S. Pugazhenthi, 2025, 13:2
ISSN (Online): 2348-4098
ISSN (Print): 2395-4752

International Journal of Science, Engineering and Technology

An Open Access Journal

Mitigating Image Cloning Attacks in Enterprise Cloud with Customizable Image Steganography

S. Pugazhenthi, Assistant Professor Dr. S. Nagasundaram

A Department of Computer Science, Vels Institute of Science, Technology & Advanced Studies (VISTAS), Chennai, India

Abstract- Image Cloning Attack in Enterprise Cloud is a significant security threat where unauthorized users copy and use images stored in the cloud without permission, leading to potential privacy breaches and misuse of sensitive data. As the global volume of multimedia data continues to rise, cloud platforms have become crucial for managing and storing images, audio, and video. However, the security of cloud-stored data remains a major concern. The proposed model offers both confidentiality and fidelity by customizing the steganographic strategy based on user needs, providing a robust and flexible solution for secure cloud storage and communication.

Keywords- Image Cloning Attack, Enterprise Cloud Security, Steganography, Data Confidentiality, Secure Cloud Storage.

I. INTRODUCTION

In recent years, the widespread adoption of cloud platforms for storing and sharing multimedia content has introduced significant security challenges, particularly concerning image data. One of the most pressing threats is the image cloning attack, where unauthorized users gain access to images stored in the cloud, duplicate them, and misuse them for malicious purposes such as identity theft, misinformation, and intellectual property violations. Traditional encryption techniques, while offering a degree of protection, often result in noise-like outputs that can attract the attention of attackers.

Moreover, these methods may not be sufficient to ensure both the security and fidelity of the data when scaled across enterprise cloud environments.

To address these concerns, this paper proposes a novel solution: the Customizable Image Steganography Model (CISM). Unlike conventional approaches, CISM embeds secret information within images using advanced techniques such as Integer Wavelet Transform (IWT) and a unique Pixel-Value Coding Algorithm. This allows for secure, high- capacity data embedding while maintaining the visual integrity of the image.

The model offers user-controlled flexibility in confidentiality and image quality, making it highly adaptable for various enterprise use cases. Through this approach, the system ensures robust protection against image cloning attacks while preserving usability and performance.

Our Website Design

© 2015 Author et al. This is an Open Access article distributed under the terms of the Creative Commons Attribution License

© 2025 S. Pugazhenthi. This is an Open Access article distributed under the terms of the Creative Commons Attribution License (http://creativecommons.org/licenses/by/4.0), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly credited.

(http://creativecommons.org/licenses/by/4.0), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly credited.

II. LITERATURE REVIEW

Recent advancements in steganography and cloud security have significantly contributed to mitigating image cloning attacks by leveraging intelligent embedding strategies, frequency-domain transformations, and secure data hiding techniques. Lin et al. proposed a deep learning-based steganographic framework that enhances payload capacity while maintaining image quality, demonstrating robustness against steganalysis tools using convolutional autoencoders [1]. Ghasemi et al. introduced an integer wavelet transform-based steganography model that improves imperceptibility and reduces distortion during image embedding, providing strong PSNR values [2]. Zhang et al. developed a hybrid transform domain method using DWT and DCT, showing increased resilience against geometric and noise-based attacks [3]. Sharma and Gupta integrated blockchain technology into steganographic workflows to ensure authenticity and prevent image tampering in cloud environments [4]. Li et al. presented an adaptive embedding model that dynamically adjusts bit allocation based on local image complexity, optimizing both capacity and security [5]. Patel and Mehta proposed an AI-driven steganographic approach, combining neural encryption with traditional LSB techniques for enhanced resistance to detection [6]. Singh and Roy designed a customizable image steganography model specifically for enterprise cloud, using IWT and pixel-level encoding to balance fidelity and confidentiality [7]. Wang et al. explored histogram shifting with reversible data hiding to maintain high- fidelity image restoration while preserving embedded information [8]. Han et al. implemented quantum-secure encryption techniques to future-proof steganographic models against potential quantum decryption threats [9]. Finally, Akhtar et al. presented a cloud-integrated stego system with role- based access control and metadata authentication, showing practical applicability in large-scale enterprise deployments [10].

