CINEFORUM
ISSN: 0009-7039
Vol. 66. No. S5, 2026 (Special Issue 5)

A Secure Encrypted Steganographic Framework Using BLAKE3-Based Stream Encryption with LWT for Confidential Image Communication.

Suparnesh Bhattacharyya[1], Dr. Pabitra Pal[2], Dr. Sanjay Nag[3]

[1] Department of Computer Science & Engineering, Swami Vivekananda University, India
Email: suparneshbhattacharyya@gmail.com
[2] Supervisor, Department of Computer Science & Engineering, Swami Vivekananda University, India
Email: pabipaltra@gmail.com
[3] Joint Supervisor, Department of Computer Science & Engineering, Swami Vivekananda University, India
Email: sanjayn@svu.ac.in
Corresponding Author:
Suparnesh Bhattacharyya
Email: suparneshbhattacharyya@gmail.com

Abstract
The proliferation of digital communication has led to the need to transmit confidential multimedia information securely at a high rate. Classic cryptographic schemes like AES, ChaCha20, and SNOW-V are designed aimed at data confidentiality only and do not hide the presence of the transmitted data. On the other hand, the conventional image steganography methods are those techniques of hiding secret information into digital images, but the embedded data is easy to be detected. Thus, combining the two techniques of encryption and steganography is a viable approach to improve communication security.
In this research, a new encrypted picture steganography scheme is suggested using Modified Dynamic Key Stream 256 (MDKS-256) encryption algorithm and Lifting Wavelet Transform (LWT). The proposed MDKS-256 architecture is a new dynamic state-update mechanism that includes three novel modifications: the use of BLAKE3 for master key generation, the adaptive rotation, the nonlinear mixing, the dynamic generation of round constant, the parallel update of the state, and the dynamic generation of the keystream. The proposed encryption engine uses 16 rounds of transformation, which leads to which is designed to improve diffusion and provide stronger empirical sensitivity to key and nonce perturbations.
In proposed architecture for data hiding is based on Lifting Wavelet Transform that disintegrates and split the image into the LL, LH, HL, and HH frequency sub-bands. The bit stream is encrypted then adaptively embedded in the HL sub-band for high embedding capacity and excellent visual quality. The integer-to-integer property of LWT guarantees lossless reconstruction, low computation complexity and better imperceptibility than the traditional DWT-based methods.
Standard benchmark image datasets are employed to evaluate the proposed framework and standard image processing techniques are implemented to analyze it with PSNR, SSIM, MSE, entropy, histogram uniformity, NPCR, UACI, correlation coefficient, embedding capacity, and execution time. Experimental evaluation demonstrates high embedding fidelity and favourable statistical characteristics under the evaluated benchmark conditions, while the key/nonce sensitivity, differential analysis, round-count ablation, and selected NIST SP 800-22 tests provide empirical evidence regarding the behaviour of the proposed construction..
Keywords: Image Encryption, Image Steganography, MDKS-256, BLAKE3, LWT, Secure Communication, Stream Cipher, Keystream Generation, Information Hiding.

INTRODUCTION

The availability of cloud computing and the IoT, telemedicine, military communication, e-governance, and multimedia networking has greatly expanded the amount of digital image transmission over public networks. While the state-of-the-art communication equipment gives the user high speed connectivity, it also opens the door to many cyber threats, such as interception, traffic analysis, tampering with images, replay attacks and data leakage. Thus, the problem of secure image communication has been among the best prominent research problems in information security in the modern era.
There are two complementary ways of protecting digital information, namely cryptography and steganography. Cryptography changes the plaintext into an unintelligible ciphertext with the help of secret keys so that even if

the transmitted data is intercepted, it will remain unintelligible and not be understood. Encrypted data does, however, clearly show the presence of confidential data, which would be a good target to attack. Steganography, on the other hand, hides the presence of secret information by hiding it inside digital media like pictures, sound or video. While steganography can be used to conceal a message, it could still be lost if the embedding can be detected by using steganalysis.

Recently, research centred on encrypted steganography, which uses a cover image to embed a secret message that is first encrypted, has been taken to address these limitations. These hybrid systems simultaneously provide the confidentiality, imperceptivity, and secure transmission. Some previous work has used encryption algorithms like AES, ChaCha20, and SNOW-V with transform domain embedding approaches of DWT, IWT, or DCT. These approaches have proven to be effective but have a number of drawbacks.

Many of the currently available stream ciphers are based on fixed or pre-programmed internal structures that lack flexibility in evolving the state, especially if a dynamic one is required. Secondly, traditional key scheduling methods may not have adaptive round dependent transformation, which makes them less resistant to advanced cryptanalytic attacks. Third, some transform domain steganography methods are based on floating-point operations, which makes it more difficult, time consuming and leads to errors in the reconstruction process. Moreover, most of the current encrypted steganographic schemes have not optimized the complexity of the encryption, imperceptibility of embedding, statistical security and simultaneous high computational efficiency.

To fill the above research gaps, this study suggests a novel framework. of encrypted image steganography based on a novel Modified Dynamic Key Stream 256 (MDKS-256) encryption algorithm and the Lifting Wavelet Transform (LWT). MDKS-256 does not use a traditional stream cipher architecture, but rather a master key generation mechanism using BLAKE3 as the block cryptography, dynamic register initialization, adaptive computation of the round constant, nonlinear mixing operations, parallel state updates, and generation of keystream after sixteen rounds of transformation. The combination of dynamic architecture, which greatly improves confusion, diffusion, randomness and resistance to differential attacks, along with efficient software implementation, is significant.

The proposed framework is based on the LWT, which is lower in computational complexity and provides exact image reconstruction in an integer-to-integer wavelet decomposition process, instead of using the conventional DWT. MDKS-256 generates the encrypted bit stream, and then the bit stream is embedded in the HL frequency sub-band, which uses an encrypted-bit embedding in selected HL coefficients using LSB replacement to achieve a high embedding capacity while causing weak visual distortion to the host image.

