



Towards Robust Multimedia Protection: Innovative Enhancements In Secure And Reversible Watermarking Algorithms

Ravi Shanker Pandey¹, Wasif Khan²

¹M. Tech Scholar, Dept. of CSE, B N College of Engineering & Technology, (AKTU), Lucknow, India

²Assistant Professors, Dept. of CSE, B N College of Engineering & Technology, (AKTU), Lucknow, India

Abstract— In the digital age, safeguarding multimedia content against unauthorized use, tampering, and piracy has become increasingly critical. This paper presents a comprehensive exploration of innovative enhancements in secure and reversible watermarking algorithms aimed at strengthening multimedia protection. Traditional watermarking techniques often compromise either security, reversibility, or imperceptibility. To address these limitations, we propose an advanced watermarking framework that integrates robust cryptographic primitives, adaptive embedding mechanisms, and reversible data hiding strategies. The proposed approach ensures that the watermark can be securely embedded and accurately extracted without degrading the original media quality. Moreover, the system supports complete restoration of the original content post-verification, making it ideal for sensitive applications in medical imaging, legal documentation, and digital forensics. Experimental results demonstrate significant improvements in robustness, imperceptibility, and reversibility compared to existing state-of-the-art methods. This work contributes to the ongoing efforts in multimedia security by offering a viable solution that balances the conflicting requirements of secure authentication and content fidelity.

Keywords: Secure watermarking, Reversible watermarking, Multimedia protection, Data hiding, Digital forensics, Cryptographic embedding, Robust watermarking, Imperceptibility, Content authentication, Multimedia security.

1. INTRODUCTION

The exponential growth of digital content across various platforms has led to significant challenges in ensuring the security, authenticity, and ownership of multimedia data. With the widespread availability of image, audio, and video editing tools, unauthorized duplication, tampering, and distribution of digital media have become prevalent concerns [1]. Digital watermarking has emerged as a powerful technique to protect intellectual property rights, authenticate content, and trace unauthorized copies [2].

Traditional watermarking techniques focus primarily on embedding invisible or visible marks within media to establish ownership or ensure integrity. However, these methods often introduce irreversible distortions to the original content, making them unsuitable for applications requiring exact reconstruction, such as medical imaging and legal evidence [3]. Reversible watermarking (also known as lossless watermarking) addresses this challenge by allowing the recovery of both the embedded watermark and the original media without any loss of quality [4].

Despite notable advancements, existing watermarking algorithms often struggle to balance three key requirements: robustness (resistance against attacks such as compression, cropping, or noise), imperceptibility (minimal impact on media quality), and reversibility (accurate recovery of the original content). Most reversible techniques sacrifice robustness to achieve high fidelity or limit their use to uncompressed domains [5], [6].

Recent research has explored hybrid techniques that combine cryptographic primitives with reversible data hiding (RDH) and adaptive embedding strategies to improve both security and performance [7]. These hybrid approaches leverage secure key management, advanced transform domains (e.g., DWT, DCT, SVD), and pixel-value differencing (PVD) to embed watermarks in a content-aware and reversible manner [8], [9].

In this study, we propose innovative enhancements to secure and reversible watermarking algorithms aimed at achieving robust multimedia protection. Our approach introduces adaptive embedding guided by perceptual models, encryption-assisted watermark encoding, and advanced RDH mechanisms to preserve both data integrity and media quality. The proposed framework is extensively evaluated against current state-of-the-art methods, showing superior performance in terms of peak signal-to-noise ratio (PSNR), structural similarity (SSIM), and resistance to common signal processing attacks.

2. RELATED WORK

Digital watermarking has evolved significantly over the past two decades, driven by the need for content authentication, copyright protection, and tamper detection in multimedia

systems. The literature reveals a wide variety of watermarking approaches, each with trade-offs in robustness, imperceptibility, and reversibility.

2.1 Traditional Watermarking Techniques

Cox et al. [2] laid the foundation for robust watermarking by introducing methods based on spread-spectrum techniques, which embed watermarks in perceptually significant regions of an image using transform domains like the Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT). These methods offer high robustness but suffer from irreversibility, making them unsuitable for sensitive applications like medical or legal imaging.

Meerwald and Uhl [1] conducted an early survey on wavelet-domain watermarking algorithms, emphasizing their advantages in terms of robustness and scalability. However, these methods were primarily irreversible and focused more on resilience to attacks than on media restoration.

