

A Lightweight Dual-Layer Framework for Image Protection Using DWT-DCT Watermarking and Lossless Chained XOR Secret Sharing

Aaradhna Mishra¹ and M. S. Gupta²

¹Department of Mathematics, Govt. N.P.G. College of Science, Raipur, (C.G.), India
(aaradhanamishra1994@gmail.com)

²Department of Mathematics, Govt. N.P.G. College of Science, Raipur, (C.G.), India
(drmsgupta1965@gmail.com)

Abstract- Ensuring digital image security over public networks requires both content privacy during transmission and verifiable ownership after recovery. Standard watermarking proves ownership but leaves image content exposed, while secret sharing conceals the visual content but cannot track ownership once shares are merged. To resolve both limitations, this paper presents a practical dual-layer security framework. First, an imperceptible watermark is embedded into the host image using a hybrid Discrete Wavelet Transform (DWT) and Discrete Cosine Transform (DCT) approach. Second, the watermarked image is split into uninformative shares using a lightweight chained Exclusive-OR (XOR) secret sharing scheme. Experimental results demonstrate that the watermarked image maintains high perceptual fidelity with minimal distortion and effectively survives common signal processing attacks. The generated shares exhibit noise-like random properties with zero-pixel expansion, and combining all shares achieves exact lossless reconstruction with zero error in low computational time. Consequently, the framework provides a robust and efficient solution for secure multimedia distribution.

Keywords: Digital Image Watermarking, Discrete Wavelet Transform (DWT), Discrete Cosine Transform (DCT), Visual Secret Sharing, Chained XOR Operations, Lossless Reconstruction.

1. INTRODUCTION

Sharing digital images across open networks and cloud storage platforms creates serious security risks, primarily unauthorized access and copyright theft [1]. To secure digital images, researchers commonly rely on two distinct mechanisms: digital image watermarking and visual secret sharing (VSS) [2].

Digital watermarking hides copyright marks (such as text strings or identification codes) inside a cover image without causing noticeable visual degradation [3]. While spatial-domain methods like Least Significant Bit (LSB) substitution are simple, they are easily destroyed by routine operations such as compression, filtering, and noise addition [4]. In contrast, transform-domain methods combining Discrete Wavelet Transform (DWT) and Discrete Cosine Transform (DCT) offer significantly higher robustness [5], [6]. DWT separates the image into multi-resolution frequency sub-bands, while DCT concentrates the dominant perceptual energy into key coefficients, allowing the embedded watermark to survive aggressive channel attacks [5], [6]. However, watermarking only proves ownership; it does not conceal the visual content itself. If an image is intercepted during transmission, an adversary can still view and exploit it directly [2].

To keep image content confidential during transit, Visual Secret Sharing (VSS) splits a secret image into multiple noise-like

shares [7]. Early visual cryptography schemes suffered from significant pixel expansion and severe contrast loss [7]. To resolve these drawbacks, Boolean-based secret sharing schemes using bitwise Exclusive-OR (XOR) operations were introduced by Wang et al. [8] and later extended to chained XOR architectures by Munir and Harlili [9], achieving zero-pixel expansion and exact reconstruction. However, standalone secret sharing has a critical limitation: once the shares are collected and merged at the destination, the recovered image retains no ownership tracking trail [10]. If an authorized recipient leaks or redistributes the recovered file, the original owner has no technical means to prove copyright.

This creates a clear gap: watermarking provides post-recovery ownership proof but lacks privacy during transfer, while secret sharing guarantees confidentiality during transfer but offers zero ownership tracking after recovery.

To address both challenges simultaneously, this paper presents a practical dual-layer framework combining DWT-DCT watermarking with a chained XOR secret sharing scheme. The primary contributions of this work are:

- **Dual-Layer Protection:** Embedding an imperceptible copyright watermark using DWT-DCT before splitting the image into chained XOR shares, securing both transmission privacy and post-recovery ownership.
- **Zero Pixel Expansion & Exact Recovery:** Generating shares that match the dimensions of the original image exactly, while guaranteeing exact bit-level reconstruction with zero-pixel error upon merging all shares.
- **High Fidelity & Attack Robustness:** Preserving high visual quality and structural similarity in the watermarked asset while keeping the watermark reliably extractable under common distortions including JPEG compression, noise addition, and cropping.
- **Fast Execution:** Utilizing hardware-friendly bitwise XOR operations so that share creation and image recovery execute with minimal processing delay, making the system suitable for real-time applications.