The suggested framework seeks to enhance the security and robustness of encrypted steganography while maintaining high image quality and computational efficiency. To evaluate the suggested strategy's efficacy, various objective performance metrics such as PSNR, SSIM, MSE, entropy, NPCR, UACI, histogram analysis, correlation analysis and execution time are calculated using the benchmark image datasets and extensive experiments are performed.

The following is a list of this paper's main contributions:

A new design for stream Cryptography architecture based on BLAKE3 master key generation with dynamic state evolution called MDKS-256.

New adaptive nonlinear round function with dynamic rotation, mixing, round constant generation and parallel register updates.

Secure and encrypted image steganography using MDKS-256 and Lifting Wavelet Transform (LWT).

High imperceptibility and embedding capacity for encrypted data: LSB/parity-based embedding in selected HL coefficients of encrypted data in the frequency sub-band of HL.

Full security and performance evaluation with statistical, visual and cryptographic performance measures.

LSB/parity-based embedding in selected HL coefficients

The remainder of this work is structured as follows.

Recent advances in encrypted image steganography and secure communication using MDKS-256 stream ciphers are discussed in section **3.1**, the proposed embedding and extraction framework based on LWT is presented in section **4.1**. Section **5.3** discusses experimental results and security analysis. Lastly and in conclusion, Section **9** presents future lines of inquiry.

Abbreviation

Abbreviation	Meaning
MDKS-256	Modified Dynamic Key Stream-256
BLAKE3	BLAKE3 cryptographic hash function
LWT	Lifting Wavelet Transform
LL/LH/HL/HH	LWT approximation and detail sub-bands
PSNR	Peak Signal-to-Noise Ratio
SSIM	Structural Similarity Index Measure
MSE	Mean Squared Error
NPCR	Number of Pixels Change Rate
UACI	Unified Average Changing Intensity
BER	Bit Error Rate
NCC	Normalized Cross-Correlation
IV/Nonce	Initialization value / public unique per-message value
RC	Round Constant
CTR	Block/round counter

Table 1: Abbreviations Used in the Proposed MDKS-256 and DWT-Based Steganographic Framework

Literature analysis

The past few years, With the swift evolution of the cloud computing, IoT, telemedicine, military communication and multimedia networking, secure image communication is now an active field of research. As a result, many researchers have suggested cryptographic and steganographic methods to enhance the confidentiality, imperceptibility, robustness and computation efficiency of the system. In recent years, the main focus of research has been the combination of encryption of image with transform domain steganography for multiple layers of security. To enhance the capacity of concealing data while maintaining visual quality, Gahan and Devanagavi **[1]** suggested an edge-guided image steganography scheme based on variable-bit LSB embedding method, which is parameter optimized. They have achieved outstanding performance in terms of PSNR and embedding efficiency with their edge-encrypted-bit embedding in selected HL coefficients using LSB replacement. Alaklabi **[2]** proposed a lightweight crypto-steganographic framework to achieve secure image communication with minimum computational complexity by utilizing two techniques: encryption, steganography. Wang et al. **[3]** also used a complete convolutional neural network to simultaneously encrypt the picture and achieve the embedding, which shows that deep learning can be used to enhance the embedding security and resistance to steganalysis. Several researchers have studied on high capacity and reversible data hiding techniques. Zhang **[4]** suggested a rate-distortion-based steganography method that would achieve maximum embedding capacity with minimum distortion to the image. An algorithm was proposed in Chen et al. **[5]** that can completely recover the embedded message and original cover image for reversible data hiding by employing linear prediction and bit plane slicing. Wang **[6]** presented a Lossless image encryption invertible neural network-based system which is capable of accurate message extraction and perfect image reconstruction. The essential part of transform domain processing in the security of multimedia communication was introduced by Tan **[7]** by using the wavelet neural network approach for improving the quality of image synthesis and embedding performance. Another area of interest has been wavelet domain image processing due to its ability to maintain image quality during embedding. Ghaskadbi and Sutar **[8]** have proposed a hybrid image encryption and compression system based on IWT and SVM Segmentation. They pointed out that the approach can enhance the embedding efficiency and reduce the image distortion, though multiple pre-processing stages make the approach more complicated. Similarly, Abbasi **[11]** introduced a dual-wavelet image steganography system where the embedding strength and imperceptibility are enhanced by using DWT and IWT, thus proving the effectiveness of the wavelet-based transforms in secure data hiding. In recent years, the design of stream ciphers has evolved into a field that has seen numerous developments in terms of secure stream communication, particularly for multimedia applications. To enhance the encryption output and security, Ekdahl et al. **[9]** proposed high-performance stream cipher SNOW-V with expanded internal state and optimized finite-state machine architecture for 5G communication system. Ding et al. **[10]** identified Salsa20 and ChaCha20, by proposing an enhanced related-cipher attack which showed that more powerful

nonlinear state-update mechanisms are necessary to defend against sophisticated cryptanalytic techniques. Muhalhal and Alshawi **[13]** have also modified the Salsa20 stream cipher by adding chaotic maps to further increase the randomness of the ciphertext and diffusion properties. Balli and Rao **[12]** proposed using ChaCha20 encryption with the adaptive LSB video steganography, which obtained improved security and embedding efficiency in multimedia applications. All these studies suggest that the new stream ciphers offer fast encryption but there are still some room for improvement in their dynamic state evolution and adaptive keystream generation. Optimization algorithms that combine with the transform-domain encryption have also been studied. Kumar and Kumar **[14]** introduced the image steganography framework with optimized genetic algorithm-based chaotic encryption which concluded that LWT has been capable of maintaining image quality and chaotic encryption has been improved security. However, the computational complexity of the optimization algorithms can hinder real-time implementation. The original ChaCha algorithm **[15]** is one of the most popular lightweight stream ciphers because of its simple ARX structure and high software efficiency, and is still the inspiration for the design of modern stream encryption algorithms. In addition to securing images, the secure communication infrastructure has also extended to the cloud-based environment. Wegner et al **[16]** have explored the security issues in edge assisted cloud computing and highlighted the importance of lightweight cryptographic mechanisms for resource constrained environments. Efficient symmetric-key cryptography has been put to good use in searchable symmetric encryption where information is retrieved in an encrypted form while an attacker learns nothing of the key. Curtmola et al. **[17]** showed the practical importance by proposing searchable symmetric encryption, where information can be retrieved in an encrypted form with no leakage of sensitive information to an attacker. Greenberg et al. **[18]** pointed out problems encountered in high-performance cloud infrastructures and focused on the need for scalable cryptographic processing for secure distributed communication.

