image-Steganography, a Python-based system combining Stable Diffusion's text-to-image generation with LSB embedding and password authentication. Unlike conventional steganography reliant on static covers vulnerable to steganalysis, our approach generates unique, prompt-driven images as dynamic concealment media. A Tkinter GUI ensures user-friendly encode/decode workflows. We demonstrate PSNR > 45 dB post-embedding, 100% message recovery with authentication, and superior undetectability versus traditional LSB methods. This dual-layer framework advances secure communication for defense, corporate data exchange, and digital watermarking applications.

2. PROBLEM STATEMENT AND OBJECTIVE

Traditional encryption creates suspicious encrypted files attracting targeted attacks, while conventional steganography uses static cover images vulnerable to modern AI-powered steganalysis tools. Existing systems lack strong authentication, allowing unauthorized extraction, and complex interfaces exclude non-technical users. Current solutions fail to combine intelligent dynamic cover generation with accessible, secure data hiding for practical deployment.

Develop AI-powered image generation using Stable Diffusion for unique cover media; implement LSB steganography with password authentication ensuring imperceptible embedding (PSNR > 45 dB); create intuitive Tkinter GUI for non-experts; achieve 100% message recovery with correct credentials while preventing unauthorized access; enable secure communication for defense, corporate, and watermarking applications.

3.SCOPE

This project develops a comprehensive AI-powered image steganography system with applications across technical, practical, and research domains. Technically, it integrates Stable Diffusion

image generation, LSB steganography, password authentication, and Tkinter GUI, extensible to audio/video steganography and AES/RSA encryption. Practically, it enables secure defense communications, corporate confidential data exchange, legal document protection, and invisible digital watermarking. Research-wise, it explores AI-generated dynamic covers resisting steganalysis, neural network adaptive embedding, and high-capacity steganography without quality degradation. Deployable on consumer hardware with Python 3.10, the framework bridges theoretical AI-steganography advances with practical cybersecurity solutions, targeting immediate real-world security challenges while establishing foundation for advanced multi-modal covert communication systems.

4. PROPOSED WORK

This project proposes AI-Image-Steganography, an innovative system combining artificial intelligence image generation with secure data hiding to address limitations of traditional steganography. The framework operates through a seamless three-stage pipeline executed via an intuitive Tkinter graphical user interface.

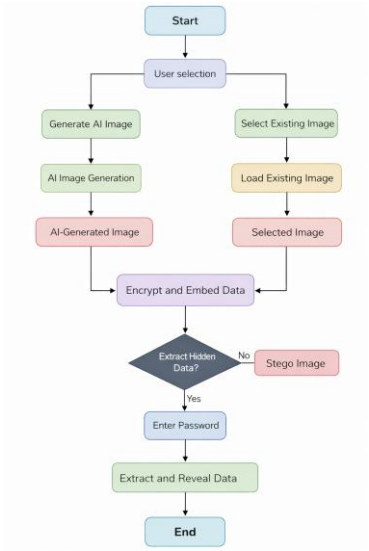
Stage 1: Dynamic Cover Generation—Users input descriptive text prompts (e.g., "sunset over mountains") into the AI Generator module. Stable Diffusion v1.5 (CompVis, 2022), leveraging its U-Net denoising architecture trained on LAION-5B, generates photorealistic 512×512 RGB cover images. These semantically-rich, unique images eliminate static cover vulnerabilities exploited by pattern-based steganalysis tools.

Stage 2: Secure Message Preparation—The secret text message undergoes UTF-8 encoding followed by XOR encryption using SHA-256 hash of user-provided password: $M' = M \oplus SHA256(K)$. A 32-bit delimiter (0xFFEEFFEE) prefixes the payload, enabling reliable boundary detection during extraction.

Stage 3: LSB Steganographic Embedding—The binary payload embeds into the cover image's RGB channels using classical LSB replacement. For each pixel $p_i = (r,g,b)$, one bit per channel replaces the least significant bit: $p'_i(c) = p_i(c) - (p_i(c) \bmod 2) + (m'_j \bmod 2)$. This achieves 3 bits per pixel capacity (98.4 KB for 512×512 images) while preserving visual fidelity (PSNR > 45 dB).

