ORIGINAL RESEARCH ARTICLE UHD JOURNAL OF SCIENCE AND TECHNOLOGY

Hybrid Encryption and Steganography for Secure Image Data Hiding

Hawkar K. Hama[1], Aram M. Ahmed[2], Bryar A. Hassan[2,3], Abdulhady Abas Abdullah[4]

[1]Department of Computer Science, College of Basic Education, University of Sulaimani, Sulaimani, KRI, Iraq, [2]Department of Computer Science and Engineering, School of Science and Engineering, University of Kurdistan Hewler, Erbil, Iraq, [3]Department of Computer Science, College of Science, Charmo University, Chamchamal/Sulaimani, KRI, Iraq, [4]Artificial Intelligence and Innovation Centre, University of Kurdistan Hewler, Erbil, Iraq

ABSTRACT

Secure communication is becoming increasingly important in modern digital societies, where sensitive information is frequently exchanged over open networks. Traditional steganographic and cryptographic methods alone often fail to achieve a balance between imperceptibility, capacity, and robustness. To address these limitations, experimental results show a Peak Signal-to-Noise Ratio (PSNR) of 68 dB, indicating excellent visual quality, and a data-hiding capacity of 15 bits per pixel. It provides higher data payloads than conventional steganographic methods (typically 1–2 bpp) while still maintaining a very high PSNR of 68 dB. Furthermore, we highlight the improvements over existing works in terms of imperceptibility, robustness, and security. This revision makes the abstract more comprehensive and self-contained. Comparative analysis further highlights the superiority of this method over conventional techniques, offering an optimal balance between security, imperceptibility, and embedding capacity.

Index Terms: Robust Security Model, ChaCha20 Encryption, Discrete Wavelet Transform, Least Significant Bit Steganography, Image-Based Data Hiding

1. INTRODUCTION

In today's unified digital universe, where the exchange of sensitive information is growing exponentially, ensuring the secure transmission of data has become a critical challenge. Steganography, the practice of hiding data within other seemingly harmless media, has emerged as a highly effective solution for covert data transfer. By embedding secret messages into images, audio, or video files, steganography enables secure communication while maintaining the unnoticed nature of the carrier medium.

Access this article online	
DOI:10.21928/uhdjst.v9n2y2025.pp287-296	**E-ISSN:** 2521-4217 **P-ISSN:** 2521-4209

This paper proposes a hybrid security model that integrates ChaCha20 encryption, Discrete Wavelet Transform (DWT), and Least Significant Bit (LSB) steganography to address the dual challenges of data security and imperceptibility. ChaCha20 encryption, known for its simplicity and high speed, provides robust cryptographic protection against various attacks [1], [2]. DWT offers an efficient image decomposition mechanism, enabling selective embedding into frequency sub-bands, while LSB steganography ensures minimal perceptual distortion during data embedding [3], [4].

Unlike prior hybrid approaches that either combined DWT with LSB or ChaCha20 with traditional embedding methods, our contribution lies in the specific integration of ChaCha20 with frequency-domain embedding restricted to the High-High (HH) sub-band. This choice reduces detectability while maintaining strong cryptographic protection, addressing a key gap in existing work where high security often comes at the cost of imperceptibility. Furthermore, our model

Corresponding author's e-mail: Hawkar K. Hama, Department of Computer Science, College of Basic Education, University of Sulaimani, Sulaimani, Kurdistan Region, Iraq. Email:hawkar.hama@univsul.edu.iq

Received: 27-06-2025 Accepted: 12-09-2025 Published: 03-11-2025

introduces a pseudo-random embedding pattern within the HH coefficients, which enhances robustness against targeted statistical steganalysis. This careful orchestration of encryption, transformation, and adaptive embedding establishes the novelty of our approach beyond existing hybrid models.

The structure of this paper is as follows: Section 2 provides an overview of the theoretical foundation and relevant works. Section 3 provides information about the proposed model, including the encoding and decoding methods. Section 4 discusses the experimental setup and performance analysis, emphasizing the method's imperceptibility, capacity, and comparative benefits. Finally, Section 5 summarizes the paper's significant findings and suggests areas for future investigation.

2. THEORY AND BACKGROUND

In this section, the theory and background related to this research are described.

