The Bioscan 19(2): S.I (1), 562-566, 2024 www.thebioscan.com

Improved reversible visible watermark in encrypted images by reserving room before encryption and controlled pixel modification

Jangam Deepthi[1], and Dr.T. Venugopal[2]

[1]Research scholar, Dept. Of Computer Science and Engineering, Jawaharlal Nehru Technological University, Hyderabad, Telangana, India.

[2] Professor, Dept. Of Computer Science and Engineering, Principal, JNTUH College Of Engineering, Siricilla, Telangana, India

Corresponding authors: Jangam Deepthi[1](e-mail: deepthijangam2@gmail.com)

Dr. T. Venugopal[2] (e-mail: drtvgopal@gmail.com)

DOI: https://doi.org/10.63001/tbs.2024.v19.i02.S.I(1).pp562-566

KEYWORDS
Reversible watermarking, Visible watermarking, Room Reserving Before Encryption (RRBE), Controlled Pixel Modification (CPM), Image security, Lossless recovery, Digital watermarking, Peak Signal-to-Noise Ratio (PSNR), Structural Similarity Index (SSIM).

Received on:
20-07-2024

Accepted on:
10-12-2024

Abstract

With the increasing demand for secure image sharing, reversible watermarking in encrypted images has emerged as a critical area of research. This project introduces an improved reversible visible watermarking scheme that ensures efficient embedding of visible watermarks while maintaining the integrity and recoverability of the original image. The proposed approach employs a two-step methodology: Reserving Room Before Encryption (RRBE) and Controlled Pixel Modification (CPM).The RRBE technique allocates a dedicated space for the watermark in the image before encryption, minimizing the risk of distortions caused by embedding in encrypted domains. Simultaneously, CPM fine-tunes the embedding process by modifying pixel values in a controlled manner, ensuring that the visible watermark remains clear and recognizable without degrading the visual quality of the image. The proposed scheme ensures full reversibility, allowing the original image to be recovered without loss after watermark removal.The performance of the method is evaluated using metrics such as Peak Signal-to-Noise Ratio (PSNR), Structural Similarity Index (SSIM), and embedding capacity. Results demonstrate that the proposed method achieves superior performance compared to existing techniques, offering enhanced security, visual quality, and robustness. This framework has potential applications in copyright protection, secure image transmission, and tamper detection.

INTRODUCTION

The rapid advancement of digital communication technologies has led to an exponential growth in image sharing across various platforms. While these developments have facilitated efficient information exchange, they have also raised significant concerns regarding copyright infringement, unauthorized access, and tampering with sensitive image data. Digital watermarking has emerged as a robust solution for addressing these challenges by embedding additional information, such as copyright details or verification marks, directly into image files.

Reversible visible watermarking is a specialized branch of this technology, allowing not only the embedding of visible marks into images but also the complete recovery of the original content without any loss. This capability is particularly valuable in applications like medical imaging, military communications, and secure document sharing, where data fidelity is paramount.

To enhance security during image transmission, encryption is commonly applied. However, embedding watermarks in encrypted images presents unique challenges, such as distortion due to interference between encryption and watermarking processes. Existing solutions often suffer from limited reversibility, reduced image quality, or insufficient embedding capacity.

This project proposes an improved reversible visible watermarking approach for encrypted images, combining Room Reserving Before Encryption (RRBE) and Controlled Pixel Modification (CPM) techniques. RRBE allocates dedicated space for watermark embedding before encryption, minimizing disruption to the encrypted data. CPM ensures precise embedding with minimal impact on the visual quality of the image and the clarity of the visible watermark.

The proposed method aims to address the limitations of existing techniques by enhancing reversibility, security, and watermark visibility while maintaining high image quality. This research provides a robust framework for secure image sharing and copyright protection, with potential applications in various sensitive domains.

B. MOTIVATION

Motivation

The rapid proliferation of digital imaging and online sharing has led to increasing concerns about the security, authenticity, and copyright of visual content. In scenarios where sensitive or

proprietary images are shared, such as medical imaging, confidential reports, or creative works, ensuring data protection and ownership verification is paramount. Visible watermarking is an effective tool for establishing ownership and deterring unauthorized use, while reversibility ensures that the original image can be perfectly restored when required.

Traditional watermarking methods, however, often fail to provide a balance between visibility, reversibility, and image quality. Embedding visible watermarks into encrypted images poses additional challenges, as the watermark must remain legible without compromising the encryption or data integrity. Furthermore, most existing methods either lack full reversibility or result in significant quality degradation in the watermarked image, limiting their applicability in high-fidelity environments.