2. RELATED WORK

Digital image security focuses on two main areas: robust copyright verification and confidential transmission. Recent studies demonstrate that relying on only one mechanism leaves critical vulnerabilities during open-network distribution.

In transform-domain watermarking, combining the Discrete Wavelet Transform (DWT) with the Discrete Cosine Transform (DCT) remains the standard for balancing imperceptibility and

robustness [5], [6]. To enhance watermark resilience, Mohammed et al. [11] demonstrated that applying a hybrid DCT–DWT decomposition to color images achieves high perceptual quality while maintaining strong robustness against filtering, noise addition, and compression attacks. Complementing this, Kanwal et al. [12] showed that combining DWT and DCT frequency bands provides an effective balance between imperceptibility and resilience against common signal processing distortions. In parallel wavelet-based explorations, Gen et al. [13] utilized discrete wavelet transform (DWT) decomposition to verify image integrity and preserve copyright data, while Al-Obaidi et al. [14] focused on high-capacity blind watermarking across RGB color bands in the wavelet domain. However, relying strictly on single-transform representations often restricts multi-attack resilience. Addressing this limitation, Ooi et al. [15] integrated DWT with DCT and singular value decomposition (DWT-DCT-SVD) alongside randomized embedding to substantially improve watermarking security and geometric resilience. Despite these advantages, watermarking does not conceal image content; the asset remains completely exposed to unauthorized viewing during transit and cloud storage [2].

To protect visual privacy, Visual Cryptography (VC) and Secret Image Sharing (SIS) divide an image into unreadable shares. Following the Boolean foundations by Wang et al. [8] and chained XOR extensions by Munir [9], recent implementations focus heavily on XOR-based visual cryptography to eliminate pixel expansion. Specifically, Wu et al. [16] demonstrated that Boolean XOR-based secret sharing eliminates pixel expansion while ensuring high recovery quality. In a comprehensive survey, Saha et al. [17] confirmed that Boolean operation-based (XOR) secret sharing schemes significantly reduce computational overhead and outperform traditional polynomial-based models in processing speed. Furthermore, Nujumudeen et al. [18] verified that lightweight XOR operations using random shares achieve secure, real-time color image sharing with exact lossless recovery. However, standalone secret sharing has a critical limitation: once all shares are collected and merged, all security tracking ends, leaving owners with no mechanism to prove copyright if an authorized recipient leaks the recovered asset [10].

Although both domains have advanced independently, a clear research gap remains at their intersection. Standalone watermarking leaves visual content exposed during transmission, while standalone secret sharing offers no way to verify ownership once the image is reconstructed. Moreover, existing schemes that attempt to combine both approaches often rely on complex mathematical operations, causing significant computational delays and degradation of image quality. Therefore, a lightweight framework that simultaneously protects transmission privacy through fast XOR sharing, ensures ownership verification via robust DWT–DCT watermarking, and reconstructs the image with exact accuracy without heavy computational cost is still missing in the literature.

3. PRELIMINARIES

This section presents the fundamental concepts required for understanding the proposed framework.

3.1. Discrete Wavelet Transform (DWT)

The Discrete Wavelet Transform (DWT) is a multi-resolution signal analysis technique that decomposes an image into

different frequency sub-bands, LL, LH, HL and HH [19]. The LL sub-band represents the approximation component, while the LH, HL, and HH sub-bands represent the horizontal, vertical, and diagonal detail components, respectively. a one-level 2D DWT decomposition is represented as:

$$I(x, y) \rightarrow \{LL, LH, HL, HH\} \quad (1)$$

Where $I(x, y)$ is the input image. DWT provides good spatial-frequency localization and is widely used in robust watermarking systems due to its resistance to compression and noise attacks [19].

3.2. Discrete Cosine Transform (DCT)

The Discrete Cosine Transform (DCT) converts spatial domain image data into frequency domain representation [20]. It has strong energy compaction properties, where most of the signal energy is concentrated in the low-frequency coefficients, making it suitable for watermark embedding.