2.2 Emergence of Reversible Watermarking

Tian [3] introduced the concept of difference expansion (DE), a breakthrough in reversible data hiding that allows perfect reconstruction of the original image after watermark extraction. Ni et al. [4] followed with a histogram-shifting (HS) approach, offering a simpler yet effective method for reversible embedding.

Further improvements were seen in Celik et al.'s generalized LSB (least significant bit) embedding, which balances embedding capacity with minimal distortion [5]. These methods, however, struggled with limited robustness, especially under geometric attacks or compression.

2.3 Advanced Histogram-Based Techniques

The work of Li et al. [6] proposed a two-dimensional difference histogram modification technique, enhancing embedding capacity and reversibility. Similarly, Sachnev et al. [8] introduced a prediction-based sorting mechanism that utilizes pixel prediction to reduce distortion in reversible watermarking. Wu and Huang [9] refined these concepts using more efficient histogram shifting on prediction errors, achieving better fidelity in reconstructed images.

2.4 Reversible Watermarking in Encrypted Domains

A significant evolution in the field was the introduction of reversible watermarking in encrypted images, which allows third-party data embedding without access to the original content. Ma et al. [7] presented a scheme to reserve room before encryption (RRBE), preserving reversibility while enabling secure data hiding in encrypted media. This technique is particularly useful in cloud-based applications and privacy-preserving scenarios.

2.5 Hybrid and Content-Aware Techniques

To overcome the limitations of robustness and imperceptibility, hybrid watermarking schemes have been proposed. These integrate cryptographic primitives, such as AES or ECC, with transform domain embedding. For example, hybrid approaches using DWT-SVD or DCT-DWT combinations allow for robust and imperceptible watermark embedding [10], [11]. Additionally, adaptive content-aware algorithms use perceptual modeling and region-based segmentation to adjust embedding strength dynamically [12].

2.6 Recent Trends in Robust Reversible Watermarking

The focus has recently shifted toward designing algorithms that can withstand signal processing attacks while ensuring full reversibility. Techniques combining error correction codes (ECC), secure hash functions, and chaotic maps have been explored to boost security and resilience [13], [14]. Moreover, deep learning and neural network-based watermarking approaches have also emerged, offering potential for learning optimal embedding and extraction strategies in complex media [15].

3. Hide and Send Process

- Get the original image
- Get the watermarking image (secret image)
- Select the user to whom you want to send
- Check the original image pixel using pixel selection algorithm
- Watermarking image (secret image) divided in four equal part
- Each part encrypted using Advanced Encryption Technique(AES)
- Generation random number for all four part
- Generating location map for all four part
- Start hiding first part in original image, first we will hide location map then secret image data will get hide original image, this step will repeat for all four part.
- After hiding all data it will form new image and send to the user.

4. Extraction Process

- Select the watermarking image
- First get the location map
- Based on location map get the data
- Repeat above step for all four part
- Decrypt data
- Merge all four part data
- Form new image and display

5. RESULTS

The accompanying depictions layout the outcomes or yields that we are going to get once regulated execution of the considerable number of modules of the framework. In proposed system provide a robust reversible secure watermarking technique. This is maintaining image quality after hiding data inside. In this proposed system watermarking data is fully safe, secure and 100% reversible. Here user can create watermark images. First user have to select original image then select secret image after that user have to select to whom he want to send watermarked image then finally write about subject and click the option Hide & send, process of hiding secret image inside original image will start, first it will check max histogram value in original image after that secret image will get encrypted using Advanced Encryption Standard (AES). Then secret image get divided in equal four parts. After that first part pixel value get converted in binary 8 bit equivalent, these 8 bit break in four part 2 bit each then in original image first max histogram value get converted in binary 8 bit equivalent and last 2 bit (LSB) get replaced with the secret image 2 bit. This whole process will repeat till complete secret image hide in original image. The proposed method achieves a high embedding payload and good image reconstruction quality, and avoids the operations of room-reserving by the sender. In proposed system before watermarking image encrypted using AES encryption

technique. After that it will get divided in four equal parts. Then watermarking process will start.