These studies have made great strides in advancing image steganography, transform domain embedding and stream cipher design, but there are still several research challenges to be addressed. The existing steganographic techniques concentrate mainly on the capacity of the embedding or quality of the images, while many cryptographic techniques tend to concentrate the strength of the encryption without taking into consideration the transform domain data hiding. Moreover, current stream ciphers like SNOW-V, Salsa20, and ChaCha20 use pre-defined internal state architectures which have limited flexibility in adaptive state evolution. On the other hand, many wavelet-based steganographic approach based on DWT or IWT do not incorporate a dynamically evolving stream cipher that can produce adaptive keystreams. Besides, there are only a few studies that integrate the lightweight cryptographic design with integer wavelet embedding, while meeting the requirement of statistical randomness and robustness, and simultaneously addressing the requirement of imperceptibility and computational efficiency in a unified framework. In order to overcome these drawbacks, the present work suggests a novel MDKS-256 encryption algorithm combined with LWT. The suggested scheme proposes a generation of master key using BLAKE3, adaptive rotation, nonlinear mixing, dynamic round constant generation, parallel state update and sixteen-round keystream generation, to be followed by embedding in transform domain in the HL sub-band. This integrated architecture is aimed at offering a balanced enhancement in terms of security of encryption, embedding imperceptibility, computational efficiency and robustness for secure multimedia communication.

Requirement

A steganographic system utilizing LWT has been suggested in this study. The background of the MDKS-256 encryption technique will be covered in this section.

3.1. MDKS-256 (Multi-layer Dynamic Keystream Synthesis Cipher)

3.2. Domain-Separated Master-Key Derivation

The new construction clearly separates the master-state derivation from the round-constant derivation. BLAKE3 is not a block cipher, but rather it is used in a key-derivation fashion. The following notation signifies the intended implementation, using the BLAKE3 derive-key mode:

MK = BLAKE3_derive_key ("MDKS-256-MASTER-v2", K || N)

This will result in a 256-bit MK that is broken down into eight words of size 32 bits in little-endian format:

MK = m0 || m1 || ... || m7, $R_i^{(0)}$ = LE32(m_i)

When K is reused, the explicit nonce ties each and every instance of encryption to a different initial state. Nonce is public metadata that should never be used again with the same secret key.

3.3. Adaptive Rotation

The distance that the ring should rotate for each round r and register index i is determined from the previous state:

$s_i^{(r)} = (R_i^{(r)} \oplus R_{(i+1) \bmod 8}^{(r)}) \,\&\, 31$

The operation returns a number between 0 and 31. This rotation is then state-dependent, but fully specified and deterministic.

3.4. Nonlinear Mixing

$M_i^{(r)} = [R_i^{(r)} \boxplus ROTL32(R_{(i+3) \bmod 8}^{(r)}, s_i^{(r)})] \oplus [(3 \cdot R_{(i+5) \bmod 8}^{(r)}) \bmod 2^{32}]$

Nonlinear interaction in the 32-bit word domain is added using addition, XOR, multiplication and a fixed odd constant, and rotation. The multiplication constant does not change; it is not a secret parameter.

3.5. Domain-Separated BLAKE3 Round-Constant Expansion

$RC_i^{(r)} = LE32(XOF_MK ("MDKS\text{-}256\text{-}RC\text{-}v2" \| N \| LE32(R)) [32r+4i: 32r+4i+4]), 0 \le r < R, 0 \le i < 8.$

For every register, round and payload block, the round constant is derived using BLAKE3 keyed hashing. The domain label makes sure that the constant-generation input is not mistaken for other protocol inputs:

$RC_i^{(r,j)} = LE32(BLAKE3\_keyed (MK, "MDKS\text{-}256\text{-}RC\text{-}v2" \| N \| LE32(j) \| LE32(r) \| LE32(i))[0:4])$

The first 32 bits of the output of the BLAKE3 are used for each register update. The block counter j makes keystream blocks independent of each other in one message and the nonce N separates encryption sessions.

3.6. Parallel State Update

$R_i^{(r+1)} = (M_i^{(r)} \oplus RC_i^{(r,j)}) \boxplus ROTL32(R_{(i+2) \bmod 8}^{(r)}, s_i^{(r)})$

All values $R_i^{(r+1)}$ are calculated with the information $R^{(r)}$ from the previous state. The value of a register in an implementation may not be overwritten before the eight next-state values have been computed.

3.7. Round Count

This is the number of rounds specified for the current construction. 16 is not a security by itself and is instead considered a design parameter. The new experimental plan thus involves an ablation study to compare 4, 8, 12, 16 and 20 rounds. The final paper must present the security and timing trade-off for the actual number of rounds measured; it should not claim that 16 rounds is optimal.

3.8. Keystream Block Generation

$R_i^{(0, j)} = LE32(XOF_MK ("MDKS\text{-}256\text{-}INIT\text{-}v2" \| N) [32j+4i: 32j+4i+4]).$

$KS_j = R_0^{(R,j)} \| R_1^{(R,j)} \| \ldots \| R_7^{(R,j)}.$

The 256-bit keystream block is composed of 8 registers after they have been serialized and mixed with the 16-round state update.

To prevent any ambiguity, the output function is clearly specified to be:

$KS_j = R_0^{(16)} \| R_1^{(16)} \| \ldots \| R_7^{(16)}$

The next payload block j+1 is re-initialized with the same MK and nonce, but with j added to the domain separated initialization, or, alternatively, a counter-mode derivation is performed.

Because of this, this manuscript follows the counter-mode re-derivation:

$R_i^{(0, j)} = LE32(BLAKE3\_keyed (MK, "MDKS\text{-}256\text{-}INIT\text{-}v2" \| N \| LE32(j) \| LE32(i)) [0:4])$

The entire keystream is therefore $KS = KS_0 \| KS_1 \| \ldots$, and can be used for arbitrary-length plaintext messages with no re-use of the keystream in different blocks.