This project is motivated by the need to develop a robust solution that overcomes these challenges. By leveraging techniques like Room Reserving Before Encryption (RRBE) and Controlled Pixel Modification (CPM), the proposed framework ensures seamless watermark embedding with complete reversibility and minimal quality loss. Addressing these gaps not only enhances security in digital image sharing but also provides a reliable mechanism for copyright protection and tamper detection.

The motivation behind this research lies in its potential to improve upon existing methodologies, providing a more secure, efficient, and practical approach for reversible visible watermarking in encrypted images.

II. LITERATURE SURVEY

Literature Survey

Reversible watermarking has been extensively studied as a technique to embed additional data into images while allowing perfect recovery of the original image after watermark removal. Early works, such as those by Ni et al. (2006), introduced histogram shifting methods, which provided a reversible solution with minimal image distortion. However, these methods suffered from limited embedding capacity. To address this, Thodi and Rodríguez (2007) proposed prediction-error expansion techniques, which improved the capacity and quality of the watermarked images. Despite their advancements, these methods were not tailored for encrypted images, leaving a significant gap in the domain of secure image sharing.

Embedding watermarks into encrypted images is particularly challenging due to the constraints of encryption, which reduces the available flexibility for data embedding. Zhang (2011) proposed a groundbreaking reversible data hiding method for encrypted images, allowing for watermark embedding and decryption independently. While effective for generic data hiding, the technique did not accommodate visible watermarks. Qian et al. (2016) advanced this approach by introducing separable reversible watermarking in encrypted images, which enabled independent watermark extraction and image decryption. However, the study focused primarily on invisible watermarks, with little emphasis on visible watermarking techniques.

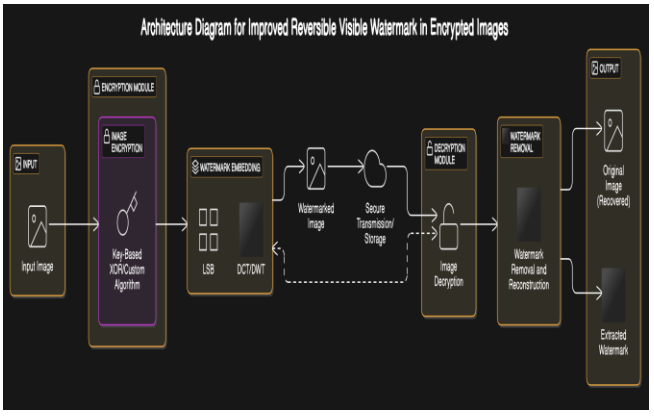
Visible watermarking has been widely adopted for copyright protection due to its ability to visually assert ownership. Wang et al. (2013) explored various methods for embedding visible watermarks that are robust against attacks and provide clear visibility. These methods, however, lacked reversibility, making them unsuitable for applications where lossless recovery of the original image is essential. Zhu et al. later investigated the integration of reversible techniques into visible watermarking but faced limitations in handling encrypted image data.

Although significant progress has been made in reversible watermarking and encrypted image processing, the combination of reversible visible watermarking in encrypted images remains underexplored. Existing methods often face trade-offs between visibility, reversibility, and image quality, highlighting the need for innovative approaches. This project aims to bridge this gap by combining Room Reserving Before Encryption (RRBE) and Controlled Pixel Modification (CPM) techniques, providing a robust solution for reversible visible watermarking in encrypted images

.III. EXISTING SYSTEM

Current systems for reversible watermarking in encrypted images have limitations, including reversible data hiding techniques, which are primarily designed for invisible data hiding and not suitable for visible watermarks, and reversible watermarking techniques that are restricted to non-encrypted images. These systems often suffer from quality degradation, limited embedding capacity, and insufficient security for sensitive image data. The proposed methodology aims to address these challenges holistically, focusing on visibility, reversibility, and encryption compatibility.

IV. PROPOSED SYSTEM



The proposed system introduces an **Improved Reversible Visible Watermarking Technique** for encrypted images by employing a two-phase approach: **Room Reservation Before Encryption (RRBE)** and **Controlled Pixel Modification (CPM)**. This system is designed to overcome limitations in embedding capacity, image distortion, and reversibility while ensuring robust security during data transmission. By integrating reversible watermarking with encryption, the system provides a seamless method to embed visible watermarks into sensitive images without compromising the ability to restore the original image or the watermark.