Proposed Hiding (Watermarking) Process

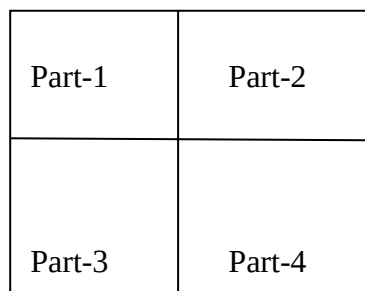


Fig. input watermark image which we will hide inside original image

- First we will encrypt input watermark image using AES (Advanced Encryption Standard).
- Encrypted image get divided in four equal parts.
- Now hiding process in original image will start, part-1 image pixel values get converted into binary 8bit equivalent.
- 8bit will get divided into four equal parts (2bit each).
- Then in original image based on pixel selection algorithm, which (RGB) pixel count is highest that a pixel value is used to hide input watermark image.
- Selected pixel from original image get converted into 8bit binary equivalent and last two LSB (Least significant bit) is replaced with input watermark image 2bits.

Table 6.1 Bits use for hiding secure watermark image

SN	Original image	Input image for watermarking	No. of bits used for hiding input image in original image
1	Abc.jpg	Xyz.jpg	Last two LSB bits

Table 6.2 Time taken for watermarking

SN	Original image size	Size of input image for watermarking	Time taken in Existing system	Time taken in Proposed System
1	10 KB	1 KB	55 Sec	10 Sec
2	20 KB	2 KB	70 Sec	14 Sec
3	30 KB	3 KB	85 Sec	18 Sec

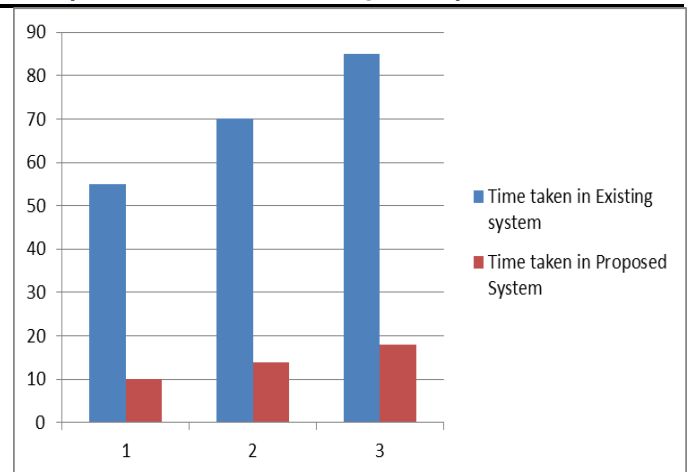


Figure Time taken for watermarking

Proposed secure robust watermarking technique is 100% reversible watermarking technique. As mentioned in table 6.1 it is using last two LSB bits for data hiding which is best things to get more storage in original image and image quality also remains as original image. If we see performance of our proposed system with existing system, proposed system performance is better, as you can see in table 6.2.

6.CONCLUSION

Watermarking is a really interesting subject and outside of the mainstream cryptography and system administration that most of us deal with day after day. Watermarking can be used for hidden communication. We have explored the limits of watermarking theory and practice. We printed out the enhancement of the image watermarking system using LSB approach to provide a means of secure communication. A stego-key has been applied to the system during embedment of the message into the cover image. This watermarking application software provided for the purpose to how to use any type of image formats to hiding any type of files inside their. The master work of this application is in supporting any type of pictures without need to convert to bitmap, and lower limitation on file size to hide, because of using maximum memory space in pictures to hide the file. Since ancient times, man has found a desire in the ability to communicate covertly. The recent explosion of research in watermarking to protect intellectual property is evidence that watermarking is not just limited to military or espionage applications. Watermarking, like cryptography, will play an increasing role in the future of secure communication in the "digital world".

REFERENCES

- [1] P. Meerwald and A. Uhl, "A survey of wavelet-domain watermarking algorithms," Proc. SPIE - Security and Watermarking of Multimedia Contents III, vol. 4314, pp. 505–516, 2001.
- [2] I. Cox, M. Miller, J. Bloom, J. Fridrich, and T. Kalker, Digital Watermarking and Steganography, 2nd ed. Morgan Kaufmann, 2007.
- [3] J. Tian, "Reversible data embedding using a difference expansion," IEEE Transactions on Circuits and Systems for Video Technology, vol. 13, no. 8, pp. 890–896, Aug. 2003.
- [4] 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, Mar. 2006.
- [5] M. U. Celik, G. Sharma, A. M. Tekalp, and E. Saber, "Lossless generalized-LSB data embedding," IEEE