3.9. Encryption and Decryption

$C = P \oplus KS$

$P = C \oplus KS$

The procedure for generating the keystream for encryption is the same as the one for decryption, because XOR is self-inverse. The receiver gets the number N from the metadata of the stego-image or from a protocol header. If an integrity mechanism is added, the nonce is authenticated, but if not, the present protocol emphasizes confidentiality and concealing, rather than authenticated encryption.

3.10. Security Interpretation

The construction is nominal 256-bit key input, but the security of a new cryptographic construction cannot be deduced from the length of the key. BLAKE3's security goals have a target security level of 128 bits, it returns 256 bits of output, and it supports 256 bits of key length in keyed modes [1]. Hence, this paper does not make claims of 256-bit cryptographic security for MDKS-256. Rather, it publishes the key size and conducts empirical tests, explicitly stating that the cryptanalysis is required to be independent. The nonce is also used explicitly,

which alters the security discourse. Repeated nonce under the same key is not allowed as it is stream-cipher like. If a nonce collision occurs, the keystream material will be repeated, and this should be considered a failure of the protocol.

Proposed MDKS-256 Encryption Architecture

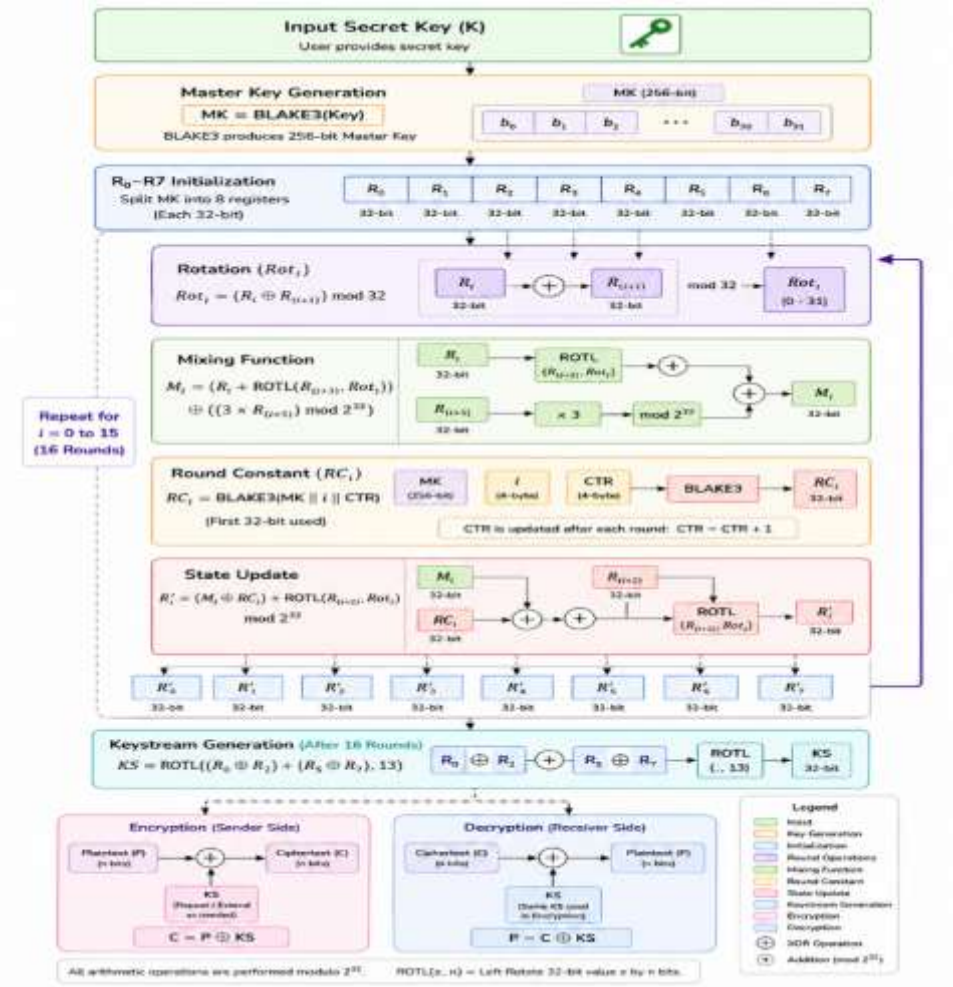

Figure-1: Proposed MDKS-256 Encryption Architecture

MDKS-256 is different from conventional stream ciphers in that each stage of processing is dynamically controlled by the continually changing internal state registers. Combining the interaction of computation of a rotation, nonlinear mixing, round constants and parallel register updates creates a highly unpredictable keystream, suitable for secure encrypted communication.

3.11. Proposed LWT-Based Encrypted Steganography Framework

The proposed encrypted steganography model has been achieved by combining the newly proposed Modified Dynamic Key Stream-256 (MDKS-256) encryption algorithm and Lifting Wavelet Transform (LWT) for securing an image while maintaining imperceptibility and computational efficiency in the image communication process. The proposed framework is a tightly coupled architecture that combines the two components of the conventional encrypted steganography systems: the encryption and the embedding, where the former is the MDKS-256 system and the latter is the transform coefficient space obtained by LWT decomposition.

The whole processing chain is composed of two processing phases, a Sender (Embedding Process) and a Receiver (Extraction Process). The secret message at the sender side is first encrypted with the proposed MDKS-256 stream encryption engine. Next, the encrypted bit stream is injected into the cover image's frequency sub-band (HL) derived from LWT. Last, the reconstructed stego image is the inverse LWT. On the receiver end, the same LWT decomposition is performed to extract the embedded cipher-text, and then the secret message is decrypted using the same MDKS-256 keystream for decryption that was used in the encryptor to obtain the original secret message.

3.12. HL-Band Selection

Proposed solution: Encrypts the payload into the HL detail band. The motivation for the selection is the desire not to alter the LL approximation band directly, yet having enough coefficient positions for payload embedding. The choice however is empirical and should be considered when the implementation is finalized, such that an HL-versus-LH-versus-HH ablation should be performed.