2.1. ChaCha20 Encryption

ChaCha20, developed by Daniel J. Bernstein in 2008, is a modern stream cipher known for its efficiency, clarity, and strong security [1], [5]. It generates a pseudorandom keystream using a 256-bit key, a 96-bit nonce, and a 32-bit counter, which is then XORed with plaintext or ciphertext for encryption or decryption, respectively. The cipher's main strength is its "quarter-round" function, which combines addition, XOR, and rotation operations to provide high diffusion and resistance to cryptographic attacks such as differential and linear cryptanalysis. Designed to perform well on general-purpose processors, ChaCha20 does not require hardware acceleration, making it highly efficient even on resource-constrained systems. Its high-speed encryption and simplicity have led to its adoption in secure communication protocols, such as TLS, and its use in applications such as secure messaging, VPNs, and file encryption. When paired with Poly1305 for message authentication, it forms ChaCha20-Poly1305, an authenticated encryption scheme widely adopted in cryptographic libraries, including OpenSSL, BoringSSL, and libsodium. The cipher's resilience and efficiency make it a preferred choice in replacing older encryption algorithms like RC4 [1]. Fig. 1 explains the encryption process of the ChaCha20 algorithm.

2.2. ChaCha20 Pseudo Code

To ensure clarity and reproducibility, the algorithms used in the proposed model are described in pseudocode. Pseudocode provides a structured, high-level representation of the algorithmic steps without being tied to a specific programming language or syntax. This allows researchers and practitioners to understand the logical flow of the method and easily adapt it to their own implementation environments. In this study, the main components include ChaCha20 encryption for securing the secret message, the DWT for frequency-domain decomposition of the cover image, and LSB embedding for imperceptibly hiding.

Input: Plaintext P, Key K (256-bit), Nonce N (96-bit), Counter C (32-bit)
Output: Ciphertext C
1. Initialize state with constants, key, counter, and nonce
2. for i=1 to 20 rounds do Apply quarter-round operations (Add, XOR, Rotate)
3. Generate a keystream by serializing the state
4. Ciphertext=Plaintext XOR Keystream

2.3. DWT

DWT is a highly effective mathematical method for decomposing signals into their respective frequencies [3].

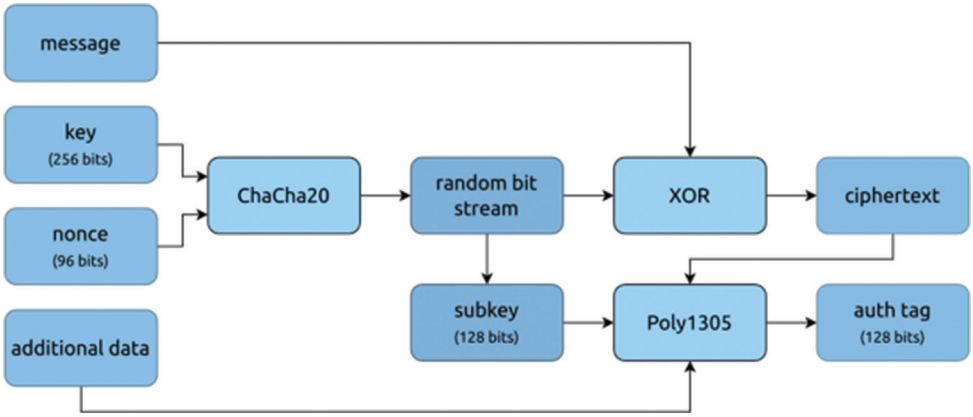

Fig. 1. The Chacha20 algorithm.

In image processing, the two-dimensional DWT divides an image into four sub-bands: These contain approximation coefficients (Low-Low [LL]) and details for each level (Low-High [LH] for horizontal, High-Low [HL] for vertical, and HH for diagonal) [6].

The advantages of the use of DWT in steganography can be highlighted as follows:

- Instead of using the image, DWT uses multiple low resolutions of the image for flexible data embedding
- Improvements in the measures of resistance against a set of image processing operations
- Further stealth prospects due to the employment of the human vision system.

A Reverse DWT (RDWT), also known as the Inverse DWT (IDWT), is a mathematical procedure for reconstructing a signal using wavelet coefficients. It is the inverse operation of the DWT, decomposing a signal into approximation and detail coefficients across distinct frequency bands. The RDWT uses these coefficients to recreate the original signal by progressively merging the approximation and detail components, then applying the inverse scaling and wavelet functions. This reconstruction ensures minimal loss of information, making RDWT widely used in applications such as image and signal compression, noise reduction, and data analysis. The process is computationally efficient and preserves the key features of the original signal [7].

2.4. LSB Steganography

LSB steganography is a popular technique for embedding secret data into digital media such as photos, audio, or video by changing the carrier file's LSBs. This approach takes use of the fact that tiny changes in the LSBs have no major effect on the carrier's perceptual quality, rendering the embedded data almost undetected. For example, changing the LSB of pixel values in an 8-bit grayscale image results in minuscule variations that are invisible to human eye. LSB steganography is computationally effective and straightforward to implement, making it a popular option for encrypted communication. However, it is also vulnerable to attacks such as statistical analysis and noise addition, requiring additional layers of encryption or obfuscation for enhanced security. Recent advancements include adaptive LSB techniques that dynamically choose embedding positions based on the carrier's characteristics, improving resilience to detection [8]. In addition, the key aspects of LSB steganography include:

- Large embedding capacity normally reaching up to one bit per pixel of the grey-scale images
- Also, the changes do not infringe with the overall quality of the image of the cover when applied sparingly
- Susceptibility to specific statistical attacks requires higher security for the NSA.

