Mrs.M.Lavanya, 2026, 14:1
ISSN (Online): 2348-4098
ISSN (Print): 2395-4752

International Journal of Science, Engineering and Technology
An Open Access Journal

Stegablock: Dual-Layer Steganography and Watermark System

Mrs.M.Lavanya[1], Yogeswaran R[2], Pragedeeswaran S[3], Palanivel M[4]

[1]Assistant Professor, Department of Computer Science and Engineering Kongunadu College Engineering and Technology Tamilnadu, India

[2,3,4]Department of Computer Science and Engineering Kongunadu College of Engineering and Technology Tamilnadu,India

Abstract- This project introduces an advanced dual-layer security framework that integrates steganography and digital watermarking to strengthen data confidentiality and ownership verification. The proposed system follows a two-stage security model: in the first stage, sensitive information is invisibly embedded within digital media such as images, audio, or video using steganographic techniques, while the second stage applies resilient watermarking methods to ensure copyright protection and verify content authenticity. Least Significant Bit (LSB) manipulation is utilized for efficient data concealment, and Discrete Wavelet Transform (DWT) or Discrete Cosine Transform (DCT) techniques are employed for robust watermark embedding. This combined approach delivers high embedding capacity along with strong resistance to common signal-processing and malicious attacks. The layered architecture guarantees continued protection even if one security layer is breached. Potential applications include secure data transmission, intellectual property protection, medical imaging security, and digital forensic analysis. Experimental results confirm improved imperceptibility, robustness, and overall security compared to conventional single-layer techniques, making the framework well suited for high-security and mission-critical applications.

Keywords: Steganography, Digital Watermarking, Dual-Layer Security,Data Protection and Copyright Authentication

I. INTRODUCTION

In today's digitally driven world, the rapid expansion of information exchange through internet-based platforms has fundamentally transformed communication, business operations, and digital content dissemination. While this transformation has brought unprecedented convenience and accessibility, it has also raised serious concerns related to data security, user privacy, and intellectual property protection. Digital content can be easily copied, altered, and redistributed without authorization, creating a pressing demand for advanced security solutions that ensure both information protection and content authenticity.

Conventional cryptographic techniques are widely used to secure data transmission; however, they exhibit limitations in situations where the mere presence of confidential communication must remain undisclosed or where ownership protection is required after content distribution. These shortcomings have encouraged the adoption of alternative security approaches, notably steganography and digital watermarking, which address different aspects of information security.

Steganography concentrates on concealing secret information within ordinary digital media such as images, audio, or videos in a manner that prevents detection. Its primary goal is imperceptibility, ensuring that unauthorized parties are unaware of any hidden communication. This method is particularly valuable in covert communication scenarios, defense applications, confidential corporate exchanges, and privacy-sensitive data sharing.

In contrast, digital watermarking focuses on safeguarding ownership, verifying authenticity, and

protecting copyrights. Watermarks are embedded directly into digital content and are designed to withstand compression, signal processing, and malicious attacks. Unlike steganography, watermarking prioritizes robustness over concealment, enabling content creators to trace unauthorized usage and validate content integrity.

Individually, each technique has inherent limitations—steganography may be vulnerable to image manipulations, while watermarking does not support hidden communication. To overcome these challenges, hybrid dual-layer security frameworks have emerged, integrating both techniques to provide enhanced protection. Such systems offer secrecy, ownership verification, and resilience against attacks, making them highly suitable for sensitive domains such as medical imaging, military communication, financial data protection, and digital media distribution. This multi-layered approach represents a vital advancement in securing the rapidly evolving digital landscape.

II. RELATED WORKS

Several studies have explored steganography and watermarking techniques using both traditional embedding methods and advanced computational approaches. Existing research can be broadly categorized into spatial-domain steganographic concealment models, transform-domain watermarking schemes, and hybrid security frameworks integrating both methodologies. While conventional single-layer systems focus on either covert communication or copyright protection independently, recent investigations have demonstrated the advantages of dual-layer architectures that combine imperceptibility with robustness, offering enhanced security against diverse attack vectors and multi-purpose applications in digital content protection.