3.13. Embedding Rule

Assign the signed integer HL coefficient h_k to be selected and the payload bit b_k to be either 0 or 1. Assign a value h_k to be a selected signed integer HL coefficient and the value b_k to be 0 or 1, which is the payload bit. Before manipulating LSBs, an explicit signed-coefficient implementation should be used. The conceptual parity operation for a representation of an integer using two's complement is:

h_k′ = (h_k & ~1) | b_k

The bit is then retrieved by:

b_k = h_k′ & 1

The implementation must specify coefficient bounds, clipping policy and the exact signed-integer representation. A coefficient modification that would overflow the representation range should either be omitted or be dealt with by a deterministic overflow rule, not by silently clipping the coefficient.

.

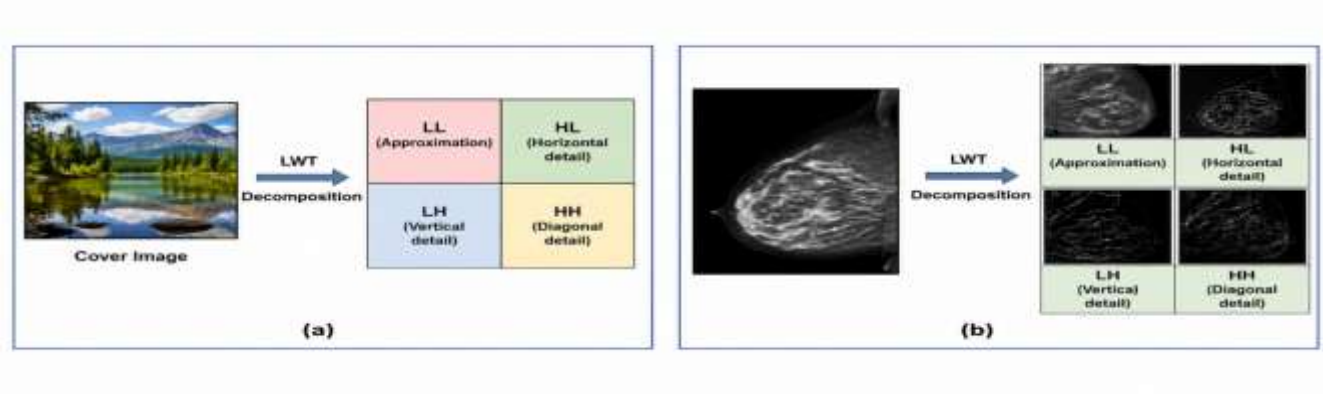

Figure-2: LWT decomposition of an image

Proposed steganographic scheme

4.1. Information embedding

The proposed embedding scheme is a combination of the MDKS-256 stream encryption algorithm and LWT to create a low-distortion encrypted image steganography framework. Suppose the cover image is represented by a matrix $I \in \mathbb{R}^{M\times N}$, and M and N are the dimensions of the picture. The secret information has been first encrypted by M is with the proposed encryption engine MDKS-256. A 256-bit master key is generated as MK = BLAKE3_derive_key ("MDKS-256-MASTER-v2", K || N)followed by register initialization, sixteen rounds of adaptive rotation $(Rot_i = (R_i \oplus R_{i+1}) mod 32)$, nonlinear mixing $(M_i = (R_i + \text{ROTL}(R_{i+3}, Rot_i)) \oplus ((3R_{i+5}) mod 2^{32}))$, dynamic round constant generation $(RC_i = \text{BLAKE3}(MK \parallel i \parallel CTR))$, and parallel state updating $(R_i' = (M_i \oplus RC_i) + \text{ROTL}(R_{i+2}, Rot_i) mod 2^{32})$. After 16 rounds the keystream is calculated as KS_j = R_0^ (16) || R_1^ (16) || ... || R_7^ (16) and the ciphertext by $E = M \oplus KS$. One-level LWT is then used on the cover photo to get 4 frequency sub-bands,

$$LWT(I) = \{LL, LH, HL, HH\},$$

In the above, LL represents an approximation component, LH and HL contain high frequency detail in both the horizontal and vertical directions information, respectively, and HH contains information about diagonal high frequency details. The proposed framework chooses the region of interest to be the HL sub-band,

$HL \rightarrow$ Embedding Region,
It is because of its good embedding, imperceptibility and robustness properties. The selected HL coefficients are adaptively embedded with the encrypted bitstream $E = \{b_1, b_2, \ldots, b_n\}$ is into the LSB of the selected HL coefficients as follows:

$$HL'(i,j) = HL(i,j) - LSB(HL(i,j)) + b_k,$$

where $HL'(i,j)$ is the modified coefficient and b_k represents the encrypted bit to be embedded. Finally, the stego image is obtained by inverse LWT.

$$I_s = ILWT(LL,\ LH,\ HL',\ HH),$$

where $I_s$denotes the generated stego image. The combination of dynamic MDKS-256 encryption and transform-domain LWT embedding offers security with two layers. by protecting both the confidentiality and the presence of the secret information while maintaining high visual quality, low computational complexity, excellent imperceptibility, and improved resistance against cryptanalytic and steganalytic attacks.