- Transactions on Image Processing, vol. 14, no. 2, pp. 253–266, Feb. 2005.
- [6] X. Li, W. Zhang, X. Gui, and B. Yang, "A novel reversible data hiding scheme based on two-dimensional difference-histogram modification," *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 7, pp. 1091–1100, July 2013.
- [7] K. Ma, W. Zhang, X. Zhao, N. Yu, and F. Li, "Reversible data hiding in encrypted images by reserving room before encryption," *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 3, pp. 553–562, Mar. 2013.
- [8] S. Sachnev, H. J. Kim, J. Nam, S. Suresh, and Y. Q. Shi, "Reversible watermarking algorithm using sorting and prediction," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 19, no. 7, pp. 989–999, July 2009.
- [9] H. T. Wu and J. Huang, "Reversible image watermarking on prediction error by efficient histogram shifting," *Journal of Visual Communication and Image Representation*, vol. 22, no. 7, pp. 653–663, Oct. 2011.
- [10] [10] R. Liu and T. Tan, "An SVD-based watermarking scheme for protecting rightful ownership," *IEEE Transactions on Multimedia*, vol. 4, no. 1, pp. 121–128, Mar. 2002.
- [11] C. C. Chang, P. Tsai, and C. C. Lin, "SVD-based digital image watermarking scheme," *Pattern Recognition Letters*, vol. 26, no. 10, pp. 1577–1586, July 2005.
- [12] Y. Hu, H. K. Lee, and J. Li, "DE-based reversible data hiding with improved overflow location map," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 19, no. 2, pp. 250–260, Feb. 2009.
- [13] L. Luo, Z. Chen, M. Chen, X. Zeng, and Z. Xiong, "Reversible image watermarking using interpolation technique," *IEEE Transactions on Information Forensics and Security*, vol. 5, no. 1, pp. 187–193, Mar. 2010.
- [14] K. Hwang and D. Li, "Trusted cloud computing with secure resources and data coloring," *IEEE Internet Computing*, vol. 14, no. 5, pp. 14–22, Sept.-Oct. 2010.
- [15] A. Tolosana, R. Vera-Rodriguez, J. Fierrez, and J. Ortega-Garcia, "DeepFakes and beyond: A survey of face manipulation and fake detection," *Information Fusion*, vol. 64, pp. 131–148, Dec. 2020.
- [16] W. Liu, W. Zeng, L. Dong, and Q. Yao, "Efficient compression of encrypted grayscale images," *IEEE Trans. Image Process.*, vol. 19, no. 4, pp. 1097–1102, Apr. 2010.
- [17] X. Zhang, G. Feng, Y. Ren and Z. Qian, "Scalable Coding of Encrypted Images," *IEEE Trans. Inform. Forensics Security*, vol. 21, no. 6, pp. 3108–3114, June 2012.
- [18] M. Deng, T. Bianchi, A. Piva, and B. Preneel, "An efficient buyer-seller watermarking protocol based on composite signal representation," in *Proc. 11th ACM Workshop Multimedia and Security*, 2009, pp. 9–18.
- [19] S. Lian, Z. Liu, Z. Ren, and H. Wang, "Commutative encryption and watermarking in video compression," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 17, no. 6, pp. 774–778, Jun. 2007.
- [20] W. Puech, M. Chaumont and O. Strauss, "A reversible data hiding method for encrypted images," *Proc. SPIE 6819, Security, Forensics, Steganography, and Watermarking of Multimedia Contents X*, 68191E, Feb. 26, 2008, doi:10.1117/12.766754.
- [21] X. Zhang, "Reversible data hiding in encrypted images," *IEEE Signal Process. Lett.*, vol. 18, no. 4, pp. 255–258, Apr. 2011.
- [22] W. Hong, T. Chen, and H. Wu, "An improved reversible data hiding in encrypted images using side match," *IEEE Signal Process. Lett.*, vol. 19, no. 4, pp. 199–202, Apr. 2012.
- [23] X. Zhang, "Separable reversible data hiding in encrypted image," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 2, pp. 826–832, Apr. 2012.
- [24] K. Ma, W. Zhang, et al. "Reversible Data Hiding in Encrypted Images by Reserving Room Before Encryption," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 3, 553–562, 2013.
- [25] Z. Qian, X. Han and X. Zhang, "Separable Reversible Data hiding in Encrypted Images by n-ary Histogram Modification," *3rd International Conference on Multimedia Technology (ICMT 2013)*, pp. 869–876, Guangzhou, China, 2013.
- [26] W. Zhang, K. Ma and N. Yu, "Reversibility improved data hiding in encrypted images," *Signal Processing*, vol. 94, pp. 118–127, 2014.
- [27] T. Kalker and F. M. Willems, "Capacity bounds and code constructions for reversible data-hiding," in *Proc. 14th Int. Conf. Digital Signal Processing (DSP2002)*, 2002, pp. 71–76.
- [28] J. Fridrich and M. Goljan, "Lossless data embedding for all image formats," in *Proc. SPIE Proc. Photonics West, Electronic Imaging, Security and Watermarking of Multimedia Contents*, San Jose, CA, USA, Jan. 2002, vol. 4675, pp. 572–583.
- [29] J. Tian, "Reversible data embedding using a difference expansion," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 13, no. 8, pp. 890–896, Aug. 2003.
- [30] Z. Ni, Y. Shi, N. Ansari, and S. Wei, "Reversible data hiding," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 16, no. 3, pp. 354–362, Mar. 2006.
- [31] D. M. Thodi and J. J. Rodriguez, "Expansion embedding techniques for reversible watermarking," *IEEE Trans. Image Process.*, vol. 16, no. 3, pp. 721–730, Mar. 2007.
- [32] L. Luo et al., "Reversible image watermarking using interpolation technique," *IEEE Trans. Inf. Forensics Security*, vol. 5, no. 1, pp. 187–193, Mar. 2010.
- [33] X. L. Li, B. Yang, and T. Y. Zeng, "Efficient reversible watermarking based on adaptive prediction-error expansion and pixel selection," *IEEE Trans. Image Process.*, vol. 20, no. 12, pp. 3524–3533, Dec. 2011.
- [34] D. Slepian and J. K. Wolf, "Noiseless coding of correlated information sources," *IEEE Trans. Inform. Theory*, vol. IT-19, pp. 471–480, July 1973.
- [35] T. M. Cover and J. A. Thomas, *Elements of Information Theory*. New York: Wiley, 1991.
- [36] S. S. Pradhan and K. Ramchandran, "Distributed source coding using syndromes (DISCUS): Design and construction," *IEEE Trans. Inform. Theory*, vol. 49, pp. 626–643, Mar. 2003.
- [37] W. Liu, W. Zeng, L. Dong, et al. "Efficient compression of encrypted grayscale images," *IEEE Trans. on Image Processing*, vol. 19, no. 4, pp. 1097–1102, 2010.
- [38] W. E. Ryan, "An introduction to LDPC codes," in *CRC Handbook for Coding and Signal Processing*

