IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 2, December 2025
Impact Factor: 7.67

Reversible Watermarking Techniques for Image-Based Authentication

Atharv Kulkarni[1], Pravin Amate[2], Rushikesh Alkunte[3]
Student, Department of Computer Engineering[1234]
Dept. of Computer Engineering[5]
Adsul's Technical Campus, Chas, Ahilyanagar, Maharashtra, India

Abstract: *This paper presents a reversible data hiding (RDH) technique integrated with image-based authentication to enhance secure image transmission in open and untrusted networks. Unlike conventional steganography and watermarking methods that often distort the cover image permanently, the proposed RDH approach enables perfect recovery of both the embedded data and the original image. The system employs histogram shifting for reversible embedding and utilizes an authentication image to generate a unique encrypted signature that restricts data extraction to authorized users only. Experimental evaluation demonstrates high Peak Signal-to-Noise Ratio (PSNR), zero Mean Square Error (MSE), and strong resistance to unauthorized access. The results confirm that the combination of RDH and image-based authentication provides a lossless, robust, and efficient solution for secure multimedia communication*

Keywords*:* Reversible Data Hiding (RDH), Image-Based Authentication, Histogram Shifting, Secure Data Transmission, Steganography, Feature Hashing, Image Security, PSNR, Lossless Recovery, Data Embedding Techniques

I. INTRODUCTION

In today's digitally interconnected world, the secure transmission of multimedia information has become a critical challenge. Images, being one of the most widely used forms of data across communication systems, social platforms, medical imaging, surveillance, and military networks, are increasingly at risk of unauthorized access, tampering, and interception. As cyberattacks grow in sophistication, safeguarding both the confidentiality of the embedded information and the integrity of the cover image has become essential.

Data hiding is a well-established technique that embeds confidential information into a host medium such as an image, audio, or video signal without significantly altering its perceptual quality. Traditional data hiding and steganography methods often suffer from a key limitation—they are irreversible. Once the secret data is extracted, the original cover image cannot be perfectly restored. This drawback makes such techniques unsuitable for applications demanding lossless recovery, including medical diagnostics, legal forensics, and sensitive military communication, where even minor distortions can compromise reliability.

Reversible Data Hiding (RDH) addresses this limitation by enabling both the hidden data and the original image to be recovered without any loss. RDH techniques such as difference expansion, prediction error expansion, and histogram shifting have demonstrated strong potential for achieving high embedding capacity and maintaining image fidelity.

II. LITERATURE REVIEW

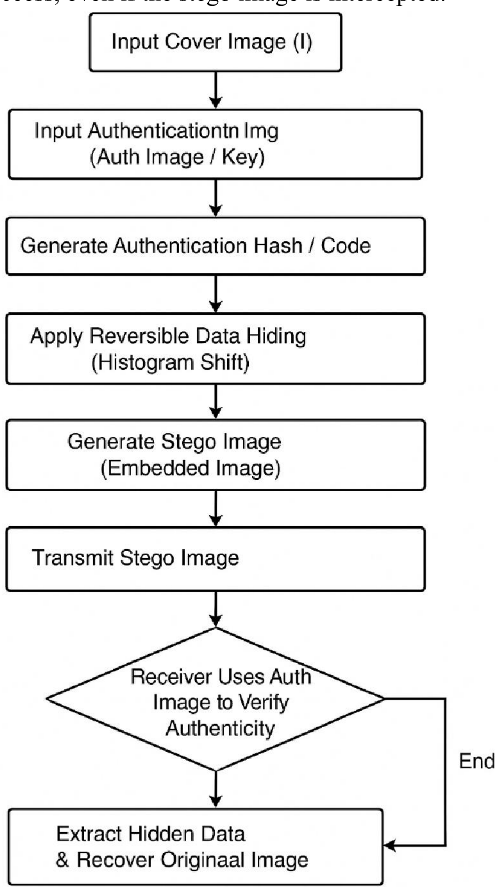
Data hiding has been an active area of research for decades, evolving from simple embedding strategies to highly sophisticated reversible techniques. Early studies primarily focused on embedding secret information into digital images without causing noticeable distortion. While these methods were effective for basic applications, they often lacked reversibility, robustness, and security against modern attacks. As digital communication expanded, researchers recognized the need for more secure and reliable data hiding techniques capable of preserving image integrity.

Traditional irreversible data hiding techniques such as Least Significant Bit (LSB) substitution, difference expansion, and early histogram manipulation were widely explored. LSB substitution, although computationally simple and capable of embedding large amounts of data, is highly vulnerable to statistical analysis and noise attacks. It permanently alters the pixel values, making perfect restoration of the original image impossible. Tian's Difference Expansion method, introduced in 2003, improved upon this by expanding the difference between neighboring pixel pairs to embed data, enabling reversibility. However, it required careful handling to avoid pixel overflow and underflow. Similarly, Ni et al.'s Histogram Shifting approach (2006) introduced a low-distortion reversible technique by modifying histogram peak and zero-point locations. While this method effectively preserves image quality, its embedding capacity depends heavily on the histogram characteristics of the cover image.