The 2D DCT is defined as:

$$C(u, v) = \alpha(u)\alpha(v) \sum_{x=0}^{N-1} \sum_{y=0}^{N-1} I(x, y) \cos \left[\frac{(2x+1)u\pi}{2N} \right] \cos \left[\frac{(2y+1)v\pi}{2N} \right] \quad (2)$$

Where $I(x, y)$ = pixel intensity at position (x, y) , $C(u, v)$ = DCT coefficient, N = block size and $u, v = 0, 1, 2, \dots, N - 1$. The normalization factor is:

$$\alpha(k) = \begin{cases} \sqrt{\frac{1}{N}}, & k = 0 \\ \sqrt{\frac{2}{N}}, & k > 0 \end{cases} \quad (3)$$

DCT is widely used in image and video compression standards such as JPEG and MPEG due to its efficiency and robustness [20].

3.3. XOR-Based Secret Sharing

Secret sharing is a cryptographic technique in which a secret is divided into multiple shares, and reconstruction is possible only when all shares are combined [21].

In XOR-based secret sharing, random shares are generated using XOR operations. For a secret image I , the two shares are generated as:

$$S_2 = I \oplus S_1 \quad (4)$$

Where S_1 is a randomly generated 1st share and S_2 is the 2nd share, having the same dimensions as the secret image I . Reconstruction is performed as:

$$I = S_1 \oplus S_2 \quad (5)$$

For multiple shares:

$$I = S_1 \oplus S_2 \oplus S_3 \oplus \dots \oplus S_n \quad (6)$$

Each individual share does not reveal any meaningful information about the original data, ensuring confidentiality during transmission [22].

4. PROPOSED METHODOLOGY

The proposed framework integrates transform-domain watermarking with Boolean visual secret sharing to secure both transmission privacy and post-recovery provenance. The architecture comprises four sequential phases: watermark

embedding, chained XOR share generation, lossless share reconstruction and watermark extraction for copyright verification or secret message recovery. For multi-channel images (e.g., RGB), the spatial and Boolean operations are applied channel-wise without loss of generality.

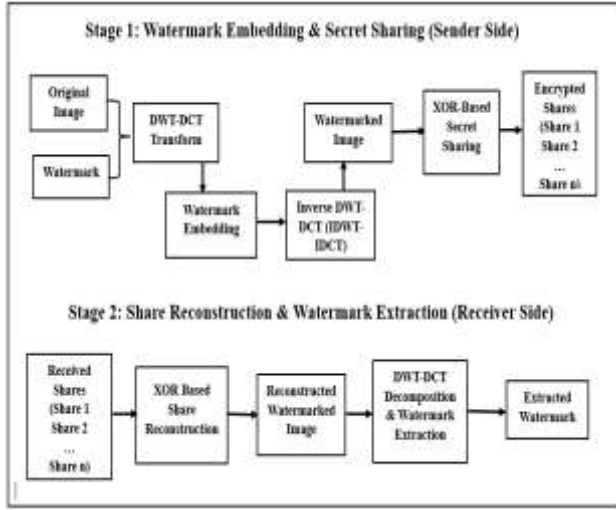


Fig. 1. Block diagram of the proposed watermarking and secret sharing framework

The complete architectural pipeline of the proposed scheme is illustrated in Fig. 1. The framework operates in two distinct stages: (1) Watermark embedding and confidential share generation at the sender side, and (2) Lossless share reconstruction and watermark extraction at the receiver side. The detailed mathematical formulation for each stage is described in the following subsections.

4.1. Watermark Embedding

Let the host image be I of size $M \times N$ and the watermark be a binary sequence $W \in \{0, 1\}^L$.

4.1.1. Color Space Selection:

For color imagery, convert I to the YCbCr color space and select the luminance (Y) channel for watermark insertion, as human visual perception is less sensitive to small changes in luminance. For grayscale images, I is processed directly.