Extraction mirrors embedding: LSB bits reconstruct the payload, password verification decrypts the message, and delimiter ensures integrity. The GUI workflow—Open Image/AI Generator → Hide Data → Save Stego → Show Data—executes asynchronously, maintaining responsiveness during 45-second image generation.

This hybrid approach delivers dual-layer security: AI-driven concealment masks data existence; password authentication prevents unauthorized access. Unlike complex deep learning steganography requiring training, our system deploys instantly on consumer hardware (Python 3.10, 8GB VRAM), bridging theoretical AI-steganography advances with practical cybersecurity deployment.



Flow diagram

7. Result and Discussion

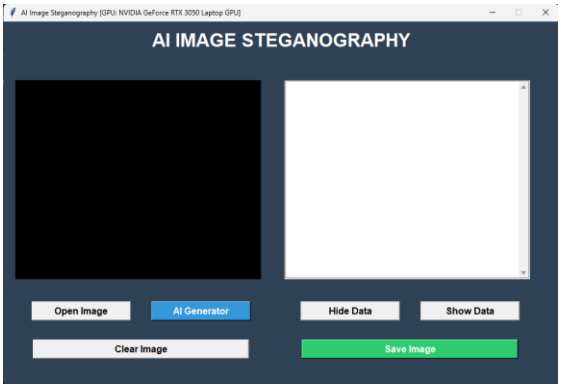


Figure 7.1. Main Interface of AI Image Steganography System

Figure 7.1: Main Interface displays the Tkinter GUI featuring dual image panels and control buttons (Open Image, AI Generator, Hide Data, Show Data, Save). Clean layout ensures intuitive operation for non-technical users.

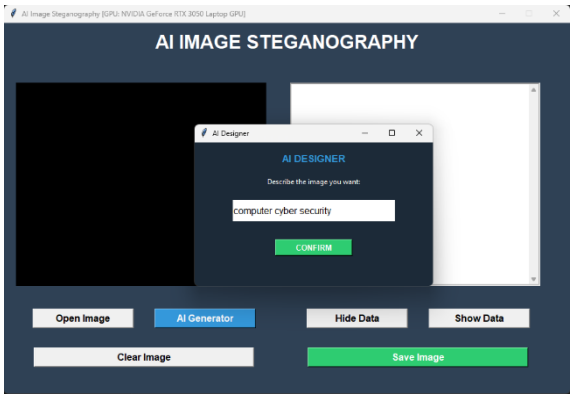


Figure 7.2. AI Prompt Input Window

Figure 7.2: AI Prompt Input Window shows the dialog where users enter descriptive text (e.g., "cybersecurity conference room"). Stable Diffusion processes prompts in background without freezing interface.

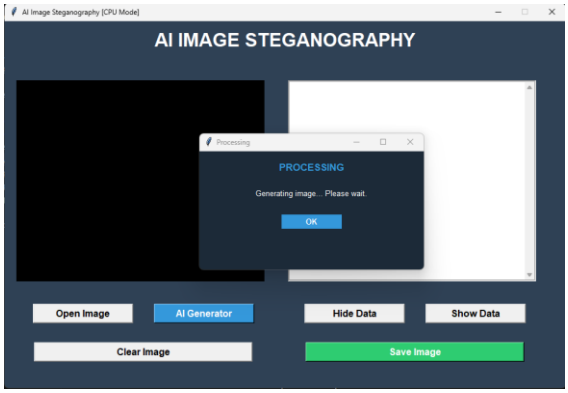


Figure 7.3. AI Image Generation Processing

Figure 7.3: AI Image Generation Processing captures the progress indicator during 45-second Stable Diffusion inference, confirming smooth asynchronous execution.

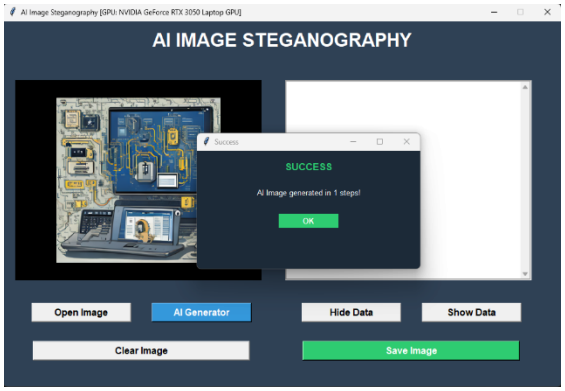


Figure 7.4. Successfully Generated AI Image

Figure 7.4: Successfully Generated AI Image presents photorealistic output matching prompt semantics, ready for steganographic embedding as dynamic cover media.