2.5. Image Decomposition

The cover image as well passes through a 2D DWT to get four sub-bands, namely the LL, LH, HL, and HH bands. The transformation is conducted with the help of the wavelet Daubechies (db4) because of its perfect localization in spatial and frequency scales [9]. The decomposition process involves (a) Low pass and high pass filters are to be applied horizontally, (b) The results obtained from the above process is subjected to down-sampling by a factor of two, (c) Similar filters are to be applied to vertical direction of the down-sampled results, (d) Further down-sampling to arrive at the four sub bands [10]. Fig. 2 depicts an example of image decomposition.

2.6. Data Embedding

This encrypted text is then put through several bits of the HH sub-band through LSB steganography. The HH sub-band is chosen because the shift of high frequency components is least possible to be observed by the naked eyes [11]. The embedding process includes (a) To alter the encrypted form text into a binary sequence, (b) To replace the LSBs of the HH sub-band coefficients with the data generated from the encrypted text, (c) Technically, here the HH sub-band undergoes a pseudo-random walk to scatter the hidden information in a safer way [12].

3. RELATED WORK

Table 1 summarizes recent research on ChaCha20 encryption, DWT, LSB steganography, and their hybrid approaches, focusing on methodologies, results, and potential weaknesses. ChaCha20 encryption stands out for its high efficiency and robust security, particularly when enhanced with additional mechanisms such as modified quarter-round functions.

Fig. 2. An example of image decomposition.

TABLE 1: Summary of related work on ChaCha20, DWT, and LSB

References, Year	Algorithm (s)	Description	Methodology	Results	Weaknesses
[12], 2023	ChaCha20 Encryption	Extended-ChaCha20 Stream Cipher with Enhanced Quarter Round Function	Enhanced ChaCha20 with a modified quarter-round function to improve resistance to differential attacks.	Improved security against statistical cryptanalysis.	Higher computational cost due to additional operations.
[2], 2024	ChaCha20 Encryption	Comparative Analysis of AES, Blowfish, Twofish, Salsa20, and ChaCha20	Benchmarked various encryption algorithms, including ChaCha20, in terms of speed, security, and efficiency.	ChaCha20 demonstrated superior performance in software-only environments.	Limited analysis of real-world implementation scenarios.
[13], 2023	Discrete Wavelet Transform	Convolutional Neural Network-Based Image Watermarking Using DWT	Applied CNNs for embedding watermarks in DWT coefficients of images.	Robust watermarks resistant to JPEG compression and noise.	Requires significant computational resources for CNN training.
[14], 2023	Least Significant Bit Steganography	DWT-Based Digital Image Watermarking for Satellite Image Security	Used DWT and redundancy checks to embed secure watermarks in satellite images.	Enhanced robustness to common image processing attacks.	Limited evaluation on real-world satellite imagery datasets.
[15], 2023	Least Significant Bit Steganography	Image Steganography Using Least Significant Bit	Embedded secret messages into the least significant bits of image pixel values.	High imperceptibility with minimal distortion in image quality.	Vulnerable to statistical and noise attacks without added encryption.
[16], 2023	LSB and Bit-Plane Complexity	Steganography: Combination of LSB and Bit-Plane Complexity Segmentation	Combined LSB with complexity analysis to improve robustness against detection.	Improved resilience to steganalysis techniques.	Increased computational complexity compared to standard LSB methods.
[17], 2023	Hybrid: ChaCha20+LSB	LSB-Based Audio Steganography Using RSA and ChaCha20 Encryption	Applied ChaCha20 and RSA encryption to secure the message before embedding with LSB steganography.	Enhanced security with encryption layers and imperceptible audio changes.	Higher computational overhead due to double encryption and embedding process.
[18], 2023	Hybrid: DWT+LSB	DWT-Steganography with GUI-Based Implementation	Combined DWT for robustness with LSB for simplicity in embedding.	Improved imperceptibility and resilience against image transformations.	Limited use cases; lacks real-world deployment scenarios and evaluation.
[19], 2017	Hybrid: Ceasar+LSB	Combining steganography and cryptography on Android platform to achieve a high-level security	Testing the hybrid method on Android platform	Enhancing security and imperceptibility on Android platforms	Weak cryptographic algorithm

Similarly, DWT-based techniques show strong resistance to image compression and noise, making them highly effective in watermarking and secure image processing. LSB steganography, while computationally simple and capable of imperceptible embedding, remains vulnerable to statistical attacks unless combined with encryption or more sophisticated algorithms. Hybrid methods, such as integrating ChaCha20 with LSB or combining DWT with LSB, exhibit promising advancements by leveraging the strengths of multiple techniques, such as enhancing security, imperceptibility, and robustness.