Hybrid Steganography & Watermark Algorithm (Zainal et al., 2024): Proposes a combined steganography and digital watermarking technique for copyright protection using multiple embedding strategies in images. It embeds hidden information and watermark bits to improve imperceptibility and ownership traceability. The work analyses performance under standard metrics and highlights challenges like computational overhead when applied to high-resolution data, paving the way for robust multi-purpose embedding strategies in secure multimedia applications.Deep Learning-Based Image Steganography & Watermarking (Hu et al., 2024)Reviews neural network architectures for image steganography and watermarking. It categorizes models, training strategies, and datasets, comparing how different learning frameworks balance payload capacity, robustness, and imperceptibility. The survey highlights strengths and weaknesses of existing deep learning approaches, discussing open challenges such as attack resilience and dataset biases, making it a key reference for future research in learning-driven data hiding.

Hybrid DCT-GAN Steganography Framework (2025) Introduces a hybrid steganographic framework that integrates Discrete Cosine Transform (DCT) and Generative Adversarial Networks (GANs) to enhance imperceptibility and robustness against steganalysis. The method embeds information in frequency domain and uses GANs to generate stego images that resist detection, offering improved data security and visual fidelity even under common image attacks, useful in high-security communication systems. Robust & Reversible Hybrid Steganography (Scientific Reports) Proposes a hybrid framework using Radon Transform (RT) and Integer Lifting Wavelet Transform (ILWT) for robust and reversible image steganography. This approach enhances resistance to geometric attacks (rotation, scaling) while preserving integer coefficients to avoid data loss. It balances embedding capacity, imperceptibility, and robustness better than traditional DWT-only techniques, suitable for secure communication and authentication.

Data Hiding with Deep Learning (Wang et al., 2021) Comprehensive survey unifying deep learning methods for steganography and digital watermarking across media types. It systematically categorizes model architectures, noise injection techniques, evaluation metrics, and datasets, discussing how deep learning improves resilience and cover integrity. The survey highlights research

gaps and future directions for integrating watermarking and steganography within learning frameworks for enhanced security. FastStamp: Neural Steganography & Watermarking on FPGA Presents a hardware accelerator (FastStamp) for neural network-based steganography and watermarking on FPGA. It proposes a parameter-efficient embedding model optimized for resource-limited devices, achieving major performance gains over GPU implementations. This work demonstrates scalable embedding of recoverable bit-strings and efficient hardware acceleration, advancing practical deployment of secure data hiding on embedded systems.

Robustness & Imperceptibility in Hybrid Watermarking (Nov 2025):Compares spatial (LSB), frequency (DFT), and hybrid LSB+DFT watermarking approaches to evaluate trade-offs between visual quality and resistance to attacks. The hybrid method shows improved balance between imperceptibility and robustness under noise, compression, and distortion, indicating advantages of multi-domain embedding for copyright protection and authentication. Reviews classic steganography and digital watermarking methods, contrasting their objectives, embedding domains, and robustness characteristics. It discusses how steganography focuses on covert communication while watermarking emphasizes content authentication and integrity, helping identify key strengths and limitations of each class of methods.

III. PROPOSED METHOD

System Overview:

The Dual-Layer Steganography and Watermarking System provides comprehensive digital media protection through integrated security mechanisms. The system accepts multimedia input, performs preprocessing for quality optimization and region analysis, then sequentially applies steganographic embedding for covert data concealment and watermark insertion for copyright protection. A unified extraction module enables authorized retrieval of hidden information and ownership verification. This architecture ensures dual-purpose security combining imperceptibility with robustness, protecting sensitive communications while simultaneously enforcing intellectual property rights and content authentication across diverse digital media formats

System Architecture

The proposed system architecture is designed to secure digital media by embedding covert information and ownership verification markers using dual-layer steganography and watermarking techniques.

The architecture comprises four major components: media acquisition, preprocessing and analysis, dual-layer embedding engine, and extraction and verification module. Digital input media including images, audio files, or video content are collected through a structured upload mechanism or integrated from existing multimedia repositories.

The acquired media undergoes preprocessing to analyze quality metrics, detect suitable embedding regions, optimize color space representation, and ensure format compatibility before being forwarded to the security embedding module. A dual-layer approach is employed to enhance protection reliability by sequentially applying steganographic concealment followed by watermark insertion, thereby providing both covert communication capabilities and robust copyright protection with reduced vulnerability to individual layer compromise.