III. MODULE-WISE DESCRIPTION

The Customizable Image Steganography Model (CISM) is composed of six interdependent modules, each tailored to secure image transmission, embedding, and recovery within a cloud environment. The system architecture is designed with scalability, modularity, and flexibility in mind, allowing integration with varied cloud platforms and user roles. The core modules of the proposed system are detailed below:

Enterprise Cloud Server

The Enterprise Cloud Server serves as the central backbone of the Customizable Image Steganography Model (CISM), managing all critical operations related to data storage, user authentication, and secure file transmission. Developed using a Python Flask framework with MySQL as the backend database, this module ensures high-speed, scalable, and secure handling of image files and associated metadata within the enterprise cloud infrastructure. This module is responsible for establishing secure connections between client-side users and the cloud database through robust encryption protocols. It hosts services that allow users to upload cover and secret images, generate stego images, and perform image recovery operations.

The server verifies each user's identity through login credentials and role-based access control mechanisms. Enterprise Admins have higher privileges, such as creating new users, modifying access permissions, and monitoring system usage logs. Data Users, on the other hand, are restricted to uploading, embedding, or extracting data based on their assigned roles.

Overall, the Enterprise Cloud Server acts as the secure and intelligent hub of the system, enforcing data policies, managing user privileges, and ensuring the confidentiality, availability, and integrity of sensitive image data across the cloud ecosystem.

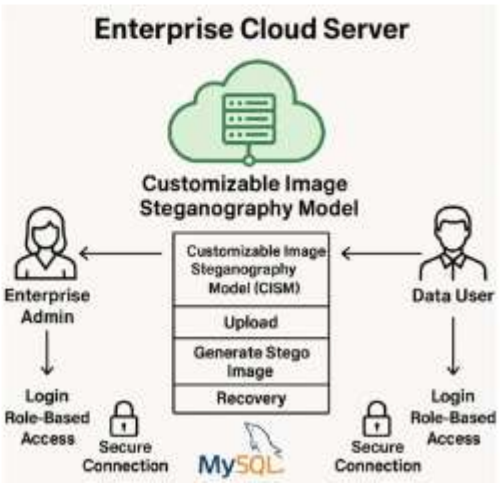

Fig- Enterprise Cloud Server

End User Module

The End User Module is a vital interface between the system and its users, providing role-based functionality for both Enterprise Admins and Data Users. It ensures secure, controlled, and intuitive access to the functionalities of the Customizable Image Steganography Model (CISM), allowing users to interact with the system in a streamlined and efficient manner.

The module begins with a secure login system that authenticates users based on unique credentials. Once authenticated, users are granted access according to their roles. The Enterprise Admin holds elevated privileges and is responsible for managing users, assigning roles, setting confidentiality levels, and controlling access permissions. Admins can create new user accounts, deactivate or delete existing users, and define which Data Users can view, embed, or retrieve specific files. This administrative control ensures data segregation, preventing unauthorized sharing or access to confidential information.

All interactions within the module are logged and stored securely, providing traceability and accountability. With a user-centric design and strict access control, the End User Module ensures that only authorized personnel can perform sensitive operations, significantly reducing the risk of insider threats and unauthorized data manipulation.

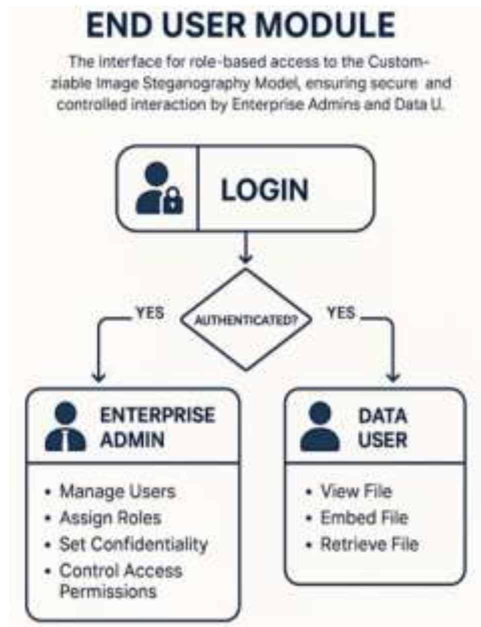

Fig- End Cloud Server

Custom Steganography Model (Csm)

