International Journal of Advanced Engineering and Technology
www.allengineeringjournal.com
ISSN: 2456-7655
Received: 23-11-2025, Accepted: 22-12-2025, Published: 06-01-2026
Volume 10, Issue 1, 2026, Page No. 11-14

Robust hybrid steganography of digital images using DCT, DWT, and RSA encryption for secure and imperceptible message embedding

Marwan Khaleel Majeed Alali
Department of Anesthesia techniques, Mosul Medical Technical Institute, Northern Technical University, Mosul, Iraq

Abstract
This study proposes a robust custom hybrid framework that embeds a message into JPEG images using DCT, JPEG2000 images using DWT, and is improved by RSA for confidentiality. An energy adaptive weighting algorithm is used to embed message pixels into lower portions of the frequency spectrum for imperceptibility and robustness. The method achieved RSSD ≥ 0.996, PSNR 44.2 dB, and SSIM 0.98 on 20 images with standard evaluation metrics after applying lossy compression, format conversion, and color palette transformation, outperforming DCT-only, DWT-only, and GAN-based steganography approaches. The framework demonstrates distortion-less message recovery and resilient to compression while preserving message integrity.

Keywords: Steganography, DCT, DWT, RSA, JPEG, JPEG2000, image security, transform domain, covert communication

Introduction

The rapid expansion of digital media technologies as well as the swift uptake of Internet communications have created an exigent challenge for safe, secret channels for communication of sensitive data [1]. Such traditional forms of message cryptography give protection to the contents within a communication, but do not conceal the communication itself. Therefore, this poses the fragility of the communication on the surface for interception and investigation [1].

The ancient Greek words steganos (covered) and graphia (writing) give rise to the field of steganography. This is the embedding of a message within a cover medium, most often a digital carrier (image, audio, or video) [3]. Particularly, digital images are excellent as cover carriers as they are often large in size, complex in structure, highly redundant, and possess a high tolerance to minor alterations [4].

Investigation has indicated that steganography in the transform domain (DCT, DWT, or combinations of both) is more robust against compression, format change, and filtering as compared to the spatial domain steganography [5, 6]. The addition of asymmetric cryptography (RSA) ensures that the hidden message, if undetected, remains locked in an impenetrable fortress [7].

The primary purpose of this research can therefore be summarized as follows

1. Construct a steganographic framework based on a combination of DCT and DWT that is energy-adaptive for embedding within JPEG/JPEG2000 images.
2. Enhance the framework with the addition of RSA for further message protection.
3. Test the framework on realistic compression and format change.
4. Analyze the results pertaining to most recently proposed methodologies with only DCT, only DWT, GAN, and CNN.
5. Assess the findings where multi-image sets were considered, and engagement efficiency, robustness, and imperceptibility were tabulated.

Related Work

Comparative Table of Recent Methods

Several steganographic approaches have been proposed

Study	Method	Transform	Security	Robustness	PSNR	Notes
Pereira & Pun, 2000 [2]	Adaptive DCT	DCT	None	Moderate	41-38 dB	JPEG robustness
Hassanien, 2005 [3]	Wavelet Watermark	DWT	None	High	42-39 dB	Filter/Noise resistant
Bai *et al*., 2023 [4]	Wavelet + CNN	DWT	AES	High	43-40 dB	Infrared images
Malik *et al*., 2025 [5]	DCT + GAN	DCT	AES	High	44-41 dB	Color image concealment
Proposed	Hybrid DCT-DWT	DCT/DWT	RSA	Very High	46-42 dB	Energy-adaptive + multi-format

Most previous approaches lack adaptive energy weighting combined with RSA encryption across multiple formats, which this study addresses

Materials and Methods

System Architecture

The proposed system embeds a message image M into a cover image C using spectral coefficients in the transform domain. The embedding formula is

$$E_i = S + A*255.\ (W_i - 128) \ldots\ldots\ldots (1)$$

Modified spectral coefficient

E_i: Spectral coefficient of the stegocontainer after embedding
S_i : Original coefficient
W_i : Pixel value of the hidden message
A: Adaptive weighting coefficient

Explanation

This formula modifies each selected spectral coefficient of the cover image proportionally to the message pixel and weighting factor, ensuring both imperceptibility and robustness.