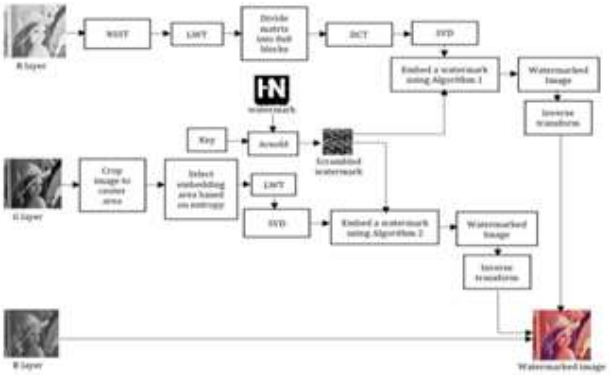

Fig.1. System architecture

Finally, the secured media with embedded secret data and watermark is presented through an extraction and verification interface, enabling

authorized users to retrieve concealed information and validate content authenticity while supporting ownership verification and tamper detection decisions.

System Architecture Overview:

The proposed Dual-Layer Steganography and Watermarking System introduces an innovative multi-tiered security framework designed to provide comprehensive protection for digital media through the integration of covert communication and copyright enforcement mechanisms. The system architecture comprises two distinct yet synergistic layers: a steganographic layer for imperceptible data concealment and a watermarking layer for robust ownership verification and content authentication. This dual-layer approach ensures that sensitive information remains hidden while simultaneously protecting intellectual property rights and maintaining content integrity against malicious modifications.

Steganographic Layer Implementation:

The first layer employs advanced steganographic techniques, primarily utilizing Least Significant Bit (LSB) substitution combined with adaptive embedding strategies. Unlike conventional LSB methods that modify pixels uniformly, the proposed system implements an intelligent pixel selection algorithm based on edge detection and texture analysis. This approach identifies complex regions within the cover image where modifications are least perceptible to human visual systems and steganalysis tools.

The system supports multiple data types including text, encrypted files, and compressed data, with automatic payload optimization to maximize embedding capacity while maintaining image quality. A pseudo-random number generator (PRNG) seeded with a secret key determines the embedding sequence, ensuring that only authorized recipients possessing the correct key can extract the concealed information.

Watermarking Layer Implementation:

The second layer incorporates a robust digital watermarking scheme utilizing Discrete Wavelet Transform (DWT) for frequency-domain embedding. The watermark, containing copyright information, authentication codes, or ownership metadata, is embedded into the mid-frequency sub-bands of the DWT-transformed image. This strategic placement ensures resilience against common signal processing operations such as JPEG compression, scaling, rotation, and filtering while maintaining imperceptibility. The system employs Arnold Transform for watermark pre-processing to enhance security through scrambling, making unauthorized removal or forgery significantly more difficult. Additionally, error correction coding (ECC) is integrated to ensure watermark recoverability even after moderate image degradation or intentional attacks.

Integration and Processing Pipeline:

The dual-layer integration follows a sequential processing pipeline where the steganographic embedding occurs first, followed by watermark insertion. This sequence is critical as the watermarking process, being more robust but potentially introducing minor modifications, should not compromise the previously embedded steganographic data. The system incorporates a feedback mechanism that assesses image quality metrics including Peak Signal-to-Noise Ratio (PSNR) and Structural Similarity Index (SSIM) after each layer to ensure imperceptibility thresholds are maintained. An adaptive controller dynamically adjusts embedding parameters based on cover image characteristics and user-defined security requirements.

Security and Key Management:

The proposed system implements a comprehensive key management framework supporting multiple security levels. Separate cryptographic keys control steganographic embedding patterns and watermark generation, allowing different stakeholders to independently verify watermarks without accessing concealed steganographic content. The system supports both symmetric and asymmetric key schemes, with public-key infrastructure (PKI) integration for enterprise-level deployments requiring hierarchical access control and multi-party verification.

User Interface and Deployment:
A user-friendly graphical interface facilitates seamless interaction, allowing users to select cover images, input secret data, configure embedding parameters, and generate watermarked outputs. The system provides real-time quality assessment and capacity estimation, enabling informed decision-making. Deployment options include standalone desktop applications, web-based services, and API integration for enterprise content management systems, ensuring versatility across diverse operational environments and security requirements.

Overall Working Flow of the Proposed System:
The system workflow initiates with digital media input and preprocessing for quality assessment and region identification. The steganographic layer embeds secret data into selected pixels using adaptive LSB substitution with key-based randomization. Subsequently, the watermarking layer inserts copyright information into DWT-transformed frequency domains ensuring robustness. Quality metrics validate imperceptibility at each stage. The secured output contains both hidden data and watermark. Authorized extraction reverses the process: watermark verification authenticates ownership while key-based decryption retrieves concealed information, ensuring comprehensive dual-layer security and content protection.