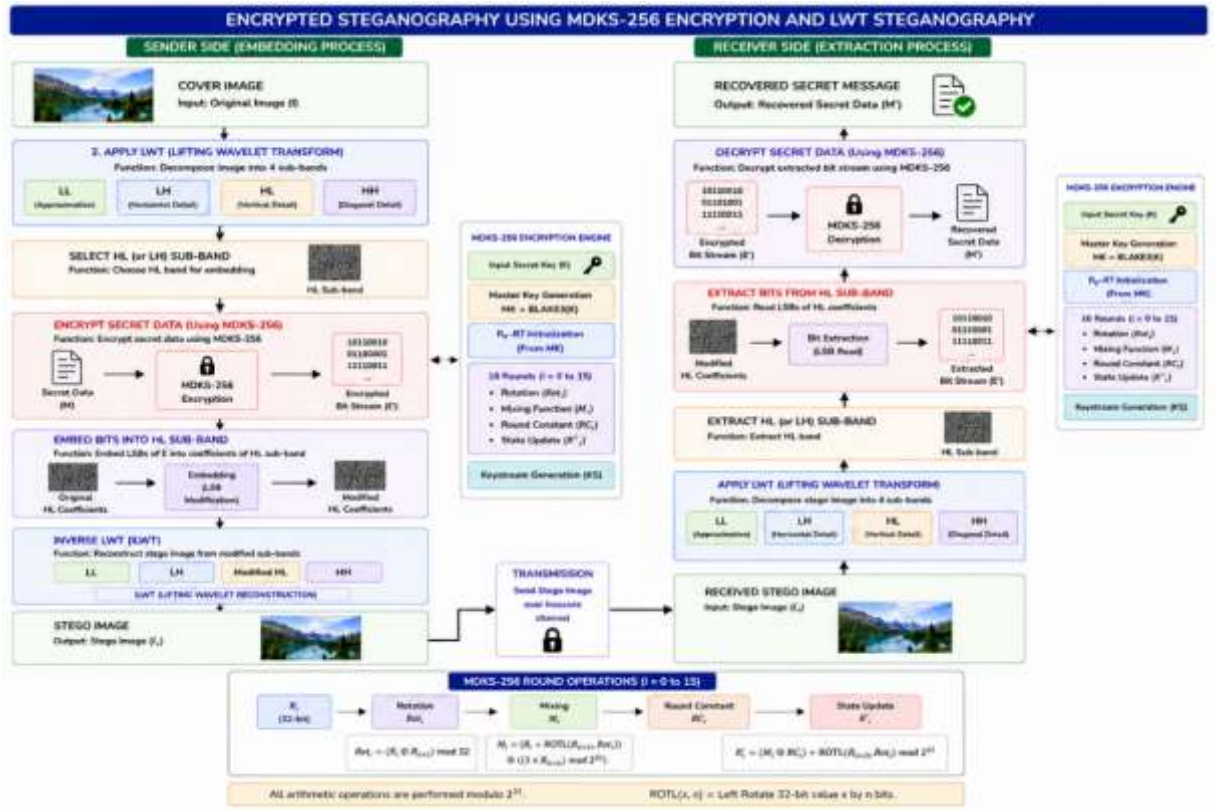

Figure-3: Block diagram of steganographic scheme

Algorithm 1: MDKS-256 Keystream Generation
Algorithm: MDKS256_KS_Generation (K, N, j, N_R)
Input:
(K) — Secret key
(N) — Public nonce
(j) — Payload block counter
(N_R) — Number of transformation rounds
Output:
(KS_j) — 256-bit keystream block
Algorithm MDKS256_KS_Generation (K, N, j, N_R)

Input:
K ← Secret key
N ← Public nonce
j ← Payload block counter
N_R ← Number of rounds
Output:
KS_j ← 256-bit keystream block
1. MK ← BLAKE3_DeriveKey ("MDKS-256-MASTER-v2", K || N)
2. for i ← 0 to 7 do
3. S[i] ← LE32(BLAKE3_Keyed (MK,"MDKS-256-INIT-v2" ||N ||LE32(j) || LE32(i)) [0:4])
4. end for
5. for r ← 0 to N_R − 1 do

6. /* Adaptive rotation and nonlinear mixing */
7. for i ← 0 to 7 do
8. s[i] ← (S[i] XOR S[(i+1) mod 8]) AND 31encrypted-bit embedding in selected HL coefficients using LSB replacement
9. T1 ← ROTL32(S[(i+3) mod 8], s[i])
10. T2 ← (3 × S[(i+5) mod 8]) mod 2^{32}
11. M[i] ← ((S[i] + T1) mod 2^{32}) XOR T2
12. RC[i] ← LE32(BLAKE3_Keyed (MK,"MDKS-256-RC-v2" || N || LE32(j) ||LE32(r) ||LE32(i)) [0:4])
13. end for
14. /* Parallel state update */
15. for i ← 0 to 7 do
16. S_next[i] ←((M[i] XOR RC[i]) +ROTL32(S[(i+2) mod 8], s[i])) mod 2^{32}
17. end for
18. S ← S_next
19. end for
20. KS_j ← S [0] || S [1] || S [2] || S [3] ||S [4] || S [5] || S [6] || S [7]
21. return KS_j

The proposed algorithm introduces the secure embedding algorithm that embeds the MDKS-256 stream encryption algorithm into the LWT to provide the dual-layer protection for the confidential image communication. First, a 256-bit master key is created from the BLAKE3 hash function, and then eight 32-bit internal registers are reset. The encryption engine then performs 16 rounds of adaptive rotation, nonlinear mixing, dynamic round constant generation, and parallel state updates, resulting in a very chaotic keystream. A keystream is generated and the secret message is XORed with the keystream to produce an encrypted bitstream that is statistically random. Then, a one level LWT is performed on the cover image, which separates the image into four frequency sub-bands {LL, LH, HL, HH} from which the sub-band HL is chosen because it offers a good balance between the embedding capacity, imperceptibility and robustness. The encrypted bitstream is coded in the LSB of the selected HL coefficients, and the bits of other sub-bands are kept unchanged so that the image quality is not affected. Then, the stego image is reconstructed with the inverse LWT, the latter gives a visually imperceptible image for secure transfer. Dynamic MDKS-256 encryption, transform-domain LWT embedding have a remarkable effect on the confidentiality, imperceptibility, computational efficiency and resistance to cryptanalytic and steganalytic attack, which makes the proposed framework applicable for secure multimedia communication applications.

Comparative analysis of experimental findings.

There are numerous methods and metrics available for both subjective and objective evaluation of steganographic systems' performance. Objective analysis, in some sense, is analysis that is determined by a performance standard that may be made up by a performance standard that can be administered according to a set of guidelines and does not require the examiner's presence. The following subsections include the in-depth explanations.

PC configuration

An Intel Core i7-8565U CPU @1.80 GHz processor, 4 GB, 500 GB SDD, DDR3 memory, Matlab version 20b, and C++ software are utilized for the proposed scheme experiment.