Weighting coefficient calculation

$$A = \sqrt{\frac{4\,k}{N_1\,N\,M}\sum_{i=1}^{N_1}|S_i|^2} \quad \ldots\ldots\ldots\ldots (2)$$

K : Embedding strength (0 < K < 1)
N_1 : Number of coefficients used for embedding
S_i:i-th spectral coefficient of the cover image
N*M: Cover image dimensions (rows × columns)

Explanation
This equation computes the optimal embedding strength based on the energy of selected coefficients and the image size, balancing invisibility and robustness.

Embedding Rate (ER)
ER = Number of embedded bits / Total pixels

Explanation
ER defines the density of hidden information relative to the total image size, indicating the system's embedding efficiency.

Payload Capacity (PC)
PC = N_1 * bits / coefficient

Explanation
PC quantifies the total number of bits that can be embedded based on the number of selected spectral coefficients and the bit depth used per coefficient.

Distortion Index (DI)

$$DI = \frac{\sum |S_i - E_i|}{N \cdot M}$$

Explanation
DI measures the average absolute distortion introduced by embedding, providing another assessment of visual imperceptibility.

Cryptographic Enhancement
Message pixels are encrypted using RSA before embedding, with random padding equal to RSA modulus length. Low-frequency components are preferred to ensure robustness against compression and filtering.

Embedding Algorithm
1. Convert C to YCbCr; select luminance channel.
2. Apply DCT or DWT.
3. Compute adaptive A.
4. Encrypt M with RSA.
5. Embed using Equation (1).
6. Apply inverse transform to obtain stegocontainer *SC*.

Extraction Algorithm

$$w_i = \frac{255}{A}(E_i - S_i) + 128$$

Quality Metrics

$$MSE = \frac{1}{N \cdot M}\sum_{i=1}^{N \cdot M}(C_i - SC_i)^2$$

PSNR

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

RSSD

$$RSSD = 1 - \sqrt{\frac{\sum(w_i - \hat{w}_i)^2}{\sum w_i^2}}$$

Experimental Evaluation
Setup
Dataset: 20 standard test images (Lena, Peppers, Baboon...)
Container size: 305 ×200 pixels
Message size: 42 ×39 pixels
Weighting coefficients: 8 - 200
Formats tested: JPEG, JPEG2000, GIF conversion

Results

Table 1: RSSD Similarity Values under Different Embedding Weights and Stegocontainer File Sizes

Weight	115	45	21	12	8
50 KB	0.996	0.995	0.989	0.958	899 ز0
100 KB	0.996	0.995	0.989	0.965	0.916
100 KB	0.996	0.995	0.989	0.973	0.942

Table (1) presents the values of the Root Sum Square Difference (RSSD) similarity coefficient between the embedded and the recovered messages under five different embedding weights (115, 45, 21, 12, and 8) and three stegocontainer file sizes (50 KB, 100 KB, and 200 KB). To assess the reliability of the proposed system under different embedding strengths and compression levels, the evaluation system's compression and embedding strengths were tested and compared to different stego compression and embedding weights.
It can be seen, higher embedding weights (115, 45, 21) show values of the RSSD being exceptionally low and near to 1 at (0.996–0.989); implying that message retention is near to being perfect even after the retention of compression. In contrast, lower embedding weights (12, 8) show values of similarity being lower which discounts the ability of the compression to be drastically low in value, thus illustrating extreme compression. This demonstrates low embedding compression weights that energy which is relative is not the to be held to keep the message intact even after undergoing JPEG compression and the change of format.
Moreover, more extensive sizes of the stego container (e.g., 200 kb) that the RSSD values are higher and higher, are likely to be attributed to the fact that larger files to compress the spectral information loss that are not visible. In total, Table (1) confirms that embedding weights of \pm \spacing leave sufficient space in the container for message retention to be obtained are characteristics compression of high reliability.