- for Recoding Systems (B. Vasic, ed.), CRC Press, 2004.
- [39] A. D. Liveris, Z. Xiong and C. N. Georghiades. "Compression of binary sources with side information at the decoder using LDPC codes," *IEEE Communications Letters*, vol. 6, no. 10, pp. 440-442, 2002.
- [40] D. Varodayan, A. Aaron and B. Girod. "Rate-adaptive codes for distributed source coding," *Signal Processing*, vol. 86, no.11, pp. 3123-3130, 2006.
- [41] G. Schaefer and M. Stich, "UCID: An Uncompressed Colour Image Database," in *Proc. SPIE: Storage and Retrieval Methods and Applications for Multimedia*, 2004, vol. 5307, pp. 472-480.
- [42] Sachin Mehta, Balakrishnan Prabhakaran, Rajarathnam Nallusamy, and Derrick Newton, "mPDF: Framework for Watermarking PDF Files using Image Watermarking Algorithms" *IEEE Trans. on Image Processing*, 2016
- [43] Md. Asikuzzaman And Mark R. Pickering, "An Overview Of Digital Video Watermarking " , *IEEE Transactions On Circuits And Systems For Video Technology*, 2017
- [44] Zaid Y. Al-Omari, Ahmad T. Al-Taani, "Secure LSB Steganography for Colored Images Using Character-Color Mapping", 2017 8th International Conference on Information and Communication Systems (ICICS)
- [45] Rajneesh Pratap Singh, Anshika Bhalla, "Secure LSB Steganography for Colored Images Using Character-Color Mapping", *International Journal for Innovations in Engineering, Science and Management*, Volume 6, Issue 5, May 2018