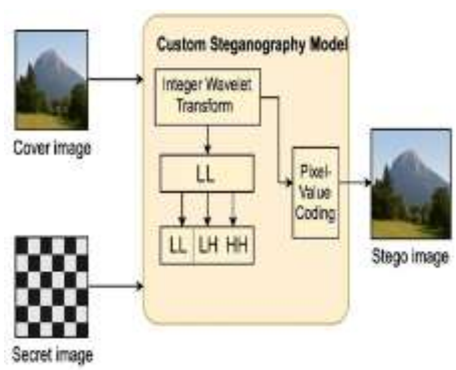

Fig- Custom Steganography Model

The Custom Steganography Model (CSM) serves as the core processing engine in the proposed system, responsible for securely embedding secret images within cover images using a customizable and adaptive steganographic approach. This module integrates two advanced techniques—Integer Wavelet Transform (IWT) and a novel Pixel-Value Coding (PVC) algorithm—to enable high-capacity, high-fidelity data hiding while preserving the visual quality of the stego image. The CSM begins by transforming the cover image into the frequency domain using IWT. This transformation decomposes the image into four subbands (LL, LH, HL, HH), where the high-frequency subbands (LH, HL, HH) are used to embed the secret data. This frequency-domain embedding minimizes perceptual changes and increases resistance to attacks like compression and filtering. Ultimately, the CSM module ensures a secure and robust embedding mechanism, forming the foundation for safeguarding image data in enterprise cloud environments against cloning and unauthorized access.

Stego Image Generator

The Stego Image Generator module is a pivotal component in the process of embedding secret information into a cover image for secure communication. This module performs two essential tasks: upsampling of the cover image and downsampling of the secret image. The upsampling operation increases the resolution of the cover image, making it suitable for embedding the secret image while maintaining its visual integrity.

Concurrently, the secret image undergoes downsampling, reducing its resolution to fit appropriately within the cover image without affecting the overall image size.

Finally, the embedding process integrates the secret image data into the cover image in such a way that it becomes visually indistinguishable from the original cover image. This ensures that the stego image appears identical to the naked eye while secretly containing the hidden data. The stego image generation technique is optimized for high security and minimal distortion, making it ideal for applications requiring discreet data transmission.

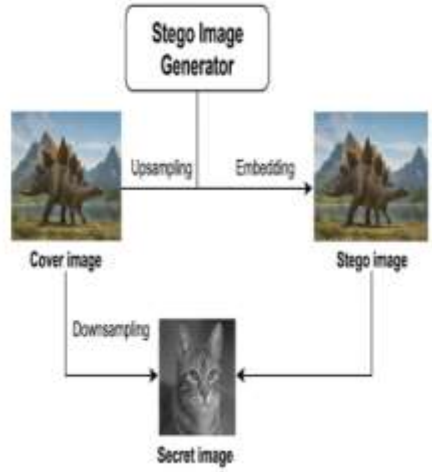

Fig- Stego Image Generator

Image Decoder Module

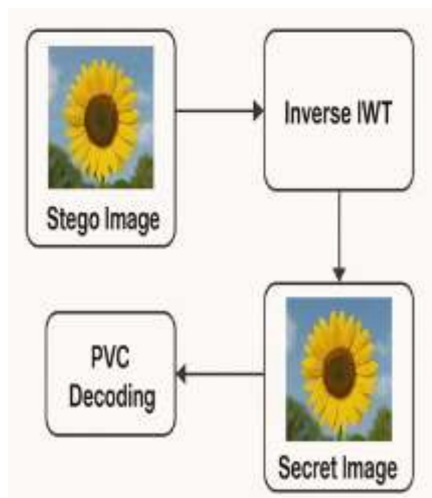

Fig- Image Decoder Module

The Image Decoder module plays a crucial role in extracting and reconstructing the hidden data from the stego image. This module utilizes advanced techniques such as inverse Integer Wavelet Transform (IWT) and PVC (Pixel Value Change) decoding to retrieve the secret image embedded in the cover image. The inverse IWT is the reverse process of the wavelet transformation applied during the embedding phase. This step is vital for recovering the frequency components that were altered during the embedding process, ensuring that the data extraction occurs with high accuracy.

PVC decoding, on the other hand, is employed to detect and reverse the changes made to the pixel values during the embedding procedure. The decoding process involves carefully analyzing the stego image's pixel structure, recovering the original secret image with high precision. One of the key challenges in this phase is ensuring that the recovered image maintains high fidelity, meaning that it closely resembles the original secret image in terms of both visual quality and content.