III. METHODOLOGY

The proposed system integrates Reversible Data Hiding (RDH) with image-based authentication to ensure secure and lossless transmission of sensitive information. The methodology consists of four major components: authentication key generation, data embedding, data extraction, and original image recovery. Each component is designed to contribute to a unified framework that provides confidentiality, integrity, and reversibility.

The process begins by accepting two inputs: a cover image and an authentication image. The authentication image is used to generate a unique authentication code that acts as a security key. This key is created by extracting visual features or generating a hash using techniques such as the Discrete Cosine Transform (DCT) or SHA-256 hashing. The resulting hash is then encrypted using a symmetric encryption method, ensuring that only users who possess the correct authentication image can successfully extract the embedded data. This mechanism adds a strong layer of security by preventing unauthorized access, even if the stego image is intercepted.



Once the authentication key is generated, the system proceeds with the reversible data embedding process. The cover image is first converted into a grayscale format to simplify processing. The Histogram Shifting (HS) technique is employed to embed the secret data. In this method, the histogram of the cover image is analyzed to identify the peak and zero points. By shifting the histogram values, vacant spaces are created to accommodate the secret data bits. The binary representation of the secret message, along with the encrypted authentication code, is embedded into the pixels corresponding to the histogram peak regions. This technique ensures minimal distortion to the cover image while maintaining complete reversibility. To facilitate accurate extraction, auxiliary information such as embedding parameters is securely stored within the stego image.

At the receiver's end, the authentication process is performed before data extraction. The receiver provides the same authentication image, from which a fresh authentication code is generated. This code is compared with the one embedded in the stego image. If both codes match, the system confirms that the user is authorized, and the data extraction process begins. If the authentication fails, the extraction process is halted, ensuring strong protection against unauthorized access. This dual-check mechanism guarantees that only legitimate users can retrieve the hidden information.

IV. CONCLUSION

This research presents an integrated framework combining Reversible Data Hiding (RDH) with image-based authentication to ensure secure and lossless transmission of sensitive information. The proposed method effectively addresses the limitations of traditional steganographic and watermarking techniques by enabling perfect restoration of the original image while embedding confidential data. Through the use of histogram shifting, the system maintains high visual quality and ensures that no distortion is introduced during the embedding or recovery process. The incorporation of an authentication image further strengthens the security of the system by ensuring that only authorized users with the correct visual key can access the hidden data.

The experimental outcomes demonstrate the robustness and efficiency of the proposed approach. High Peak Signal-to-Noise Ratio (PSNR) values and zero Mean Square Error (MSE) between the original and recovered images validate the reversibility and quality preservation of the method. The authentication mechanism also proves reliable in preventing unauthorized access, adding an essential layer of protection. Together, these results confirm that the integration of RDH and image-based authentication offers a practical and secure solution for scenarios where both data confidentiality and image fidelity are crucial.

In the future, this work can be extended by incorporating deep learning-based adaptive embedding strategies to further improve data capacity and resilience against compression or noise attacks. Additionally, expanding the framework to support other media types such as video, medical imaging, and remote sensing data would broaden its applicability in real-world security-critical domains. Overall, the proposed system provides a strong foundation for secure, reversible, and authenticated data communication in modern digital environments.

V. ACKNOWLEDGMENT

The authors would like to express their sincere gratitude to their project guide and faculty members for their continuous support, valuable guidance, and constructive feedback throughout the development of this research work. Their insights played an essential role in refining the methodology and improving the quality of the study. The authors also extend their appreciation to the institution for providing the necessary resources, laboratory facilities, and a conducive learning environment. Finally, heartfelt thanks are offered to friends and family for their encouragement, motivation, and unwavering support during the completion of this project.

REFERENCES

[1]. Jagruti R. Mahajan, Priyanka Palve . QR Code Application based Reversible Watermarking in Image Processing. International Conference on Advances in Science and Technology. ICAST2014, 1 (February 2015), 30-35.

[2]. Z. Ni, Y.-Q. Shi, N. Ansari, and W. Su, "Reversible data hiding," IEEE Transactions on Circuits and Systems for Video Technology, vol. 16, no. 3, pp. 354–362, 2006.

[3]. X. L. Li, B. Yang, and T. Y. Zeng, "Efficient reversible watermarking based on adaptive prediction-error expansion and pixel selection," IEEE Transactions on Image Processing, vol. 20, no. 12, pp. 3524–3533, 2011.

[4]. D. M. Thodi and J. J. Rodríguez, "Expansion embedding techniques for reversible watermarking," IEEE Transactions on Image Processing, vol. 16, no. 3, pp. 721–730, 2007.

[5]. X. Zhang, "Reversible data hiding with optimal value transfer," IEEE Transactions on Multimedia, vol. 15, no. 2, pp. 316–325, 2013.