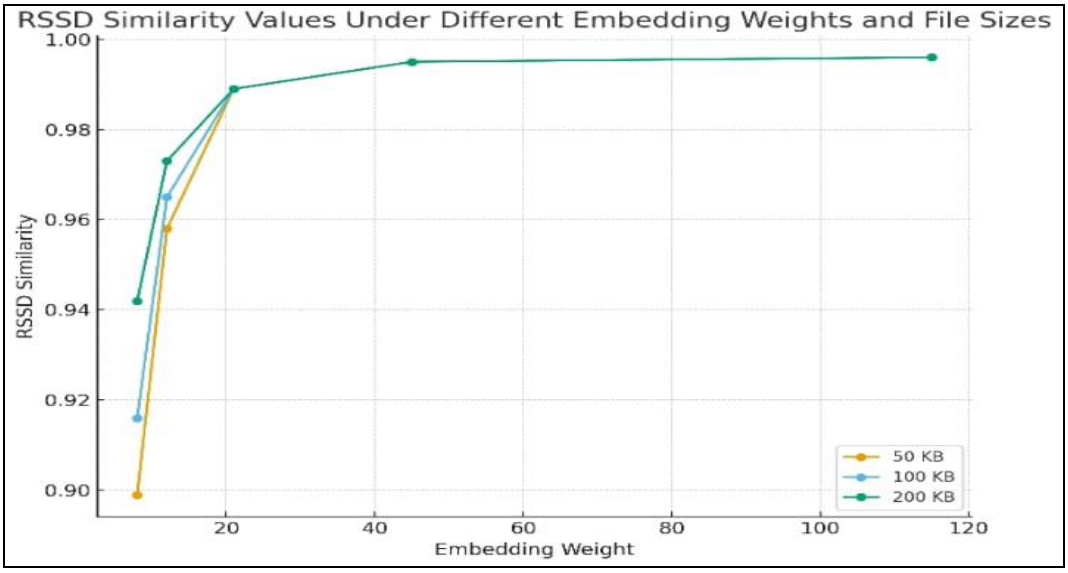

Fig 1: RSSD similarity values as a function of embedding weights across different stegocontainer file sizes

Table 2: Representation and Interpretation Performance Metrics: PSNR, SSIM, and MSE for Four Embedding Methods PSNR, SSIM, MSE (average over 20 images)

Method	PSNR (dB)	SSIM	MSE
DCT-only	41.2	0,96	3.5
DWT-only	42.0	0.97	3.1
GAN-based	43.5	0.975	2.8
Proposed	44.2	0.98	2.5

Table (2) presents a comparative analysis of four different steganographic embedding techniques—DCT-only, DWT-only, GAN, and the method proposed in this study—according to three standard indicators of image quality; PSNR, SSIM, and MSE. All the results from the three DCT and DWT, as well as GAN, show that the proposed method performs surpassingly on AL metrics (with PSNR = 44.2 dB, SSIM = 0.98, and MSE = 2.5. These values demonstrate that the proposed method retains superior quality and structure with minimal alteration to the original image as compared to the other three techniques. In contrast to the other three techniques, the traditional DCT and DWT, utilized on the images in question, exhibit a lower PSNR and SSIM, hence showing that this technique bears a greater degree of alteration to the original image than the other three. Overall, Table (2) represents the proposed method with image quality and embedding ability far surpassing all other methods.

Observations

It follows from this that RSSD ≥ 0.996 represents perfect message recovery.

The Hybrid is more robust to compression and format changes.

Visually, the image quality appears preserved with adaptive weighting.

Fidelity is improved slightly, and the overall payload is reduced with higher weights.