4.1.2. Wavelet Decomposition:

Apply single-level 2D Haar DWT to decompose the target matrix into four frequency sub-bands:

$$[LL_1, LH_1, HL_1, HH_1] = \text{DWT}(I) \quad (7)$$

The approximation sub-band LL_1 contains the structural energy of the image, offering the highest resilience against signal distortions.

4.1.3. Block DCT Transformation:

Divide LL_1 into non-overlapping blocks of size 8×8 . Apply 2D-DCT on each block k ($1 \leq k \leq L$) to compute its frequency coefficients:

$$C_k = \text{DCT}(B_k). \quad (8)$$

4.1.4. Coefficient Modulation:

Select two mid-frequency coefficients (u_1, v_1) and (u_2, v_2) in each block to balance imperceptibility and robustness. Let $c_1 = C_k(u_1, v_1)$ and $c_2 = C_k(u_2, v_2)$, and compute their local mean:

$$C_{avg} = \frac{c_1 + c_2}{2} \quad (9)$$

The coefficients are modulated according to the watermark bit $W(k) \in \{0, 1\}$ using an embedding strength parameter α :

$$\begin{cases} c'_1 = C_{avg} + \frac{\alpha}{2}, & c'_2 = C_{avg} - \frac{\alpha}{2} & \text{if } W(k) = 1 \\ c'_1 = C_{avg} - \frac{\alpha}{2}, & c'_2 = C_{avg} + \frac{\alpha}{2} & \text{if } W(k) = 0 \end{cases} \quad (10)$$

4.1.5. Inverse Transformation:

Apply Inverse 2D-DCT (IDCT) on each block to form the modified sub-band LL_1 . Subsequently, apply Inverse 2D-DWT (IDWT) using $[LL_1, LH_1, HL_1, HH_1]$ to generate the watermarked image I_w of size $M \times N$.

4.2. Chained XOR Share Generation (Transit Confidentiality)

To protect the visual confidentiality of the watermarked image I_w during transmission, a bitwise XOR-based (n, n) secret sharing method is applied:

4.2.1. Random Shares Creation:

Generate $n-1$ independent random matrices $\{S_1, S_2, \dots, S_{n-1}\}$ of dimension $M \times N$, where each pixel value is drawn uniformly from $\{0, 1, \dots, 255\}$.

4.2.2. Chained XOR Share:

Construct the final share S_n by computing the bitwise XOR sum of the watermarked image I_w and all preceding random shares:

$$S_n = S_1 \oplus S_2 \oplus \dots \oplus S_{n-1} \oplus I_w = \left(\bigoplus_{k=1}^{n-1} S_k \right) \oplus I_w \quad (11)$$

4.2.3. Share Distribution:

Disperse all n shares $\{S_1, S_2, \dots, S_n\}$ through independent transmission routes or separate storage nodes. Each share reveals zero mutual information regarding I_w .

4.3. Lossless Share Reconstruction

When an authorized recipient collects all n shares $\{S_1, S_2, \dots, S_n\}$, the watermarked image is reconstructed through bitwise XOR operations:

4.3.1. Iterative Reconstruction:

The recipient computes the bitwise XOR sum across all received shares:

$$I'_w = \bigoplus_{k=1}^n S_k = S_1 \oplus S_2 \oplus \dots \oplus S_n \quad (12)$$

4.3.2. Mathematical Integrity:

Because the XOR operation satisfies associativity, commutativity and self-inversion ($A \oplus A = 0$ and $A \oplus 0 = A$), substituting S_n yields:

$$I'_w = \left(\bigoplus_{k=1}^{n-1} S_k \right) \oplus \left(\bigoplus_{k=1}^{n-1} S_k \oplus I_w \right) = 0 \oplus I_w = I_w \quad (13)$$

This guarantees that the reconstruction process is strictly lossless and deterministic at the bit level, without introducing numerical truncation or spatial distortion.

4.4. Watermark Extraction

To retrieve the embedded data from the recovered image I'_w without referencing the original host image, a blind extraction procedure is executed:

4.4.1. Wavelet Decomposition:

Apply single-level 2D Haar DWT to the reconstructed image I'_w (or its luminance channel for multi-channel images) to obtain the approximation sub-band LL'_1 .