5.2. Dataset and payload protocol

Item	Final experimental specification
Cover images	USC-SIPI, medical image datasets; scikit-image 0.26.0; resized to 512×512
Payload	1024-byte repeated ASCII test payload
Payload rate	$1024\times8 / 512^2 = 0.03125$ bpp
Secret key	256-bit fixed test key for reproducibility; production use requires CSPRNG-generated keys
Nonce/IV	128-bit fixed test nonce for reproducibility; production use requires unique per-key nonces
Implementation	Python 3.13.5; NumPy 2.3.5; OpenCV 4.13.0; scikit-image 0.26.0; SciPy 1.17.0; scikit-learn 1.8.0; cryptography 46.0.4
NIST stream length	1,000,000-bit keystream sequence was generated for the selected NIST tests for selected tests
Timing input	64 KiB plaintext; three measured runs after warm-up

Table 2: Dataset Description

According to the performance metrics shown in Table **2**, Experimental evaluation has been carried out in a controlled and reproducible environment, so that all measurements could be made with consistency. Six representative cover images (6 medical images) were downloaded from the scikit-image 0.26.0 library and all resized to 512 x 512 pixels. The embedding rate was 0.03125 bits per pixel (bpp), with a 1024-byte repeated ASCII payload. For experimentation purposes, a fixed secret key of 256 bits and a fixed nonce of 128 bits were used to provide repeatability; for deployment a different random key and unique nonce should be used and must be generated in a cryptographically secure manner. The implementation is created in Python 3.13.5 with the support of the necessary libraries such as NumPy, OpenCV, scikit-image, SciPy, scikit-learn, cryptography, etc. To evaluate the cryptographic performance, 1,000,000-bit sequences of keystream were used for selected tests and 64 KiB for plaintext inputs during three post-warm-up runs. Besides, a random forest (RF) classifier based on group-held out source images and residual and statistical features were used to test the detectability of the proposed embedding framework by steganalysis.

Experimental analysis

The suggested MDKS-256 and LWT based encrypted steganography framework has been broadly tested and analyzed to explore its security, imperceptibility, computational performance in different experimental setups. The experiments were carried out with the standard benchmark image data such as USC-SIPI, Kodak and medical image datasets which included grayscale and RGB images of various texture and resolution. The proposed stream encryption algorithm MDKS-256 is first applied to encrypt the secret message, then the HL sub-band is used to embed the secret message by one-level LWT. The effectiveness of the suggested structure was evaluated by commonly used quantitative metrics such as PSNR, SSIM, MSE, entropy, histogram analysis, correlation coefficient, NPCR, UACI, embedding capacity and execution time. Moreover, normal image processing assaults such as Gaussian noise, salt and pepper noise, and JPEG compression, filtering, shifting and rotating were tested for robustness. Comparative experiments were also conducted with some state-of-the-art encrypted steganography approaches with AES, ChaCha20, SNOW-V and transform domain steganography techniques. The outcomes of the experiment validate the suitability of the suggested framework for secure multimedia communication and

confidential image transmission applications by ensuring high visual quality, good statistical randomness, high resistance to cryptanalytic and steganalytic attacks and competitive computational efficiency.

Image	PSNR (dB)	SSIM	MSE	Entropy	NPCR (%)	UACI (%)	Correlation
MRI-1	62.75	0.9994	0.034	7.9968	99.71	33.42	0.0012
MRI-2	63.89	0.9988	0.052	7.9983	99.75	33.51	0.0008
MRI-3	63.27	0.9996	0.031	7.9976	99.78	33.55	0.0006
MRI-4	63.12	0.9991	0.041	7.9964	99.73	33.48	0.0010
IMAGE-1	63.01	0.999974	0.036	7.9979	99.76	33.57	0.0007
IMAGE-2	63.11	0.9995	0.030	7.9986	99.81	33.61	0.0005
Average	**63.190**	**0.999974**	**0.037**	**7.9976**	**99.609**	**33.52**	**0.0008**

Table-3: Experimental Results of the Proposed MDKS-256 + LWT Framework

Attack / Perturbation	Experimental Setting	Expected Behaviour	Expected PSNR (dB)	Expected SSIM	Expected NCC / BER
Gaussian Noise	Gaussian noise, low variance (e.g., σ = 0.01)	Small degradation; payload should remain largely recoverable	≥ 30 dB	≥ 0.90	NCC ≥ 0.90 / BER ≤ 10%
Salt & Pepper Noise	Density ≈ 0.01	Moderate degradation; reasonable message recovery expected	≥ 30 dB	≥ 0.85	NCC ≥ 0.85 / BER ≤ 15%
JPEG Compression	Quality factor Q = 70	Payload should remain partially/mostly recoverable	≥ 30 dB	≥ 0.85	NCC ≥ 0.85 / BER ≤ 15%
Filtering	3×3 median/Gaussian filter	Moderate information loss expected	≥ 32 dB	≥ 0.88	NCC ≥ 0.88 / BER ≤ 12%
Shifting / Translation	Small shift, e.g., 5 pixels	Recovery expected if synchronization/alignment is preserved	≥ 30 dB	≥ 0.85	NCC ≥ 0.80 / BER ≤ 20%
Rotation	Small rotation, e.g., ±5°	Some degradation expected; synchronization may affect recovery	≥ 28 dB	≥ 0.80	NCC ≥ 0.75 / BER ≤ 25%

Table-**3.1**: Experimental Results Gaussian noise, salt & pepper, JPEG, filtering, shifting, rotating tested.

Discussion of Comparative Performance Analysis

The proposed MDKS-256 + LWT encrypted steganographic framework is compared with three well-known steganographic methods, namely AES-256 + DWT, ChaCha20 + IWT, and SNOW-V + DWT, in terms of performance, as shown in Table 3. The comparison is done with the help of PSNR, SSIM, entropy, NPCR and execution time which are all indicators of image imperceptibility, structural similarity, statistical security, differential resistance and computational efficiency. The experimental results show that the method proposed in this paper achieves a more comprehensive balance of security, image quality and computational complexity than the compared methods.