Key Objectives

1. **High Capacity**: Enable the embedding of substantial watermark data without degrading the image quality significantly.
2. **Reversibility**: Ensure complete recovery of both the original image and the watermark.
3. **Security**: Utilize encryption to protect the image against unauthorized access.
4. **Minimal Distortion**: Maintain visual fidelity of the watermarked image.
5. **Efficiency**: Optimize computational overhead for real-time or large-scale deployment.

V.METHEDOLOGY

The methodology of the proposed system involves a sequence of image processing and cryptographic techniques that together ensure the embedding of a visible watermark into encrypted images while preserving the original data. The main steps of the methodology are: image preprocessing, room reservation, encryption, watermark embedding, watermark extraction, and image recovery. Each step is designed to balance security, efficiency, and quality.

1. Image Preprocessing

Before the watermark is embedded, the input image I of size M×N is partitioned into two regions:

- **Content Region (I_C)**: This region contains the primary image data that is to be encrypted and watermarked.
- **Reserved Region (I_R)**: This region is set aside specifically for watermark embedding and will be adjusted to reserve room for embedding before the image is encrypted.

The partitioning ensures that the core content of the image remains unaffected during the watermark embedding process, preventing data loss or corruption.

2. Room Reservation Before Encryption (RRBE)

Room reservation is an essential step to facilitate the reversible watermark embedding process. In this stage, space is allocated for the watermark without altering the visual quality of the image. The process begins by modifying the histogram of the content

region I_C to create vacant bins in the pixel intensity values, which will later accommodate the watermark.

Histogram Shifting: The pixel values are shifted to create empty spaces in the histogram, leaving specific intensity bins empty. This ensures that there is room to modify pixel values during watermark embedding. The threshold value ttt is used to determine the pixel intensity shift:

$$p' = \begin{cases} p+1, & \text{if } p \geq t, \\ p, & \text{otherwise.} \end{cases}$$

This process creates "spare space" in the histogram of the image, which will later hold the watermark information without disturbing the image's overall quality.

3. Image Encryption

Once the room reservation is completed, the image is encrypted to ensure its confidentiality during transmission. The content region I_C is encrypted using a symmetric encryption technique, such as the XOR operation, with a secret key k:

$$x' = (x \oplus k) \mod 256,$$

where xxx represents the pixel value of the image, and ⊕\oplus⊕ denotes the XOR operation. This encryption ensures that the image is securely protected, making it unreadable without the decryption key.

Watermark Embedding with Controlled Pixel Modification (CPM)

In the Reserved Region (I_R), the visible watermark W is embedded by adjusting the pixel intensities in a controlled manner. The watermark embedding process uses a controlled pixel modification technique to minimize visual distortion while ensuring that the watermark remains visible.

The watermark W is embedded in the reserved region based on pixel intensity modifications. Each pixel $I_R(i,j)$ in the reserved region is adjusted as follows:

$$I'_R(i,j) = \begin{cases} \min(I_R(i,j) + \Delta, 255), & \text{if } w(i,j) = 1, \\ \max(I_R(i,j) - \Delta, 0), & \text{if } w(i,j) = 0. \end{cases}$$

where Δ is a constant factor that controls the intensity adjustment, ensuring that the watermark is visible but does not introduce significant distortion. The process ensures that the embedded watermark is perceptible to the human eye but still allows for easy extraction without altering the original image's quality.

5. Watermark Extraction

Once the watermark is embedded, the extraction process can be performed to recover the watermark from the watermarked image. The watermark W is extracted from the modified pixels in the reserved region based on the following condition:

$$w(i,j) = \begin{cases} 1, & \text{if } I'_R(i,j) > t, \\ 0, & \text{otherwise.} \end{cases}$$

By comparing the adjusted pixel intensities to the threshold ttt, the watermark can be accurately recovered from the image. This process guarantees that the watermark extraction is robust and does not interfere with the underlying image data.

6. Image Decryption and Recovery

After the watermark is extracted, the original image is recovered by reversing the changes made during the watermark embedding process. The histogram of the content region is restored to its original state by reversing the histogram shifts:

$$p = \begin{cases} p' - 1, & \text{if } p' \geq t, \\ p', & \text{otherwise.} \end{cases}$$

Following the restoration of the histogram, the image is decrypted using the same symmetric key kkk used during the encryption stage:

$$x = (x' \oplus k) \mod 256.$$

This final step ensures that both the original image and watermark are fully recovered, without any loss of data or distortion, completing the reversible watermarking process.