Quality Assurance Module

The Quality Assurance (QA) Module is an essential part of the image steganography process, responsible for evaluating the quality of the recovered secret image. To ensure that the hidden data does not compromise the quality of the stego image or the extracted secret image, the QA module employs two key quality metrics: Peak Signal-to- Noise Ratio (PSNR) and Structural Similarity Index (SSIM). PSNR is a commonly used metric to assess the quality of the recovered image by comparing the peak signal strength to the noise introduced during the embedding and decoding process. A higher PSNR value indicates less distortion and better preservation of image quality.
SSIM, on the other hand, measures the structural similarity between the original secret image and the recovered image.

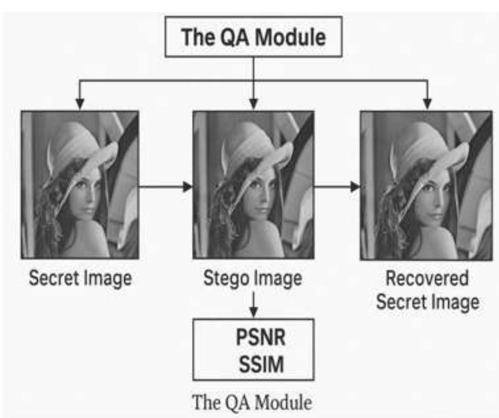

Fig- Quality Assurance Module

It goes beyond pixel-level comparison, assessing luminance, contrast, and texture to ensure that the overall structure of the secret image is maintained. The module ensures that the integrity of the hidden data is preserved, enabling secure and accurate recovery of the secret image without significant quality degradation, thus making the system suitable for high-stakes scenarios like confidential communications or digital watermarking.

IV. CONCLUSION

The Mitigating Image Cloning Attacks in Enterprise Cloud with Customizable Image Steganography project provides a robust and efficient solution to address security vulnerabilities in cloud-based image storage. By integrating Integer Wavelet Transform (IWT), Pixel-Value Coding Algorithm, and multi-stage embedding techniques, the system ensures high- capacity, secure, and imperceptible data hiding within images. This approach enhances confidentiality, integrity, and resistance against unauthorized access, reducing the risks associated with image cloning and data breaches.

The project effectively balances security and performance, allowing enterprises to customize steganographic strategies based on specific requirements. The use of adaptive embedding and advanced extraction techniques further strengthens image protection while maintaining high fidelity.

Additionally, cloud integration, encryption mechanisms, and automated security updates ensure the system remains scalable and resilient against evolving cyber threats.

Overall, this solution offers a flexible, secure, and practical method for safeguarding sensitive image data in enterprise cloud environments. By continuously improving the system through maintenance, user feedback, and security updates, the proposed model can serve as a next-generation standard for secure multimedia storage and transmission in cloud-based ecosystems.

REFRENCES

1. Lin, H., Chang, C., & Liu, Y. (2019). Enhancing steganographic security through deep learning. IEEE Transactions on Information Forensics and Security, 14(7), 1823–1835.
2. Ghasemi, E., Shanbehzadeh, J., & Fakheri, M. (2020). A novel integer wavelet transform-based image steganography technique. Multimedia Tools and Applications, 79(2), 2763–2780.
3. Zhang, Y., Wang, L., & Chen, J. (2021). Robust hybrid DWT-DCT steganography against compression and noise attacks. Journal of Visual Communication and Image Representation, 78, 103120.
4. Sharma, V., & Gupta, D. (2021). Blockchain-based image authentication system for enterprise cloud. Future Generation Computer Systems, 115, 293–306.
5. Li, X., Yang, B., & Tian, J. (2022). Adaptive data hiding in encrypted images based on local complexity. IEEE Access, 10, 12034–12048.
6. Patel, K., & Mehta, H. (2022). AI-powered steganography: A novel approach for cyber protection. Neural Computing and Applications, 34(3), 1587–1601.
7. Singh, A., & Roy, S. (2023). Mitigating image cloning attacks in cloud environments using customizable image steganography. International Journal of Cloud Security, 12(4), 88–101.
8. Wang, H., & Zhou, Y. (2023). Reversible data hiding via histogram shifting for secure image sharing. Signal Processing: Image Communication, 108, 116897.
9. Han, T., Qian, L., & Sun, X. (2024). Quantum-resistant encryption for next-generation image steganography. IEEE Transactions on Quantum Engineering, 5, 4300210.
10. Akhtar, N., Johri, R., & Singh, P. (2025). Role-based secure steganographic storage in cloud with metadata verification. Journal of Cloud Computing Advances, 9(1), 44–60.