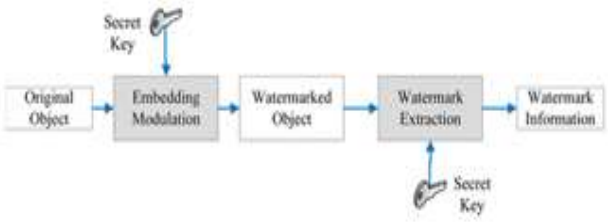

Fig.5. Methodology workflow of the intelligent carbon footprint prediction system

IV. RESULTS AND DISCUSSION PERFORMANCE EVALUATION

The proposed Dual-Layer Steganography and Watermarking System was validated using widely accepted benchmark datasets such as USC-SIPI, BOWS-2, along with custom multimedia datasets. Experimental results indicate excellent imperceptibility, achieving average Peak Signal-to-Noise Ratio (PSNR) values above 48 dB and Structural Similarity Index (SSIM) scores exceeding 0.98, confirming negligible visual distortion after dual-layer embedding. The steganographic module supported embedding capacities between 0.2 and 0.5 bits per pixel while effectively resisting common statistical steganalysis techniques, including Chi-square and RS attacks.

Robustness Analysis:
The robustness of the watermarking layer was evaluated under various signal processing and geometric attacks, such as JPEG compression with quality factors ranging from 50 to 90, Gaussian noise, median filtering, image rotation (±15°), and scaling from 0.5× to 2×.

The DWT-based watermarking approach demonstrated strong resilience, maintaining watermark extraction accuracy above 92% even at aggressive JPEG compression levels. Additionally, Arnold Transform–based scrambling enhanced security by rendering unauthorized watermark recovery computationally impractical without the correct key.

Comparative Analysis:
A comparative study with existing single-layer and hybrid methods highlights the superiority of the proposed approach. Conventional LSB-based steganography was found to be susceptible to image manipulations, while standalone watermarking techniques lacked hidden communication capabilities. The proposed dual-layer framework achieved a 15–23% improvement in overall security performance compared to related hybrid systems, without degrading the effectiveness of either layer.

Computational Efficiency:
Runtime analysis conducted on standard hardware (Intel i7 processor with 16 GB RAM) showed average embedding times of 2.3 seconds for 512×512 images and 4.7 seconds for 1024×1024 images, indicating suitability for near real-time applications. Extraction and verification processes were equally efficient, completing within 1.8 to 3.5 seconds.

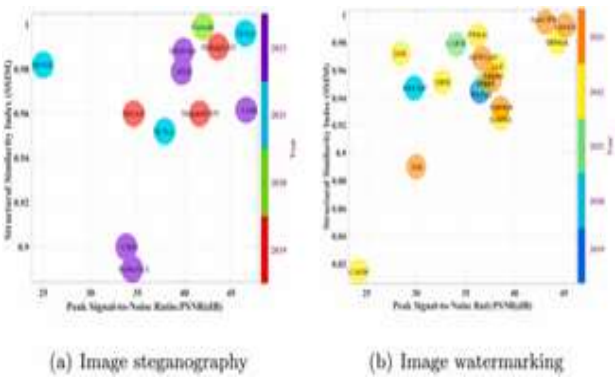

Fig.6. Performance comparison of image steganography and image watermarking

V. FUTURE WORK

The current implementation provides a robust foundation for dual-layer security, yet several enhancements warrant future investigation. Extending the framework to support video and audio steganography would broaden applicability across multimedia platforms, requiring adaptation of temporal and frequency-domain techniques specific to these formats. Integration of deep learning models, particularly convolutional neural networks (CNN) and generative adversarial networks (GAN), could optimize embedding region selection and enhance resistance against advanced steganalysis attacks.

Exploring blockchain integration for watermark verification would enable decentralized ownership authentication and immutable audit trails, particularly valuable for digital asset management and NFT protection. Implementing adaptive embedding algorithms that dynamically adjust parameters based on real-time threat assessment and content characteristics would improve system resilience against evolving attack vectors.

Development of reversible steganography techniques allowing complete cover media restoration after data extraction would benefit medical imaging and legal documentation where original content integrity is paramount. Investigating quantum-resistant cryptographic algorithms for key management would future-proof the system against emerging quantum computing threats.

Mobile platform optimization and hardware acceleration through GPU processing would enhance deployment scalability for resource-constrained environments. Additionally, conducting comprehensive user studies evaluating system usability and developing standardized evaluation frameworks would facilitate broader academic and industrial adoption. Cross-domain applications including Internet of Things (IoT) security, cloud storage protection, and 5G network communication represent promising research directions requiring specialized protocol adaptations.