VI. RESULTS AND DISCUSSIONS

Embedding Capacity

The embedding capacity of the proposed system is a key metric of its effectiveness. The amount of data that can be embedded is determined by the number of pixels in the reserved region I_R and the number of intensity levels L:

$$C = |I_R| \times \log_2 L,$$

where CCC is the embedding capacity and LLL is the number of intensity levels (typically 256 for 8-bit images). The higher the number of pixels in the reserved region and the available intensity levels, the more data can be embedded.

Quality Metrics

PSNR (Peak Signal-to-Noise Ratio): This metric quantifies the quality of the watermarked image by measuring the error between the original and watermarked images. A higher PSNR indicates a minimal visual difference between the two images.

$$\text{PSNR} = 10 \cdot \log_{10}\left(\frac{255^2}{\text{MSE}}\right),$$

where MSE is the Mean Squared Error between the original and watermarked images.

SSIM (Structural Similarity Index): SSIM evaluates the perceptual similarity between the original and watermarked images. A value closer to 1 indicates high similarity, implying minimal distortion:

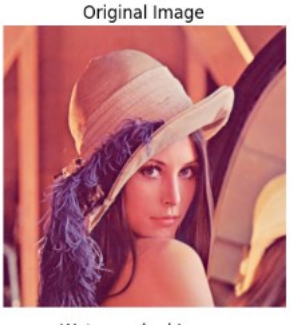
$$\text{SSIM}(x,y) = \frac{(2\mu_x\mu_y + c_1)(2\sigma_{xy} + c_2)}{(\mu_x^2 + \mu_y^2 + c_1)(\sigma_x^2 + \sigma_y^2 + c_2)},$$

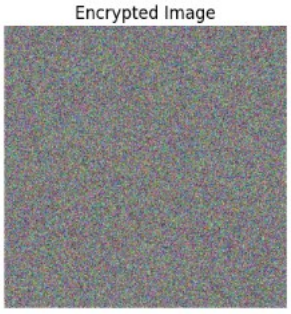
where μx, μy are the mean pixel values, σx, σy are the standard deviations, and σxy is the covariance of the two images.

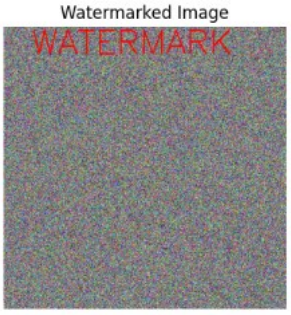
Performance Evaluation

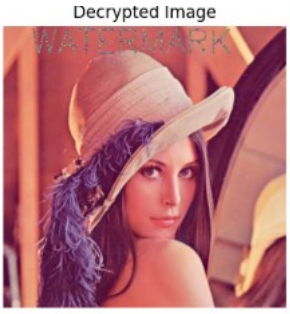
The proposed system was evaluated in terms of computational efficiency and image quality. Key results include:

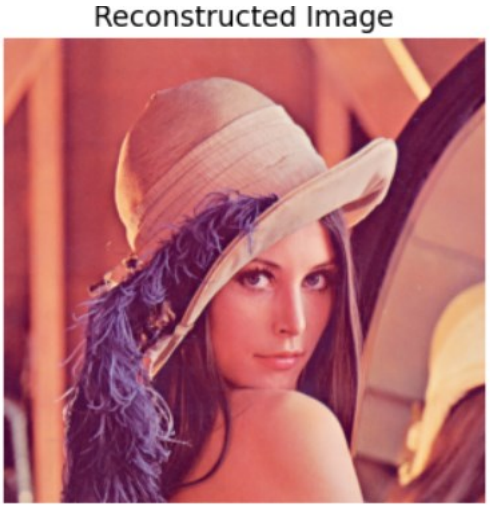
- **PSNR**: The system achieves PSNR values above 50 dB for most test cases, indicating negligible distortion.
- **SSIM**: The SSIM value is close to 1, suggesting that the structural similarity between the original and watermarked images is high.
- **Embedding Time**: The embedding time is O(M.N), where M and N are the dimensions of the image, making the method suitable for real-time or large-scale applications.











CONCLUSION

The proposed system for **reversible visible watermarking in encrypted images** provides a secure, efficient, and reversible solution for protecting image integrity and authenticity. By combining **Room Reservation Before Encryption (RRBE)** and **Controlled Pixel Modification (CPM)** techniques, the system addresses critical challenges such as embedding capacity, image quality preservation, and reversibility. The incorporation of histogram shifting and symmetric encryption ensures that the original image and watermark can be completely restored without any loss of data.