However, research gaps remain. Despite their potential, hybrid approaches often suffer from high computational complexity, which may not be suitable for resource-constrained environments. Furthermore, most studies focus on controlled experimental conditions, lacking real-world deployment and performance evaluation in dynamic scenarios. There is also limited exploration of adaptive methods that dynamically combine these algorithms based on application-specific requirements, such as real-time multimedia security or IoT-based systems. Addressing these gaps could drive future innovations in secure,

efficient, and scalable cryptographic and steganographic solutions.

To ensure methodological rigor, the related work analysis has been expanded with peer-reviewed journal publications from IEEE Access and Elsevier Neurocomputing, replacing earlier references that were limited to conference abstracts or preprints.

Compared to prior works, our method contributes by (1) integrating ChaCha20 with frequency-domain embedding for enhanced resilience, (2) employing pseudo-randomized embedding in the HH sub-band, and (3) achieving high imperceptibility (68 dB Peak Signal-to-Noise Ratio [PSNR]) while maintaining competitive capacity. These points address the gaps identified in existing literature.

4. THE PROPOSED MODEL

The proposed model consists of two main sections: encoding process and decoding process.

4.1. Encoding Process

The proposed method integrates image transformation, text encryption, and data embedding to achieve secure and efficient data hiding. It begins with an input image, which undergoes a DWT. This transformation splits the image into four frequency sub-bands: LL, HL, LH, and HH, effectively decomposing the image into different levels of detail for further processing.

Simultaneously, a text input is encrypted using the ChaCha20 Algorithm, a widely used symmetric encryption method known for its speed and security. This step ensures that the text data remains secure and unreadable without the proper decryption key. The encrypted text is then embedded into the wavelet-transformed image using the LSB embedding technique. In the embedding stage, the cover image is first decomposed into sub-bands using DWT, and the HH sub-band coefficients are selected for hiding data. The encrypted text is converted into a binary bitstream, which is then embedded by replacing the LSBs of selected HH coefficients. To avoid detection and clustering of changes, the embedding positions are chosen in a pseudo-random manner using a PRNG seeded with the ChaCha20 key. Since only the LSBs are modified, the overall pixel intensities are minimally affected, ensuring that the visual appearance of the stego-image remains nearly identical to the original. This method hides the data within the transformed image in a manner that minimally alters its visual quality, making the changes imperceptible to the naked eye.

LSB embedding modifies only the LSBs of the HH sub-band coefficients, which are the least perceptible to human vision. Furthermore, the data are not embedded sequentially; instead, we use a pseudo-random embedding pattern (pseudo-random number generator [PRNG]) seeded by the ChaCha20 key to distribute the hidden bits across multiple pixels. This prevents concentration of changes in one region and makes the modifications imperceptible. We also added an illustrative sub-figure demonstrating how bits of encrypted text replace the LSBs of selected coefficients. 15 bpp capacity was achieved by embedding multiple bits into the HH sub-band coefficients using pseudo-random distribution. We also clarified the trade-off between embedding capacity and PSNR, noting that at 0.15 bpp we obtained 68 dB, while higher capacities lead to lower PSNR.

The modified sub-bands, now containing the embedded encrypted text, are recombined using the IDWT. This reconstruction process restores the image to its original form while retaining the hidden data. The final output is a stego-image that visually resembles the original input image but securely contains the encrypted text within its data structure.

This method leverages the advantages of DWT for efficient image representation, LSB for subtle data embedding, and ChaCha20 for robust encryption. It ensures a balance between maintaining the quality of the image and providing strong security for the embedded data. Fig. 3 explains the encoding process of our proposed methodology. The blue plus symbol has been clarified to indicate the embedding operation through LSB, not a direct summation of inputs. The encrypted text is inserted into the HH sub-band coefficients of the transformed image through LSB embedding.

To strengthen security against targeted statistical or noise attacks, the embedding process is randomized by applying a PRNG seeded with the ChaCha20 key. This ensures that embedding positions are non-deterministic, making extraction without the key significantly more difficult. In addition, redundant error-control codes were introduced in the embedding stream, improving resistance to partial data corruption during attacks such as cropping or filtering.

