Stegosuite: Smart Steganography Suite with Ai-Based Detection

Pallavi Bhausaheb Narote[1], Saniya Firoj Shaikh[2], Bhagyashri Dattatray Shinde[3], Samiksha Machhindra Kedare[4], Guide: Rajashri Omkar Tagade[5]
[1,2,3,4,5]*Department of Computer Engineering, Sau. Sundarbai Manik Adsul Polytechnic, Chas, Ahmednagar, Maharashtra, India*

***Abstract*—Steganography is a widely used approach for hiding confidential information inside digital media, allowing secure communication without revealing the presence of hidden data. However, many existing steganographic tools are restricted to a single media format and do not provide adequate security layers or easy-to-use interfaces. In addition, the increasing availability of AI-generated and manipulated media has raised concerns regarding content authenticity. This paper introduces StegoSuite, a smart multimedia steganography system capable of embedding secret data into images, audio, and video files. Prior to embedding, the secret message is encrypted using the Advanced Encryption Standard (AES) to enhance confidentiality. The system also includes an AI-based image analysis module that identifies manipulated or synthetic images using a convolutional neural network. Developed using open-source technologies and a graphical user interface, StegoSuite focuses on both security and usability. Experimental results show high visual quality with PSNR values above 40 dB, minimal distortion, and more than 90% accuracy in detecting fake images. These findings demonstrate that StegoSuite provides an effective and practical solution for secure multimedia communication.**

***Index Terms*—Steganography, Multimedia Security, Cryptography, Deepfake Detection, Audio Steganography, Video Steganography**

I. INTRODUCTION

The rapid expansion of digital communication has increased the need for secure methods to protect sensitive information. Cryptographic techniques successfully secure message content but often expose the existence of communication, which may attract unwanted attention. Steganography overcomes this limitation by concealing secret data within digital media such as images, audio, and video files, making communication difficult to detect.

Most existing steganographic systems are limited to image-based techniques and provide minimal security features. Additionally, the lack of user-friendly interfaces reduces their practical usability, especially for non-technical users. At the same time, advances in artificial intelligence have enabled the creation of realistic synthetic media, increasing the risk of misinformation and fake content. To address these challenges, this work proposes StegoSuite, a unified multimedia steganography platform that combines data hiding, cryptographic protection, and AI-based media analysis. The system is designed to support multiple media formats while maintaining high security and ease of use. By integrating modern security mechanisms with an intuitive graphical interface, StegoSuite aims to provide a reliable and practical solution for secure digital communication.

II. LITERATURE REVIEW

Early research by Johnson and Jajodia [1] and Provos and Honeyman [2] established the foundational concepts of digital steganography. The Least Significant Bit (LSB) technique remains widely used due to its simplicity, although it offers limited robustness. Transform-domain approaches such as Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT) improve resistance to attacks but are computationally more complex.

Audio and video steganography techniques have also been explored; however, they are often implemented as standalone systems without integrated encryption or detection mechanisms. Recent advances in artificial intelligence have enabled effective detection of

synthetic media using convolutional neural networks (CNNs) [7]. Despite their success, these detection systems are rarely integrated into steganographic tools.

StegoSuite distinguishes itself by integrating multi-modal steganography, AES encryption, and AI-based detection into a single, user-centric framework.

Table 1: Comparative Summary of Existing Methods vs. StegoSuite

Method / Tool	Media Type Supported	Security Features	Detection Mechanism	Usability
LSB (Least Significant Bit)	Images	Low	None	Simple but limited
DCT/DWT Transform-domain	Images	Moderate	None	Technical, less user-friendly
Audio Steganography (basic)	Audio	Low	None	Limited scope
Video Steganography (basic)	Video	Low	None	Computationally heavy
AI-based Deepfake Detection	Images	Not applicable	CNN-based detection	Standalone
StegoSuite (Proposed)	Images, Audio, Video	High (AES)	Integrated CNN detection	User-friendly GUI

III. METHODOLOGY

The StegoSuite system is composed of four major functional modules:

3.1 Multimedia Steganography Module

This module enables data embedding in image, audio, and video files using LSB and transform-domain techniques such as DCT and DWT. Supporting multiple media formats enhances flexibility and applicability.