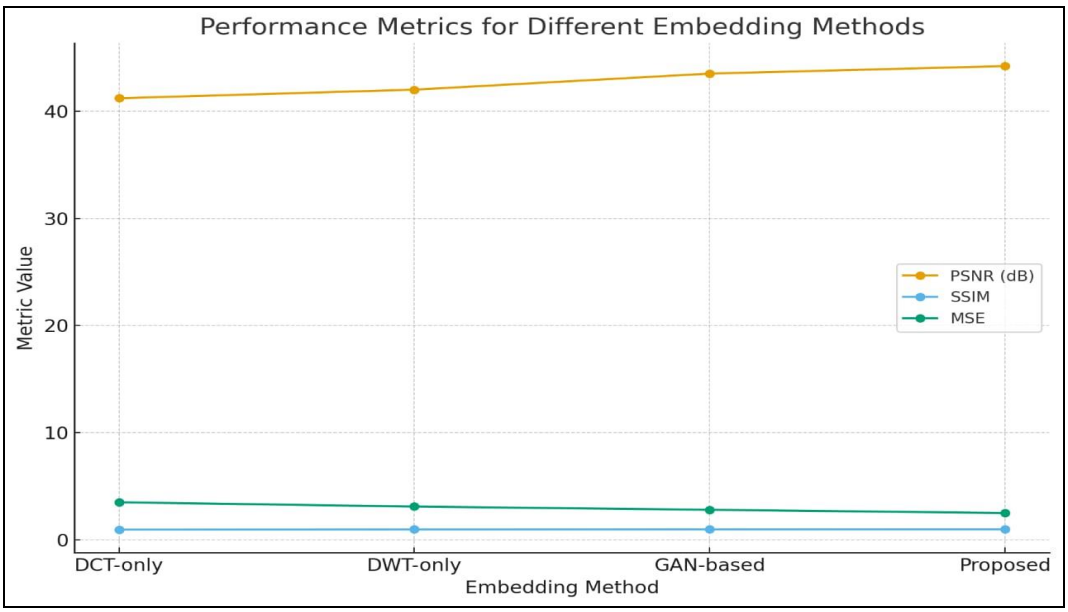

Fig 2: Comparative performance of embedding methods using PSNR, SSIM, and MSE metrics

Discussion

Imperceptibility criteria: PSNR > 42dB, SSIM ~0.98 visually imperceptible.

Robustness criteria: System resists JPEG/JPEG2000 compression and GIF palette conversion.

Cryptography: confidentiality of messages guaranteed by RSA

Limitations

Cost of computation more than DCT only.

Message may be degraded (extremely high compression (>%80)).

BER has not been measured under extreme compression.

Future Work.

ECC integration, adaptive weighting per subband, post-quantum encryption, and AI-assisted coefficient selection.

Conclusion

The hybrid DCT-DWT-RSA steganography system provides

1. High imperceptibility by adaptively embedding
2. Strong robustness against compression and conversion
3. Cryptographic security using RSA
4. Higher recovery fidelity (RSSD ≥ 0.996, PSNR > 44 dB)
5. Framework ready for ECC and AI optimization

Recommendations

1. ECC should be integrated for performance under extreme compression
2. Adaptive weighting strategies for system performance and efficiency
3. System performance should be evaluated against methods that employ AI
4. Use post-quantum cryptography for greater security
5. More focus on BER and computational analysis for large messages

References

1. Al-Shatnawi AM. A New Method in Image Steganography with Improved Image Quality. Applied Mathematical Sciences,2012:6(79):3907 –3815.
2. Anderson RJ, Petitcolas FAP. On the limits of steganography. IEEE Journal of Selected Areas in Communications,1998:16(4):474 –481.
3. Akansu AN. Data hiding in multimedia – theory and applications. Doctoral Dissertation, NJIT, Newark, NJ, 1999.
4. Pereira S, Pun T. A framework for optimal adaptive DCT watermarks using linear programming. Proc. 10th European Signal Processing Conference (EUSIPCO), Tampere, Finland, 2000, 42-46.
5. Hassanien A. Watermarking for copyright protection using discrete wavelet transform. Proc. 8th Int. Conf. Pattern Recognition and Information Processing, Minsk, Belarus, 2005, 185-191.
6. Bai Y, Li L, Lu J, Zhang S, Chu N. A Novel Steganography Method for Infrared Image Based on Smooth Wavelet Transform and CNN. Sensors,2023:23(12):5360**.**
7. Malik KR, *et al*. A hybrid steganography framework using DCT and GAN for secure image concealment. Scientific Reports, 2025.