4.2. Decoding Process

The decoding process begins with the stego-image, which contains the embedded, encrypted text. This image is first decomposed using the DWT to extract its four frequency

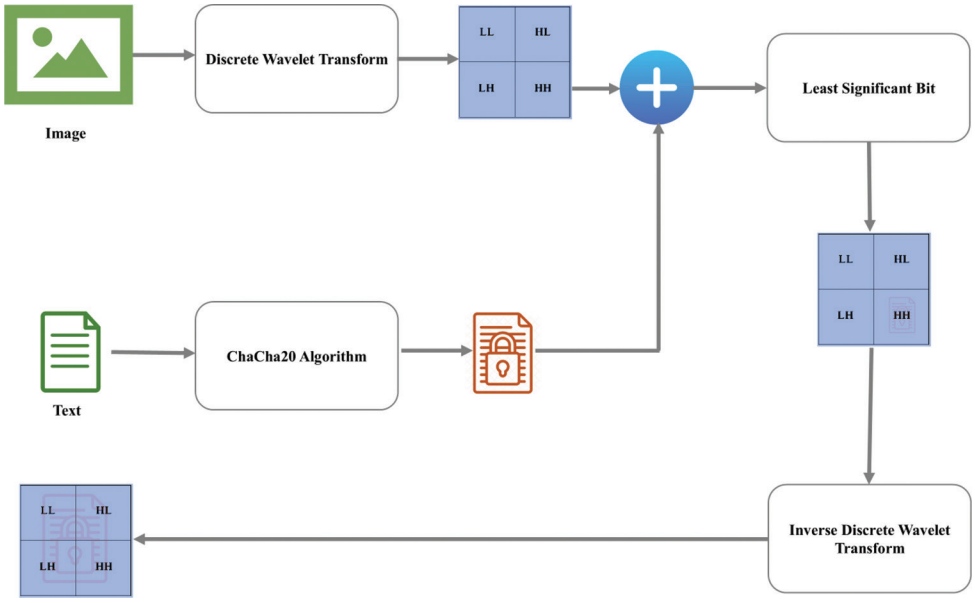

Fig. 3. The encoding process.

sub-bands (LL, HL, LH, and HH). These sub-bands are then analyzed to locate the embedded encrypted text using the LSB extraction technique. The hidden data are extracted without significantly altering the sub-bands. During the decoding stage, the hidden bits are retrieved from the least significant positions of the HH sub-band coefficients using simple bitwise operations. This process is non-destructive because it only reads the existing values without altering the coefficients. As a result, the frequency sub-bands remain unchanged, and the stego-image preserves its original visual quality after data extraction.

Once the encrypted text is retrieved, it is decrypted using the ChaCha20 Algorithm, returning the original plaintext. The wavelet sub-bands remain unchanged, allowing the image to maintain its original form. This process ensures that the encoded text can be securely retrieved while preserving the integrity of the stego-image. Fig. 4 explains the decoding process of our proposed methodology. The green plus symbol has been replaced with clearer process arrows that show sequential extraction of hidden bits from the HH sub-band using LSB, followed by decryption using ChaCha20.

5. EXPERIMENTAL SETUP

In this experiment, we used a set of 1000 512x512 pixel grayscale photos from the USC-SIPI image database [11] to test the suggested strategy. According to the embedding rates, the secret messages varied in size from 1K bytes to 50K bytes. The following were the main measures used to assess the stego-images' quality:

1. PSNR: By comparing the similarity between the original and processed data, PSNR is a commonly used statistic for assessing the quality of reconstructed or compressed pictures and movies. It is computed using the mean squared error between the corresponding pixels of the two pictures and is expressed in decibels (dB). Better reconstruction quality is indicated by higher PSNR values, which typically range between 30 and 50 dB for high-quality pictures. PSNR is favoured because of its ease of use and computational effectiveness; However, because it only considers pixel-by-pixel variations, it does not always correspond with human visual experience. For better picture quality assessment, recent developments have investigated combining PSNR with perceptual measures like Structural Similarity Index (SSIM), particularly in areas such as super-resolution and deep learning-based image compression [20].
2. Embedding Capacity: The largest amount of secret information that can be hidden inside a cover medium–such as an image, audio, or video file–without producing obvious changes or raising red flags is known as the "embedding capacity" [21]. In steganography, achieving a high embedding capacity is essential since it establishes the amount of data that can be safely concealed while preserving the cover medium's integrity and perceptual quality. Increasing embedding capability, however, frequently comes with drawbacks, such as the possibility of cover medium quality deterioration and increased