4.4.2. Block Partitioning & DCT:

Segment LL'_1 into non-overlapping 8×8 blocks and apply 2D-DCT on each block $k(1 \leq k \leq L)$ to compute transform coefficients C'_k .

4.4.3. Blind Decision Rule:

The estimated bit $W'(k)$ of the embedded payload is determined by comparing the relative magnitudes of the two designated mid-frequency coefficients at coordinates (u_1, v_1) and (u_2, v_2) :

$$W'(k) = \begin{cases} 1, & \text{if } C'_k(u_1, v_1) \geq C'_k(u_2, v_2) \\ 0, & \text{if } C'_k(u_1, v_1) < C'_k(u_2, v_2) \end{cases} \quad (14)$$

4.4.4. Secret Message Recovery & Verification

The extracted bitstream $\$W\$$ is reconstructed into its original representation—such as an ASCII character string for a secret message or a binary logo for provenance verification. Quantitative evaluation metrics, including Bit Error Rate (BER) and Normalized Correlation (NC), are computed between the original sequence W and the recovered sequence W' to verify extraction accuracy.

5. EXPERIMENTAL RESULTS AND DISCUSSION

In this section, we evaluate the performance of our proposed image security framework, which combines blind DWT-DCT watermarking with chained XOR-based secret sharing [9]. We tested the system on standard 512×512 benchmark color images: Baboon representing high-frequency textures and Peppers, representing smooth gradients and flat areas. The framework was evaluated for visual imperceptibility, robustness against common signal processing and geometric attacks, cryptographic security of the shares, lossless reconstruction, and execution speed.

5.1. Imperceptibility and Lossless Reconstruction

To measure how well the watermark is hidden and how accurately the image is recovered from the shares, we use Mean Squared Error (MSE), Peak Signal-to-Noise Ratio (PSNR), and Structural Similarity Index Measure (SSIM) [23]. High PSNR and SSIM values confirm that the watermark is invisible to human eyes, while zero error in reconstruction verifies that no pixel data is lost when combining the shares.

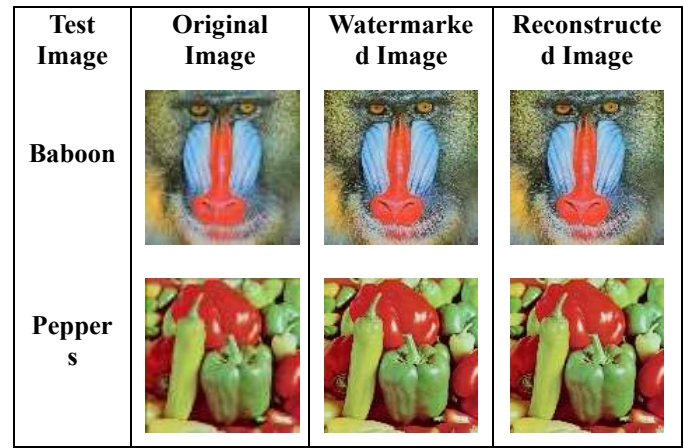


Fig. 2. Visual Quality Comparison of Original, Watermarked and Reconstructed Images for Baboon and Peppers.

As depicted in Fig. 2, the visual appearance of the watermarked and fully reconstructed images shows no perceptible distortion compared to the original assets.

TABLE I. WATERMARK IMPERCEPTIBILITY AND EMBEDDING TIME

Test Image	Embedded Message	Watermarking MSE	Watermarking PSNR (dB)	Watermarking SSIM	Embedding Time (ms)
Baboon	baboon123	1.16	47.47	0.9987	64.87
Peppers	peppers123	1.15	47.51	0.9942	46.22

TABLE II: RECONSTRUCTED IMAGE FIDELITY AND PROCESSING SPEED

Test Image	Reconstruction MSE	Reconstruction PSNR (dB)	Reconstruction SSIM	Reconstruction Time (ms)	Total Time (ms)
Baboon	0.0000	∞ (Lossless)	1.0000	2.12	94.73
Peppers	0.0000	∞ (Lossless)	1.0000	1.97	99.10

As shown in Table I and Table II, the embedding process achieves a PSNR of over 47.4 dB (47.47 dB for Baboon and 47.51 dB for Peppers) and an SSIM greater than 0.994 across both test images. Since a PSNR above 37 dB is considered visually imperceptible, this confirms that our DWT-DCT embedding introduces negligible distortion. When all three shares are recombined using XOR operations, the reconstruction MSE is 0.0000 and the PSNR is infinite (∞) confirming complete lossless recovery. Furthermore, the entire pipeline (embedding, share generation, reconstruction and watermark extraction) executes in under 100 ms (94.73 ms

for Baboon and 99.10 ms for Peppers) demonstrating high computational efficiency.