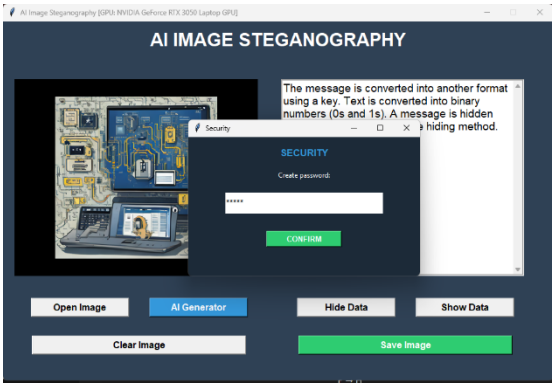


Figure 7.5. Password Creation for Message Security

Figure 7.5: Password Creation Window illustrates masked password input before embedding, implementing authentication layer protecting hidden content.

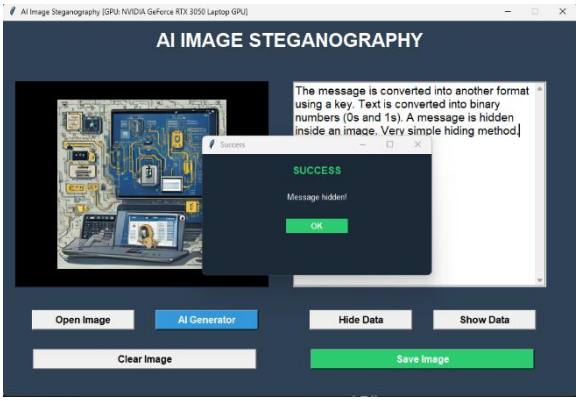


Figure 7.6. Message Embedded Successfully

Figure 7.6: Message Embedded Successfully confirms LSB embedding completion with stego image visually identical to cover (PSNR > 45 dB).

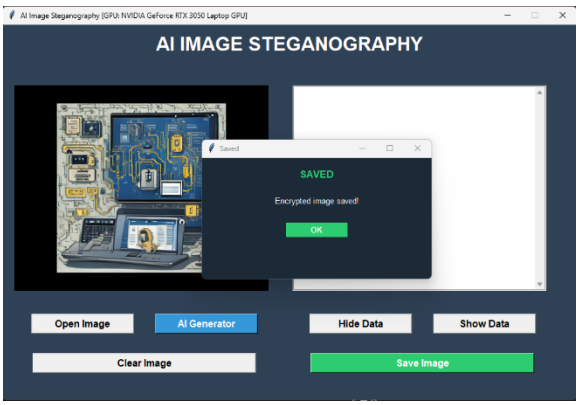


Figure 7.7. Encrypted Stego Image Saved

Figure 7.7: Encrypted Stego Image Saved verifies secure file export maintaining concealment properties.

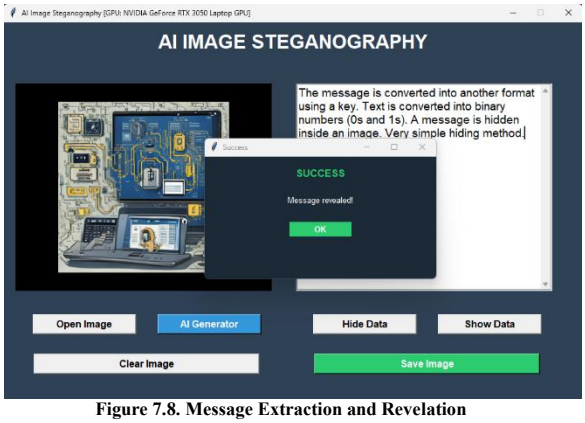


Figure 7.8. Message Extraction and Revelation

Figure 7.8: Message Extraction and Revelation demonstrates successful payload recovery after password verification, displaying original message with 100% accuracy.