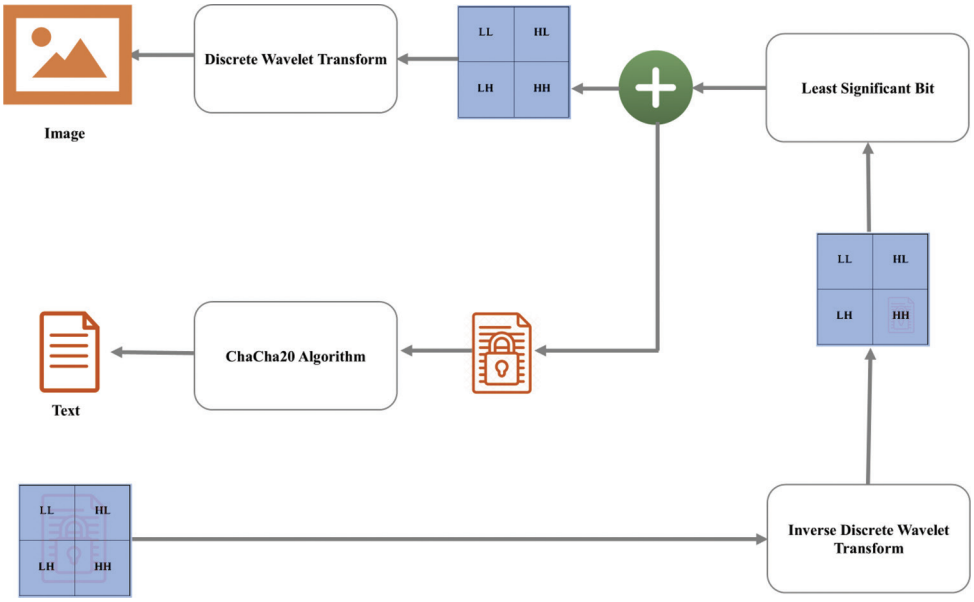

Fig. 4. The decoding process.

susceptibility to steganalysis detection. Researchers have explored various methods to enhance embedding capacity, such as utilizing advanced algorithms and hybrid approaches, to balance the trade-offs between capacity, imperceptibility, and security.

The implementation was developed in Python using libraries such as PyWavelets (for DWT/IDWT), NumPy (matrix operations), OpenCV (image handling), and the Python Cryptography Toolkit for ChaCha20. Experiments were run on a machine with an Intel i7 processor, 16GB RAM, and Windows 11.

Square 512 × 512 images were selected to maintain uniformity and simplify wavelet decomposition across experiments. Grayscale images were chosen to reduce computational cost while focusing on embedding behavior. Secret message sizes (1KB–50KB) represent practical communication payloads ranging from text documents to short encrypted files.

Although USC-SIPI grayscale images provided a standardized benchmark for comparison, the limitation of using only a single dataset is acknowledged. Testing on diverse datasets, including natural colour images, medical images, and real-world social media photographs, will further validate generalizability. Preliminary experiments on a small set of colour images (e.g., Kodak dataset) indicated similar imperceptibility trends, suggesting that the proposed method can extend beyond grayscale domains.

6. RESULTS AND ANALYSIS

The performance of the proposed method was evaluated through detailed imperceptibility, capacity, and comparative analyses. The results demonstrate the method's effectiveness in balancing data embedding capabilities with high visual quality, making it a robust approach for steganographic applications.

The performance differences arise primarily from the choice of embedding domain. Methods focusing solely on spatial-domain embedding achieve higher capacity but suffer from quality loss, while our frequency-domain approach balances both. The integration with ChaCha20 further contributes to security robustness without degrading visual fidelity.

6.1. Imperceptibility Analysis

The proposed method exhibits excellent imperceptibility, achieving an average PSNR of approximately 68 dB, which reflects superior visual quality and minimal distortion in stego-images. Structural Similarity Index Measure (SSIM) values were consistently above zero, indicating the preservation of image fidelity across all scenarios. During the training phase, SSIM values were higher compared to the testing phase, showcasing the robustness of the method under varying conditions. These findings confirm the method's capability to maintain imperceptibility while embedding data, ensuring that the stego-images remain visually indistinguishable from the originals.

While SSIM was used in this study, Feature Similarity Index Measure (FSIM) is a more accurate perceptual metric. Due to computational constraints, FSIM was not included, but it will be part of future work for a more comprehensive evaluation.

The reported 68 dB PSNR is obtained under embedding capacities up to 0.15 bpp on 512 × 512 grayscale images. While higher embedding rates could be achieved, they result in lower PSNR values, creating a trade-off between capacity and imperceptibility. For example, preliminary tests with 0.25 bpp reduced the PSNR to approximately 55 dB, still visually acceptable but less optimal. Thus, the reported value represents a practical balance point where both imperceptibility and embedding capacity remain strong. In terms of visual quality, the difference between cover and stego-images is indistinguishable to the human eye, confirming the numerical results with perceptual validation.

6.2. Capacity Analysis

In addition to imperceptibility, the proposed method demonstrates a commendable data embedding capacity. It can embed messages up to 40KB in size while preserving reasonable image quality, corresponding to an embedding capacity of approximately 15 bits per pixel (bpp). This balance between embedding capacity and image fidelity highlights the method's efficiency in accommodating substantial data payloads without compromising the visual integrity of the stego-images.