5.2. Robustness under Common Attacks

To test the robustness of the blind extraction module, the watermarked images were subjected to five common image processing and geometric attacks: Gaussian Noise, Salt & Pepper Noise, JPEG Compression, Gaussian Blur and Cropping. Performance was measured using Bit Error Rate (BER) and Normalized Correlation (NC), alongside image quality metrics after attack.

TABLE III: ROBUSTNESS PERFORMANCE UNDER VARIOUS ATTACKS (BABON)

Attack Applied	MS E	PS NR (dB)	SSI M	BE R	NC	Extraction Result
No Attack (Clean) 	1.16	47.47	0.9987	0.0000	1.0000	Correct (baboon123)
Gaussian Noise 	100.70	28.10	0.8564	0.0000	1.0000	Correct (baboon123)
Salt & Pepper 	101.31	28.07	0.9307	0.0455	0.9474	Partially Corrupted (baboon1:3)
JPEG Compression 	141.05	26.64	0.8436	0.0000	1.0000	Correct (baboon123)
Gaussian Blur 	222.80	24.65	0.8056	0.0568	0.9334	Partially Corrupted (babogf23)
Cropping 	20.28	35.06	0.9966	0.0000	1.0000	Correct (baboon123)

TABLE IV: ROBUSTNESS PERFORMANCE UNDER VARIOUS ATTACKS (PAPPERS)

Attack Applied	MS E	PS NR (dB)	SSI M	BE R	NC	Extraction Result
No Attack (Clean) 	1.15	47.51	0.9942	0.0000	1.0000	Correct (peppers123)
Gaussian Noise 	98.06	28.22	0.6517	0.0000	1.0000	Correct (peppers123)
Salt & Pepper 	104.76	27.93	0.8806	0.0521	0.9334	Partially Corrupted (PepPmrq123)
JPEG Compression 	57.84	30.51	0.8129	0.0000	1.0000	Correct (peppers123)
Gaussian Blur 	45.76	31.53	0.8756	0.0000	1.0000	Correct (peppers123)
Cropping 	69.58	29.71	0.9931	0.0000	1.0000	Correct (peppers123)

Table III and IV, demonstrate that the watermark is successfully recovered under most distortion conditions. For both Baboon and Peppers, the extraction is completely error-free (BER = 0.0000, NC = 1.0000) under Gaussian Noise, JPEG Compression and Cropping. For Peppers, Gaussian Blur also retained perfect extraction (NC = 1.0000). Under Salt & Pepper noise and heavy blur on Baboon, minor bit flips occurred, but the correlation values remained strong NC > 0.93. An NC 0.90 is considered highly robust in watermarking literature, confirming that our watermark embedding in the DWT-DCT domain provides reliable tamper resistance.

5.3. Security and Randomness Analysis of Shares

To confirm that individual shares reveal no visual or statistical clues about the secret watermarked image, we evaluated Information Entropy, Number of Pixels Change Rate (NPCR) [24] and Unified Average Changing Intensity (UACI) [24].

TABLE V: STATISTICAL SECURITY METRICS FOR GENERATED SHARES

Test Image	Share Component	Information Entropy (Ideal: 8.0)	NPCR (%)	UACI (%)	Visual Appearance
Baboon	Share 1	7.9993	99.62	29.93	Pure Noise
	Share 2	7.9994	99.61	29.92	Pure Noise
	Share 3	7.9993	99.63	29.93	Pure Noise
Peppers	Share 1	7.9994	99.63	32.22	Pure Noise
	Share 2	7.9993	99.60	32.20	Pure Noise
	Share 3	7.9993	99.61	32.28	Pure Noise

Table V presents the statistical security and randomness of the generated shares. The information entropy for all shares reaches approximately 7.9993–7.9994, which is virtually equal to the ideal theoretical maximum of 8.0 for an 8-bit image channel. In addition, the NPCR values consistently remain above 99.60% across all shares for both test images, while the UACI averages around 29.93% for Mandrill and 32.20%–32.28% for Peppers. These values confirm that each share behaves as pure pseudorandom noise without revealing any visual or structural patterns of the host image, ensuring robust protection against differential and statistical cryptanalytic attacks.