3.2 Cryptographic Preprocessing

Before embedding, the secret message is encrypted using the Advanced Encryption Standard (AES). This step ensures that extracted data remains unreadable without the correct encryption key.

3.3 AI-Based Synthetic Image Detection

A convolutional neural network is trained to classify images as real or manipulated. This module improves content authenticity by identifying deepfakes and altered images.

3.4 Graphical User Interface

A menu-driven graphical interface developed using Python Tkinter allows users to perform embedding, extraction, and detection operations easily without technical expertise.

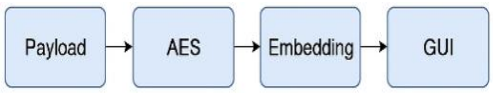

Fig. 1 system architecture of StegoSuite.

IV. RESULTS AND EVALUATION

The system was tested on multiple datasets using image (PNG, JPEG), audio (WAV), and video (MP4) files. The following metrics were evaluated:

Peak Signal-to-Noise Ratio (PSNR): Values consistently exceeded 40 dB, indicating high imperceptibility.

Mean Squared Error (MSE): Low distortion observed across all media types.

AI Detection Accuracy: Achieved greater than 90% accuracy in distinguishing real and fake images.

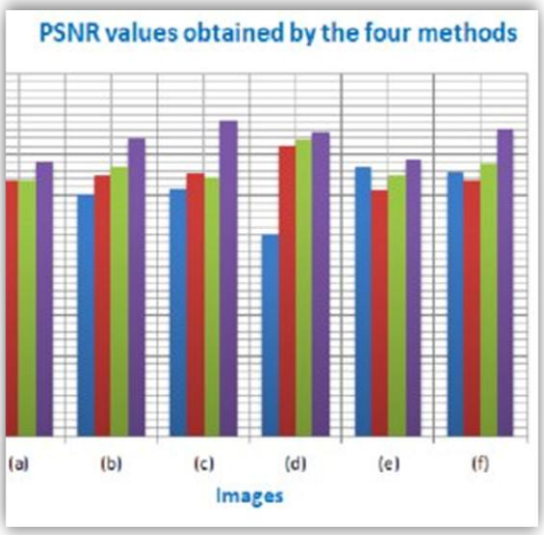

Fig.2shows PSNR values for different embedding techniques.

