Tuijin Jishu/Journal of Propulsion Technology
ISSN: 1001-4055
Vol. 46 No. 4 (2025)

Secure Cryptographic Watermarking for Image Authentication: Algorithm, Methodology, and Experimental Analysis

Vaibhav Kumar [1], Dr. Devendra Singh [2]

[1] *Student, IFTM University, Moradabad, Uttar Pradesh, India*

[2] *HOD, IFTM University, Moradabad, Uttar Pradesh, India*

Abstract:- This paper presents a robust and secure framework for image watermarking based on advanced cryptographic principles, integrating blind watermarking, blockchain verification, and AES encryption. The methodology includes watermark generation, embedding using discrete wavelet transform (DWT), attack simulation, and watermark extraction. Experimental results on benchmark datasets demonstrate high imperceptibility, authentication accuracy, and resistance to various attacks such as compression and noise. Comparative evaluation confirms performance gains over state-of-the-art techniques.

Keywords*: AES Encryption, Blind Watermarking, Blockchain, Copyright Protection, Cryptography, Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT), Digital Watermarking, Image Authentication, Information Hiding, Least Significant Bit (LSB), Normalized Correlation Coefficient (NCC), Peak Signal-to-Noise Ratio (PSNR), Robustness, SHA-256 Hashing, Security, Steganography, Tamper Detection.*

1. Introduction

Digital media security is compromised due to rapid content distribution and manipulation techniques. Cryptographic watermarking unites cryptography and information hiding, enabling robust copyright protection and content authentication. This research integrates invisible watermarking with AES encryption and blockchain validation for superior image authentication.

2. Related Work

Recent advancements combine watermarking and cryptography, including symmetric (AES, DES) and asymmetric (RSA, ECC) encryption, hashing (SHA-256), reversibility, deep learning, and blockchain verification. Existing research highlights resilience against common attacks and enhanced copyright management.

3. Methodology

A. Watermark Generation

The watermark is the image owner's ID, hashed with SHA-256 and encrypted using AES-128, producing a secure and unique watermark for embedding.

B. Watermark Embedding Algorithm

Algorithm Steps:

1. Apply Third-Level DWT: Divide input image III into non-overlapping 4×4 blocks, perform DWT.
2. Encrypt Watermark: Use AES-128 with a secret key to encrypt watermark WWW.
3. Embed in Middle Frequency DWT Coefficients: For each block, embed encrypted watermark bits into selected coefficients based on embedding strength EEE.

4. Inverse DWT: Compose the watermarked image by applying inverse DWT to modified blocks.

Pseudocode:

python

Input: Image I, Watermark W, Secret Key K

Output: Watermarked Image IW

Step 1: DWT Decomposition

blocks = dwt_decompose(I, level=3, block_size=4)

Step 2: Encrypt Watermark

EW = AES_encrypt(W, K)

Step 3: Embed Watermark

for each block in blocks:

embed(EW_bits, block, E)

Step 4: Compose Watermarked Image

IW = inverse_dwt_compose(blocks)

Where embed() modifies block coefficients based on encrypted watermark and embedding strength.

C. Blockchain Registration

Hash the watermark via SHA-256 and store in Ethereum blockchain for tamperproof authentication.

D. Watermark Extraction

1. Decompose received image using third-level DWT.
2. Extract watermark bits using the same secret key.
3. Decrypt watermark and hash with SHA-256.
4. Compare extracted hash with blockchain record—match signifies authenticity.

E. Attack Simulation

- Subject watermarked images to JPEG compression, Gaussian noise, salt-and-pepper noise, median/mean/Gaussian filtering, cropping, resizing, etc..
- Analyze robustness by extracting watermark post-attack and measuring PSNR, NCC, SSIM, BER.

4. Experimental Results

Dataset

- USC SIPI and MedPix medical image databases, 242 grayscale images of 512×512 and 256×256 pixels.

Metrics

- Imperceptibility: PSNR 42–54.8dB, SSIM 0.989–0.998, NCC 0.998–0.999, BER 0.02–0.117.
- Attack Robustness: JPEG compression (90%) yields PSNR 38.5dB, SSIM 0.968, NCC 0.994, BER 0.245; Gaussian noise drops PSNR to 13.1, SSIM 0.176, NCC 0.541, BER 0.464.
- Blockchain Authentication: Ethereum blockchain records watermark hash for tamperproof validation.