5.4. Histogram Analysis

Histogram analysis provides a clear visual demonstration of pixel distribution of watermarked images and their shares.

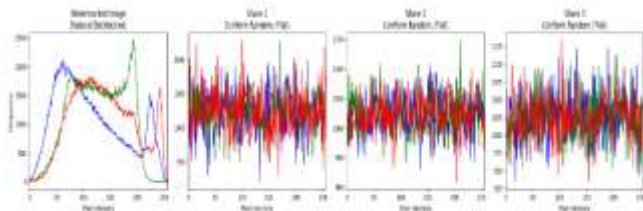


Fig. 3. Histogram of watermarked image and its three shares for baboon.

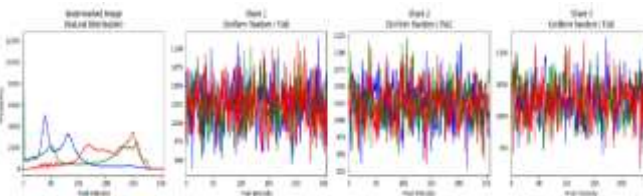


Fig. 4. Histogram of watermarked image and its three shares for Peppers.

As shown in Fig. 3 and 4, the histogram of the watermarked image shows clear variations corresponding to its visual content. In contrast, the histograms of all generated shares are completely flat and uniform across the 0 to 255 intensity range. This flat distribution proves that the shares are pure random noise and do not reveal any secret information about the host image, ensuring strong resistance against histogram-based attacks.

6. CONCLUSION

In this work, a hybrid image security framework combining blind DWT-DCT watermarking with chained XOR-based secret sharing was developed and evaluated. The experimental findings confirm that the framework provides strong visual imperceptibility while retaining high watermark extraction accuracy against common transmission distortions, compression, and geometric cropping. Additionally, the secret sharing layer reliably masks the host content into pseudorandom noise shares with flat intensity distributions, ensuring high resistance against statistical cryptanalysis without leaking secret details. Recombining the shares guarantees exact lossless recovery with minimal computational overhead, making the entire pipeline practical and effective for secure image storage, copyright verification, and real-time transmission.

REFERENCES

- [1] Gupta, A. K. Singh, C. N. Lee, and R. Buyya, "Secure data storage and sharing techniques for data protection in cloud environments: A systematic review, analysis, and future directions," *IEEE Access*, vol. 10, 2022, pp. 71247–71277.
- [2] S. C. Huang and C. F. Wang, "The image watermarking technique using visual secret sharing strategy," in *2008 Eighth International Conference on Intelligent Systems Design and Applications*, vol. 2, 2008, pp. 190–195.
- [3] I. J. Cox, M. L. Miller, J. A. Bloom, J. Fridrich, and T. Kalker, *Digital Watermarking and Steganography*, 2nd ed. Burlington, MA, USA: Morgan Kaufmann, 2008.
- [4] P. Singh and R. S. Chadha, "A survey of digital watermarking techniques, applications and attacks," *International Journal of Engineering and Innovative Technology (IJEIT)*, vol. 2, no. 9, 2013, pp. 165–175.
- [5] A. Al-Haj, "Combined DWT-DCT digital image watermarking," *Journal of Computer Science*, vol. 3, no. 9, 2007, pp. 740–746.
- [6] M. Begum, J. Ferdush, and M. S. Uddin, "A Hybrid robust watermarking system based on discrete cosine transform, discrete wavelet transforms and singular value decomposition," *Journal of King Saud University-Computer and Information Sciences*, vol. 34, no. 8, 2022, pp. 5856–5867.
- [7] M. Naor and A. Shamir, "Visual cryptography," in *Advances in Cryptology — EUROCRYPT '94*, ser. LNCS, vol. 950. Berlin: Springer, 1995, pp. 1–12.
- [8] D. Wang, L. Zhang, N. Ma, and X. Li, "Two secret sharing schemes based on Boolean operations," *Pattern Recognition*, vol. 40, no. 10, 2007, pp. 2776–2785.
- [9] R. Munir, "Comparison of secret color image sharing based on XOR operation in RGB and YCbCr color model," in *2017 6th International Conference on Electrical Engineering and Informatics (ICEEI)*, 2017, pp. 1–6.
- [10] O. B. Chanu and A. Neelima, "A survey paper on secret image sharing schemes," *International Journal of Multimedia Information Retrieval*, vol. 8, no. 4, 2019, pp. 195–215.
- [11] A. O. Mohammed, H. I. Hussein, R. J. Mstafa, and A. M. Abdulazeez, "A blind and robust color image watermarking scheme based on DCT and DWT domains," *Multimedia Tools and Applications*, vol. 82, no. 21, 2023, pp. 32855–32881.