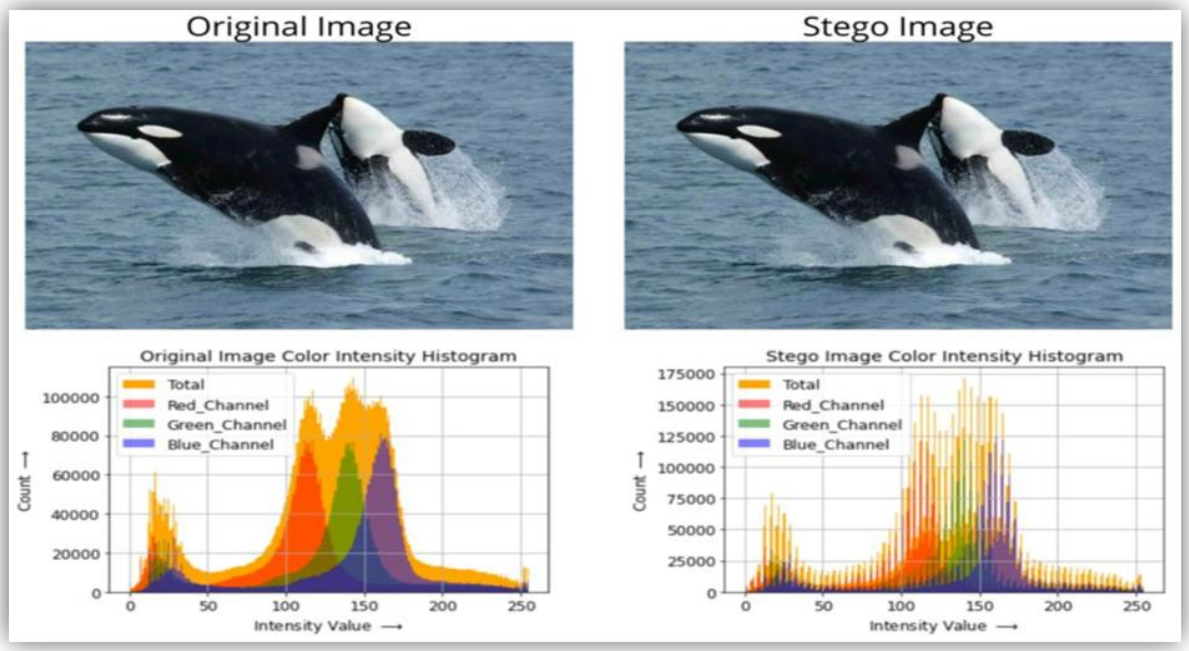

Fig. 3 presents a visual comparison of original and stego images along with their color intensity histograms, demonstrating minimal perceptual difference after embedding.

V. DISCUSSION

StegoSuite offers several advantages over conventional steganographic tools. The multi-modal design enables secure communication across diverse media formats, while AES encryption adds an essential layer of confidentiality. The integration of AI-based detection addresses modern challenges related to synthetic media and misinformation.

The user-friendly GUI enhances accessibility, making the system suitable for both technical and non-technical users. However, processing large video files requires substantial computational resources, and detection accuracy depends on the quality of training datasets. Future work can focus on optimization and dataset expansion to further improve performance.

VI. CONCLUSION

This paper presented StegoSuite, a secure and intelligent multimedia steganography system that combines data hiding techniques with encryption and AI-based detection. The proposed framework supports images, audio, and video files while ensuring data confidentiality through AES encryption. Experimental evaluation confirmed high imperceptibility, low distortion, and reliable detection of manipulated images.

By integrating steganography, cryptography, and artificial intelligence into a single user-friendly platform, StegoSuite addresses both traditional security concerns and modern challenges related to synthetic media. The results indicate that the system is suitable for real-world applications requiring secure and trustworthy multimedia communication.

REFERENCES

[1] N. F. Johnson and S. Jajodia, “Exploring steganography: Seeing the unseen,” IEEE Computer, vol. 31, no. 2, pp. 26–34, 1998.

[2] N. Provos and P. Honeyman, “Hide and seek: An introduction to steganography,” IEEE Security & Privacy, vol. 1, no. 3, pp. 32–44, 2003.

[3] I. Goodfellow, J. Pouget-Abadie, M. Mirza, et al., “Generative adversarial nets,” in Advances in Neural Information Processing Systems (NeurIPS), pp. 2672–2680, 2014.

[4] J. Fridrich, Steganography in Digital Media: Principles, Algorithms, and Applications.

Cambridge, UK: Cambridge University Press, 2009.

[5] F. Chollet, “Xception: Deep learning with depthwise separable convolutions,” in Proc. IEEE Conf. Computer Vision and Pattern Recognition (CVPR), pp. 1251–1258, 2017.

[6] S. Katzenbeisser and F. A. Petitcolas, Information Hiding Techniques for Steganography and Digital Watermarking. Norwood, MA: Artech House, 2000.

[7] T. Zhang, Y. Liu, J. Wang, et al., “A survey on deepfake detection,” ACM Computing Surveys, vol. 53, no. 6, pp. 1–41, 2020.

[8] M. Kharrazi, H. T. Sencar, and N. Memon, “Image steganography: Concepts and practice,” in Proc. WSPC Workshop on Multimedia Security, pp. 1–12, 2004.

[9] Y. Liu, W. Li, P. Luo, et al., “Deep learning for generic object detection: A survey,” arXiv preprint arXiv:1905.00083, 2019.

[10] Y. Wang, X. Zhang, and H. Li, “A review of audio steganography techniques,” IEEE Access, vol. 9, pp. 107–123, 2021.