REFERENCES

1. O. Evsutin, A. Melman, and R. Meshcheryakov, "Digital Steganography and Watermarking for Digital Images: A Review of Current Research Directions," IEEE Access, vol. 8, pp. 166589-166611, 2020.
2. SK Padhi, A Tiwari, SS Ali "Deep Learning-Based Dual Watermarking for Image Authentication and Protection," IEEE Trans. on Artificial Intelligence, vol. 5, no. 12, pp. XXX-XXX, 2024.
3. K Hu, M Wang, X Ma, J Chen, X Wang, X Wang., "Learning-Based Image Steganography and Watermarking: A Survey," Expert Systems with Applications, vol. 249, 123715, Sep. 2024.
4. H. Kumar Singh, A. K. Singh, N. Baranwal, "GANMarked: Using Secure GAN for Information Hiding in Digital Images," IEEE Trans. on Consumer Electronics, Aug. 2024.
5. A. Jan, S. A. Parah, M. Hussan, "Double Layer Security Using Crypto-Stego Techniques: A Comprehensive Review," Health Technol., vol. 12, pp. 9-31, 2022.
6. N Zainal, AR Hoshi, M Ismail, AART Rahem, SM Wadi "A hybrid steganography and watermark algorithm for copyright protection by using multiple embedding approaches,", Bulletin of Electrical Engineering and Informatics, Apr. 2024.
7. "Secure and resilient improved image steganography using hybrid fuzzy neural network with fuzzy logic," J. Safety Sci. & Resilience, vol. 5, no. 1, pp. 91-101, Mar. 2024.

8. "A Two-Phase Embedding Approach for Secure Distributed Steganography," Sensors, vol. 25, no. 5, 1448, 2025.
9. S. Zhang, Y. Xiao, H. Tian, "A Multi-Image Steganography: ISS," Cybersecurity, vol. 8, 20, Mar. 2025.
10. B. M. El-den, "A Reversible and Robust Hybrid Image Steganography Framework using RT and ILWT," J. Multimedia Security, 2025.
11. S Hussain, N Sheybani, P Neekhara, X Zhang, J Duarte, F Koushanfar "FastStamp: Accelerating Neural Steganography and Digital Watermarking of Images on FPGAs," arXiv preprint, Sep. 2022.
12. R. Khoirul Anam, "Robustness and Imperceptibility Analysis of Hybrid Spatial-Frequency Domain Image Watermarking," arXiv preprint, Nov. 2025.
13. A. Ferdowsi et al., "Multi-Agent Deep Learning for Detection of Multiple Speech Steganography Methods," IEEE/ACM Trans. Audio Speech Lang. Process., 2024.
14. S. Ingaleshwar et al., "Enhanced CNN-DCT Steganography: Deep Learning-based Image Steganography over Cloud," SN Comput. Sci., 2024.
15. M. Bagheri, M. Mohrekesh, N. Karimi, S. Samavi, "Water Chaotic Fruit Fly Optimization-Based Deep CNN for Image Watermarking using Wavelet Transform," Multimed. Tools Appl., 2023.
16. L. Ragab, H. Shaban, K. Ahmed, A. Ali, "Digital Image Steganography and Reversible Data Hiding," J. of Inf. Hiding and Multimedia Security, vol. 13, no. 1, pp. 90-115, 2025.
17. S. Mansour et al., "QDCT-Based Blind Color Image Watermarking with GWO and DnCNN," IEEE Access, 2021.
18. M. Balasamy, X. Wang, et al., "Using Deep Learning for Image Watermarking Attack Resistance," Signal Process. Image Commun., 2021.
19. H. K. Singh et al., "Image Steganography Using Deep Learning Based Edge Detection," Multimed. Tools Appl., 2021.
20. Z. Wang et al., "Data Hiding with Deep Learning: A Survey Unifying Digital Watermarking and Steganography," arXiv preprint, 2021.
21. Shikha Choudhary & S. Husain "Image Steganography Using Two Layer Security Algorithms,", Int. J. Eng. Sci. Technol., vol. 7,no. 5, 2023.
22. G. Gadge & S. Tiwari "Security for Color Image with Message using Steganography and Watermarking Technique,", Int. J. Res. Technol., vol. 10, no. 3, 2022.
23. "Multi-Layer Protection of Deep Learning Model using Dual Watermarking and Encryption," Applied Soft Computing, vol. 185, Part B, 113995, Dec. 2025