- [12] S. Kanwal, F. Tao, R. Taj, Q. Abbas, and F. Amin, "Discrete cosine transform and discrete wavelet transform based hybrid method for robust and blind medical image watermarking," *Peer-to-Peer Networking and Applications*, vol. 18, no. 5, 2025, p. 251.
- [13] L. C. Gen, S. N. Avivah, and A. J. Muzahid, "Image watermarking for ensuring image integrity and robust copyright protection based on discrete wavelet transform," *IJACI: International Journal of Advanced Computing and Informatics*, vol. 1, no. 1, 2025, pp. 28–38.
- [14] S. Al-Obaidi, N. M. Abdali, and H. Al-Khafaji, "Robust Blind Watermarking Method for High Capacity RGB Image in Wavelet Domain," *Ingénierie des Systèmes d'Information*, vol. 30, no. 5, 2025, p. 1209.
- [15] J. Ooi, L. S. Chuin, and S. B. Hisham, "A robust and secure image watermarking scheme using DWT-DCT-SVD with randomized embedding and optimization," in *2025 IEEE 9th International Conference on Software Engineering & Computer Systems (ICSECS)*, 2025, pp. 24–27.
- [16] X. Wu, N. An, and Z. Xu, "Sharing multiple secrets in XOR-based visual cryptography by non-monotonic threshold property," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 33, no. 1, 2023, pp. 88–103.
- [17] S. Saha, A. K. Chattopadhyay, A. K. Barman, A. Nag, and S. Nandi, "Secret image sharing schemes: A comprehensive survey," *IEEE Access*, vol. 11, 2023, pp. 98333–98361.
- [18] F. Nujumudeen, D. M. Mubarak, and T. Hussain, "Lightweight XOR-based visual cryptography using random shares for secure colour image sharing with minimal shares," *Scientific Reports*, vol. 15, no. 1, 2025, p. 42868.
- [19] S. Mallat, *A Wavelet Tour of Signal Processing*. San Diego, CA, USA: Academic Press, 1999.
- [20] N. Ahmed, T. Natarajan, and K. R. Rao, "Discrete Cosine Transform," *IEEE Transactions on Computers*, vol. C-23, no. 1, 1974, pp. 90–93.
- [21] A. Shamir, "How to share a secret," *Communications of the ACM*, vol. 22, no. 11, 1979, pp. 612–613.
- [22] D.-S. Wang, L. Zhang, N. Ma, and L.-S. Huang, "Secret color images sharing schemes based on XOR operation," *Cryptology ePrint Archive*, Report 2005/374, 2005, pp. 1–24.
- [23] Z. Wang, A. C. Bovik, H. R. Sheikh, and E. P. Simoncelli, "Image quality assessment: From error visibility to structural similarity," *IEEE Transactions on Image Processing*, vol. 13, no. 4, 2004, pp. 600–612.
- [24] Y. Wu, J. P. Noonan, and S. Agaian, "NPCR and UACI randomness tests for image encryption," *Journal of Selected Areas in Telecommunications (JSAT)*, vol. 1, no. 2, 2011, pp. 31–38.