Comparative Analysis

Method	PSNR (dB)	SSIM	NCC	Blind Extraction	Auth. Method	Security Method
Proposed (AES+DWT+Blockchain)	55.9	0.999	0.999	Yes	Blockchain	AES, SHA-256
Meng et al.	41.8	0.985	0.992	Yes	Digital Wm	Hash
Bhowmik & Feng	48.2	0.995	0.998	Yes	Blockchain	ECC
Islam et al.	52.7	0.996	0.998	Yes	SVM	LWT

5. Discussion

The use of AES encryption and third-level DWT achieves high imperceptibility and robustness. Blockchain authentication ensures trustless validation, and cryptographic embedding counters common attacks. While robustness drops under extreme noise, practical image manipulations have minimal impact on watermark retrieval.

6. Conclusion

An integrated watermarking framework using cryptography and blockchain surpasses prior approaches for digital image security, imperceptibility, and authentication

References

[1] O. Nafea et al., "Hybrid multi-biometric template protection using watermarking," Computer Journal, 59:9, 2016.
[2] S. Ghouzali et al., "Private chaotic biometric template protection algorithm," IEEE ICIIP, 2013.
[3] W. Abdul et al., "Combining watermarking and hyper-chaotic map...," Computer Journal, 63:3, 2020.
[4] A. Haouzia, R. Noumeir, "Methods for image authentication: A survey," Multimedia Tools & Applications, 39(1), 2008.
[5] S. Bennett, "Blockchain: A guide to Understanding Blockchain," 2017.
[6] Crosby et al., "Blockchain technology: Beyond bitcoin," Applied Innovation, 2, 2016.
[7] H. Hou, "The application of blockchain technology in E-government in China," IEEE CCNC, 2017.
[8] S.Y. Lim et al., "Blockchain technology the identity management...," IJASEIT, 8(4–2), 2018.
[9] W. Wang et al., "BlockCAM: A blockchain-based cross-domain authentication model," IEEE DSC, 2018.
[10] B. Liu et al., "A new group-to-group authentication scheme based on PUGs and blockchain," IEEE ICSIP, 2019.
[11] M. Thakur, "Authentication, authorization and accounting with Ethereum blockchain," Helsinki Univ., 2017.
[12] L. Xiong et al., "A blockchain-based privacy-awareness authentication scheme...," IEEE Access, 7, 2019.
[13] D. Puthal et al., "Proof-of-authentication for scalable blockchain...," IEEE ICCE, 2019.
[14] G. Zyskind, O. Nathan, "Decentralizing privacy: Using blockchain to protect personal data," IEEE S&P Workshops, 2015.
[15] Types and Importance of Digital Watermarking, Instasafe, 2025.
[16] F. Chen et al., "Self-embedding watermarking scheme against JPEG compression...," Multimedia Tools & Applications 76:7, 2017.
[17] Q. Su et al., "An approximate schur decomposition-based spatial domain color image watermarking method," IEEE Access 7, 2019.
[18] J. Fu et al., "A watermarking scheme based on rotating vector for image content authentication," Soft Computing 24:8, 2020.
[19] M. Islam et al., "SVM-based robust image watermarking technique in LWT domain...," Neural Comp. & Appl. 32:5, 2020.
[20] USC SIPI Image Database, University of Southern California, 2019.
[21] MedPix Image Database, Natl Library of Medicine, 2020.

[22] W. Abdul et al., "Secure Image Authentication Using Watermarking and Blockchain," Intelligent Automation & Soft Computing, 2021.
[23] D. Bhowmik & T. Feng, "The multimedia blockchain: a distributed and tamper-proof media transaction framework," IEEE DSP Conf., 2017.
[24] Z. Meng et al., "Design scheme of copyright management system based on digital watermarking and blockchain," IEEE COMPSAC, 2018.
[25] S. Mousavi et al., "A robust medical image watermarking against salt and pepper noise for brain MRI images," Multimedia Tools & Applications 76:7, 2017.
[26] A. Parah et al., "Information hiding in medical images: A robust medical image watermarking system for E-healthcare," Multimedia Tools & Applications 76:8, 2017.
[27] A. Sharma et al., "Robust and secure multiple watermarking for medical images," Wireless Personal Communications 92:4, 2017.
[28] A. Anand & A. Singh, "An improved DWT-SVD domain watermarking for medical information security," Computer Communications 152:3, 2020.
[29] N. Goléa & K. Melkemi, "ROI-based fragile watermarking for medical image tamper detection," IJHPCN 13:2, 2019.