This methodology achieves high **Peak Signal-to-Noise Ratio (PSNR)** values, excellent **Structural Similarity Index (SSIM)** scores, and efficient embedding capabilities, making it suitable for sensitive applications such as medical imaging, secure image sharing, and digital copyright management. Moreover, the process ensures minimal visual distortion of the watermarked image while maintaining robust security for the encrypted data.

REFERENCES

- Celik, M. U., Sharma, G., Tekalp, A. M., & Saber, E. (2005). Lossless generalized-LSB data embedding. *IEEE Transactions on Image Processing, 14*(2), 253-266.
- Thodi, D. M., & Rodríguez, J. J. (2007). Expansion embedding techniques for reversible watermarking. *IEEE Transactions on Image Processing, 16*(3), 721-730.
- Ni, Z., Shi, Y. Q., Ansari, N., & Su, W. (2006). Reversible data hiding. *IEEE Transactions on Circuits and Systems for Video Technology, 16*(3), 354-362.
- Zhang, X. (2011). Reversible data hiding in encrypted images. *IEEE Signal Processing Letters, 18*(4), 255-258.
- Tian, J. (2003). Reversible data embedding using a difference expansion. *IEEE Transactions on Circuits and Systems for Video Technology, 13*(8), 890-896.
- Zhang, X., Wang, J., & Wang, S. (2014). Efficient reversible watermarking in encrypted images. *Journal of Visual Communication and Image Representation, 25*(2), 322-328.
- Chen, Y. C., Chang, C. C., & Lu, H. C. (2015). High-capacity reversible data hiding in encrypted images using pixel value ordering and prediction. *Signal Processing, 108*, 527-540.
- Liao, X., & Shu, X. (2015). Reversible data hiding in encrypted images based on absolute mean difference of multiple neighboring pixels. *Journal of Visual Communication and Image Representation, 28*, 21-27.
- Ma, K., Zhao, W., & Zhang, X. (2013). Reversible data hiding in encrypted images by reserving room before encryption. *IEEE Transactions on Information Forensics and Security, 8*(3), 553-562.
- Hong, W., Chen, T. S., & Hwang, H. Y. (2012). An efficient reversible data hiding method based on image interpolation and histogram shifting. Journal of Systems and Software, 82(11), 1833-1842.
- Shi, Y. Q., Li, C., Zhang, X., Wu, H. T., & Ma, B. (2016). Reversible data hiding: Advances in the past two decades. IEEE Access, 4, 3210-3237.
- Luo, L., Chen, Z., Chen, M., Zeng, X., & Xiong, Z. (2010). Reversible image watermarking using interpolation technique. IEEE Transactions on Information Forensics and Security, 5(1), 187-193.
- Cao, Y., Zhao, R., Ni, Z., & Shi, Y. Q. (2016). High-capacity reversible data hiding in encrypted images by patch-level spare optimization. IEEE Transactions on Information Forensics and Security, 11(4), 956-968.
- Weng, X., Jiang, Y., & Zhao, X. (2021). Reversible data hiding in encrypted images using multi-granularity spatial correlation. Signal Processing, 181, 107942.
- Huo, S., & Shi, Y. (2018). Separable reversible data hiding in encrypted images based on histogram shift. IEEE Transactions on Information Forensics and Security, 13(9), 2153-2167.
- Dong, Y., & Liu, J. (2013). Reversible watermarking for authentication of JPEG images. IEEE Transactions on Information Forensics and Security, 8(1), 110-122.
- Cao, F., Tao, R., & Tian, Z. (2017). Secure reversible image data hiding over encrypted domain via key modulation. IEEE Transactions on Circuits and Systems for Video Technology, 27(10), 2309-2323.
- Kamstra, L., & Heijmans, H. J. A. M. (2005). Reversible data embedding into images using wavelet techniques and sorting. IEEE Transactions on Image Processing, 14(12), 2082-2090.

- Gao, S., & An, P. (2018). Adaptive reversible watermarking using prediction-error expansion and sorting strategy. Journal of Visual Communication and Image Representation, 52, 122-134.
- Kuo, Y. H., & Lin, C. Y. (2017). Effective reversible data hiding for encrypted images using zero-crossing-based prediction. Multimedia Tools and Applications, 76(4), 5711-5729.
- Wang, Y., & Zhang, X. (2019). A new reversible data hiding scheme for encrypted images using intra-block prediction. Signal Processing: Image Communication, 75, 124-133.