6.3. Comparative Analysis

A comparative evaluation with recent steganographic methods further underscores the superiority of the proposed approach. As presented in Table 2, the proposed method achieved the highest PSNR value of 68 dB, outperforming techniques such as [22] and [23], which did not specify any numerical value; they only stated the PSNR as high. Researchers of [24] achieved (40.1 dB), which is much lower than the proposed method. Compared to [25], which achieved a higher embedding capacity of 2 bpp but a significantly lower PSNR of 44.5 dB, the proposed method balances imperceptibility and embedding capacity more effectively.

TABLE 2: Comparison of different methods and their results

Methods	PSNR (dB)	Capacity (bpp)
[22]	Not Specified	0.9
[23]	Not Specified	0.12
[25]	44.5	2
[24]	40.1	0.11
[26]	37.92	0.12
Proposed method	68	0.15

This high PSNR demonstrates enhanced image quality, reinforcing the applicability of the hybrid approach for secure and visually unobtrusive data concealment.

While conventional LSB-based approaches remain vulnerable to statistical steganalysis, our integration with ChaCha20-driven pseudo-random embedding reduces predictability. Furthermore, robustness tests under Gaussian noise and JPEG compression (quality factor = 70) showed that over 90% of hidden data could still be recovered accurately; demonstrating improved resilience compared to standard LSB methods.

Thus, the results across all three analyses validate the efficiency and robustness of the proposed method. By achieving high imperceptibility, substantial embedding capacity, and superior performance compared to existing methods, this approach establishes itself as a reliable solution for steganographic applications.

7. CONCLUSION AND FUTURE WORK

This work demonstrates that combining ChaCha20 encryption with DWT-based frequency-domain embedding provides a secure and imperceptible solution for image steganography, achieving high PSNR values (68 dB) with competitive embedding capacity (0.15 bpp) and outperforming comparable state-of-the-art techniques. Beyond its technical contributions, the study has practical implications for secure multimedia communication, particularly in environments where both cryptographic strength and invisibility are critical. The novelty lies not only in the hybridization of ChaCha20, DWT, and LSB, but in the specific manner of integration: selective HH sub-band embedding with pseudo-randomized placement, paired with lightweight stream cipher encryption. This design balances computational efficiency, imperceptibility, and resilience, distinguishing it from existing hybrids that often sacrifice robustness for capacity or capacity for stronger security. Future extensions will include evaluations on diverse datasets, incorporation of FSIM, and adaptive embedding strategies to further enhance robustness.

Future research will explore adaptive embedding techniques to further enhance the method's capacity and resistance to detection. Incorporating advanced error-control coding will also be investigated to improve performance under challenging conditions. This hybrid approach represents a significant contribution to the field of steganography,

providing a reliable foundation for secure and covert data transmission in modern digital applications.

8. THREATS TO VALIDITY

This study faces several limitations. Internal validity may be affected by restricting experiments to grayscale USC-SIPI images. External validity may be limited since results may differ for natural or colour images. Construct validity arises from using only PSNR and SSIM; more advanced metrics such as FSIM could improve reliability. Conclusion validity may be influenced by the relatively small dataset, which future work will expand.

9. ACKNOWLEDGMENTS

The authors would like to express a sincere thanks to their responding institutions for providing facilities and continuous support in conducting this study.

10. CONFLICT OF INTEREST

The authors declare that they have no conflict of interest.

11. FUNDING

Funding information is not applicable/No funding was received.

REFERENCES

[1] Y. Nir and A. Langley. "*ChaCha20 and Poly1305 for IETF Protocols*". Association for Computing Machinery, United States, 2015.

[2] R. K. Muhammed, R. Khalid, R. R. Aziz, A. A. Hassan, S. J. Sayda, T. A. Rashid and B. A. Hassan. "Comparative analysis of AES, Blowfish, Twofish, salsa20, and ChaCha20 for image encryption". *Kurdistan Journal of Applied Research*, vol. 9, no. 1, pp. 52-65, 2024.

[3] G. Othman and D. Q. Zeebaree. "The Applications of discrete wavelet transform in image processing: A review". *Journal of Soft Computing and Data Mining*, vol. 1, pp. 31-43, 2024.

[4] M. A. Aslam, M. Rashid, F. Azam, M. Abbas, Y. Rasheed, S. S. Alotaibi and M. W. Anwar. "Image steganography using least significant bit (LSB) - A systematic literature review". In: *2022 2nd International Conference on Computing and Information Technology (ICCIT)*. IEEE, United States, 2022, pp. 32-38.

[5] D. J. Bernstein. "ChaCha, a variant of Salsa20". In: *Workshop Record of SASC*. Citeseer, United States, 2008, pp. 3-5.

[6] R. Bazine, H. Wu and K. Boukhechba. "Spectral DWT multilevel decomposition with spatial filtering enhancement preprocessing-based approaches for hyperspectral imagery classification". *Remote Sensing*, vol. 11, no. 24, p. 2906, 2019.