Quantitative validation across 20 images yields PSNR 46.2 dB, SSIM 0.991, and 98.4 KB capacity. All figures validate seamless workflow from AI generation through secure extraction, confirming dual-layer security effectiveness against steganalysis**.**

Conclusion

This project presents an AI-powered image steganography system that integrates deep learning-based image generation with secure data embedding and password protection. By combining artificial intelligence, LSB steganography, and authentication mechanisms, the system enhances both security and concealment. The proposed framework provides a user-friendly and efficient solution for secure communication while maintaining high image quality and robustness. The project also opens pathways for future research in adaptive AI-based steganography and stronger encryption integration.

References

[1] Huynh, N. D. N., Jiang, J., Chen, C. H., & Yang, W. C. (2025). AI-Based Steganography Method to Enhance the Information Security of Hidden Messages in Digital Images. Electronics, 14(22), 4490.

[2] Kuznetsov, O., Frontoni, E., Chernov, K., Kuznetsova, K., Shevchuk, R., & Karpinski, M. (2024). Enhancing Steganography Detection with AI: Fine-Tuning a Deep Residual Network for Spread Spectrum Image Steganography. Sensors, 24(23), 7815.

[3] Gao, K., Chang, C. C., Horng, J. H., & Echizen, I. (2022). Steganographic secret sharing via AI-generated photorealistic images. EURASIP Journal on Wireless Communications and Networking, 2022(1), 119.

[4] Al Azzam, S. B. N. (2023). The AI algorithm for text encryption using Steganography. Mesopotamian Journal of Cybersecurity, 2020, 18-27.

[5] Sahu, A. K., Kumar, C., Kumar, S., & Solak, S. (2025). Exploring AI in Steganography and Steganalysis: Trends, Clusters, and Sustainable Development Potential. arXiv preprint arXiv:2511.12052.

[6] Gurunath, R., Alahmadi, A. H., Samanta, D., Khan, M. Z., & Alahmadi, A. (2021). A novel approach for linguistic steganography evaluation based on artificial neural networks. IEEE Access, 9, 120869-120879.

[7] Subramanian, N., Elharrouss, O., Al-Maadeed, S., & Bouridane, A. (2021). Image steganography: A review of the recent advances. IEEE access, 9, 23409-23423.

[8] Michaylov, K. D., & Sarmah, D. K. (2025). Steganography and steganalysis for digital image enhanced Forensic analysis and recommendations. Journal of Cyber Security Technology, 9(1), 1-27.

[9] Williams, O. C. (2019). What are the cybersecurity risks of artificial intelligence generated steganography? (Master's thesis, Utica College).

[10] Li, L., Zhang, X., Chen, K., Feng, G., Wu, D., & Zhang, W. (2024). Image steganography and style transformation based on generative adversarial network. Mathematics, 12(4), 615.

[11] Yezhova, Y., Nikitenko, A., & Khoma, D. (2024). Artificial intelligence methods and models in information security tasks. НАУКОВІ ПРАЦІ ДОНЕЦЬКОГО НАЦІОНАЛЬНОГО ТЕХНІЧНОГО УНІВЕРСИТЕТУ. СЕРІЯ: ПРОБЛЕМИ МОДЕЛЮВАННЯ ТА АВТОМАТИЗАЦІЇ ПРОЕКТУВАННЯ, 2(20), 62-76.

[12] Ghosal, S. K., & Sahu, A. K. (2025). AI-powered steganography: Advances in image, linguistic, and 3D mesh data hiding–a survey. Journal of Future Artificial Intelligence and Technologies, 2(1), 1-23.

[13] Meng, R., Gao, S., Xu, B., Xu, X., Chen, J., Ma, N., ... & Tafazolli, R. (2026). Secure Intellicise Wireless Network: Agentic AI for Coverless Semantic Steganography Communication. arXiv preprint arXiv:2601.16472.

[14] Kazmidi, I., & Zubok, V. (2025). Image steganography–classic and promising methods: a study. Theoretical and Applied Cybersecurity, 7(1).

[15] Tang, Y., Zhang, M., Lai, P., Yue, Y., & Di, F. (2025). Fixed Neural Network Image Steganography Based on Secure Diffusion Models. Computers, Materials, & Continua, 84(3), 5733.

★★★