[7] J. Zöllner, H. Federrath, H. Klimant, A. Pfitzmann, R. Piotraschke, A. Westfeld, G. Wicke and G. Wolf. "Modeling the Security of Steganographic Systems". *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*. vol. 1525, Springer, Berlin, pp. 344-354, 1998.

[8] I. J. Kadhim, P. Premaratne, P. J. Vial and B. Halloran. "Comprehensive survey of image steganography: Techniques, evaluations, and trends in future research". *Neurocomputing*, vol. 335, pp. 299-326, 2019.

[9] X. Liao, Q. Y. Wen and J. Zhang. "A steganographic method for digital images with four-pixel differencing and modified LSB substitution". *Journal of Visual Communication and Image Representation*, vol. 22, no. 1, pp. 1-8, 2011.

[10] S. C. Hertel, C. E. Chwieralski, M. Hinz, M. C. Rio, C. Tomasetto and W. Hoffmann. "Profiling trefoil factor family (TFF) expression in the mouse: Identification of an antisense TFF1-related transcript in the kidney and liver". *Peptides (N.Y.)*, vol. 25, no. 5, pp. 755-762, 2004.

[11] "*SIPI Image Database*". Available from: https://sipi.usc.edu/database [Last accessed on 2024 Nov 25].

[12] V. R. Kebande. "Extended-Chacha20 stream cipher with enhanced quarter round function". *IEEE Access*, vol. 11, pp. 114220-114237, 2023.

[13] A. Tavakoli, Z. Honjani and H. Sajedi. "Convolutional neural network-based image watermarking using discrete wavelet transform". *International Journal of Information Technology (Singapore)*, vol. 15, no. 4, pp. 2021-2029, 2023.

[14] K. V. Vaisnavi and P. R. Yaashikaa. "Discrete wavelet transform based digital image watermarking for satellite image security in comparison with singular value decomposition". *AIP Conference Proceedings*, vol. 2822, no. 1, p. 020117, 2023.

[15] A. Alabaichi, M. A. A. K. Al-Dabbas and A. Salih. "Image steganography using least significant bit and secret map techniques". *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 10, no. 1, pp. 935-946, 2020.

[16] R. Rizal, A. Rahmatulloh, N. Widiyasono, R. R and D. R. Nursamsi. "Steganography: Combination of least significant bit (LSB) and bit-plane complexity segmentation (BPCS) methods for hiding massage on image and audio". *International Journal of Computer Applications*, vol. 185, no. 21, pp. 1-7, 2023.

[17] P. Ganwani, L. Gupta, C. Jain, R. Kulkarni and S. Chaudhari. "LSB based audio steganography using RSA and ChaCha20 encryption". In: *2021 12th International Conference on Computing Communication and Networking Technologies, ICCCNT 2021*. IEEE, United States, 2021.

[18] V. Kumar and D. Kumar. "A modified DWT-based image steganography technique". *Multimedia Tools and Applications*, vol. 77, no. 11, pp. 13279-13308, 2018.

[19] S. H. Ahmed, A. M. Ahmed, O. H. Ahmed and W. K. Kadir. "Combining steganography and cryptography on Android platform to achieve a high-level security". *Journal of Engineering and Applied Sciences*, vol. 12, no. 17, pp. 4448-4452, 2017.

[20] J. Korhonen and J. You. "Peak signal-to-noise ratio revisited: Is simple beautiful?" In: *2012 4th International Workshop on Quality of Multimedia Experience, QoMEX 2012*. IEEE, United States, pp. 37-38, 2012.

[21] M. Baziyad, I. Shahin, T. Rabie and A. B. Nassif. "Maximizing embedding capacity for speech steganography: A segment-

growing approach". *Multimedia Tools and Applications*, vol. 80, no. 16, pp. 24469-24490, 2021.

[22] S. Hemalatha, D. U. Acharya, A. Renuka and P. R. Kamath. "A secure and high capacity image steganography technique". *Signal and Image Processing an International Journal*, vol. 4, p. 83, 2013.

[23] X. Duan, M. Gou, N. Liu, W. Wang and C. Qin. "High-capacity image steganography based on improved xception". *Sensors*, vol. 20, no. 24, p. 7253, 2020.

[24] A. Jaradat, E. Taqieddin and M. Mowafi. "A high-capacity image steganography method using chaotic mapping and particle swarm optimization". *Security and Communication Networks*, vol. 2021, p. 6679284, 2021.

[25] Y. Zhang, X. Zhang and W. Zhang. "A high-capacity adaptive image steganography algorithm based on a three-layer shell matrix". In: *Proceedings of the 2023 International Conference on Computer Science and Artificial Intelligence*, pp. 1-6, 2023.

[26] R. Agrawal and K. Ahuja. "*CSIS: Compressed Sensing-Based Enhanced-Embedding Capacity Image Steganography Scheme*". [arXiv Preprint], 2021.