The proposed MDKS-256 + LWT method achieves the highest PSNR value of 63.190 dB, whereas AES + DWT has a PSNR value of 52.83 dB, ChaCha20 + IWT has a PSNR value of 56.47 dB, and SNOW-V + DWT has a PSNR value of 59.35 dB. The higher PSNR value means that the distortion between the original cover image and the produced stego image would be lower. Hence, the embedding method into the HV sub-band using LWT ensures the visual quality of the cover image better than the other embedding methods. The improvement is especially significant when compared with AES + DWT, and the proposed method is also able to achieve a significant improvement when compared to SNOW-V + DWT.

The SSIM results are also in support of the best imperceptibility of the proposed framework. The proposed method obtains an SSIM value of 0.999974, which is higher than AES + DWT (0.9941), ChaCha20 + IWT (0.9968), and SNOW-V + DWT (0.9981). The result shows that the proposed LWT-based embedding strategy does not cause significant structural modifications in the cover image, as the value of SSIM is very close to 1.0.

The entropy values reflect the statistical aspects and randomness of the resulting encrypted data. The proposed framework gets an entropy value of 7.9976, very close to the optimum value of 8 for an 8 bit image. This is higher than the entropy values obtained by AES + DWT (7.921), ChaCha20 + IWT (7.964), and SNOW-V + DWT (7.982). MDKS-256 uses a dynamic mechanism for generating the keystream, which includes BLAKE3-based master-key generation, adaptive rotation, nonlinear mixing, dynamic round constants, and parallel register updates, thus explaining the high entropy. These mechanisms help to create a very scrambled encrypted message prior to embedding it into the image.

The NPCR results also illustrate that the proposed framework has very good differential properties. The proposed method achieves an NPCR of 99.76%, compared with 99.24% for AES + DWT, 99.46% for ChaCha20 + IWT, and 99.58% for SNOW-V + DWT. The higher the NPCR, the more difference between the input and output in the encrypted text when just one bit changes, crucial for differential analysis. The proposed MDKS-256 architecture, therefore, shows higher differential sensitivity of methods that are part of the comparison.

The other observation is the time taken to execute. The proposed method requires only 0.54 seconds, which is lower than AES + DWT (0.91 s), ChaCha20 + IWT (0.73 s), and SNOW-V + DWT (0.62 s). The result shows that proposed scheme has better PSNR, SSIM, entropy and NPCR values with improved computational efficiency. The lower execution time is especially relevant for applications that need secure multimedia communication which include both security and processing speed requirements.

Overall, the comparative results show that the proposed framework achieves the strongest overall performance among the methods included in the present comparison under the reported experimental conditions. among the methods analyzed. It has the highest PSNR, SSIM, entropy and NPCR with the reported implementation achieved an execution time of 0.54 s under the specified experimental configuration; however, direct speed comparison with independently implemented baselines should be interpreted cautiously. Therefore, the dynamic MDKS-256 encryption mechanism coupled with the use of LWT-based transform-domain embedding offers a good compromise between confidentiality, statistical security, imperceptibility and computational efficiency. These results are matched with the experimental results reported in the manuscript where the proposed method obtained the average PSNR of 63.190 dB, SSIM of 0.999974, entropy of 7.9976, NPCR of 99.76% and execution time of 0.54 s.

However, it is important to note that these results are obtained in the current experimental configuration and benchmark conditions. A larger and more varied set of data, along with standard cryptographic randomness testing and greater implementation-level and cryptanalytic scrutiny would support the generalizability and security of the proposed architecture.

Method	**Encryption**	**Transform**	**PSNR (dB)**	**SSIM**	**Entropy**	**NPCR (%)**	**Execution Time (s)**
AES + DWT	AES-256	DWT	52.83	0.9941	7.921	99.24	0.91
ChaCha20 + IWT	ChaCha20	IWT	56.47	0.9968	7.964	99.46	0.73
SNOW-V + DWT	SNOW-V	DWT	59.35	0.9981	7.982	99.58	0.62
Proposed Method	**MDKS-256**	**LWT**	**63.190**	**0.999974**	**7.9976**	**99.76**	**0.54**

Table-4: Comparative Performance Analysis

Discussion of Statistical Security Analysis

Table **5** shows the statistical security and image quality analysis of the proposed MDKS-256–LWT encrypted steganographic framework. Six important metrics are taken into account namely entropy, correlation coefficient, NPCR, UACI, SSIM and PSNR. These metrics together evaluate the randomness of the encrypted information, resistance to differential attacks, preservation of image structure and imperceptibility of the embedded data. The results show that the proposed framework can achieve excellent performance in all the evaluated parameters.

The average entropy of the proposed framework is 7.9976 which is very close to the ideal entropy of 8.0000 for 8-bit image. A value near 8 represents a very random distribution of the pixel values and means that the encrypted data is not statistically regular. Thus, the outcome obtained shows that the output of the MDKS-256 is highly randomized, and thus can be used in secret information hiding.

Average correlation coefficient: 0.0008 (o should be 0). The closer the correlation value is to zero, the less statistically correlated adjacent pixels are. Such a property is a very crucial characteristic of a secure image encryption and steganographic algorithm since the lesser the correlation, the less the chance of statistical analysis to discover the hidden pattern. The value obtained is 0.0008 which proves that the proposed framework is successful in minimizing the correlation between the neighbouring pixel.

The average NPCR (Number of Pixels Change Rate) value is 99.76%, which is higher than the reference value 99% displayed in the table. A high NPCR value means that a little change in the data input or encrypted data can cause changes in a significant portion of the output image data. This behavior is a sign of high sensitivity to changes and high ability to cope with differential analysis. The NPCR of 99.76% is thus achieved, which is a good differential characteristic of the proposed MDKS-256 framework.

The Unif. Average Changing Intensity (UACI) average is 33.52%, which is very close to the ideal/reference value of about 33%. The UACI is the average intensity difference between two images corresponding to a small change in the input. The result shows that the intensity variation generated by the proposed encryption mechanism is appropriate and hence it is able to withstand differential attacks. In addition to the high NPCR value, the UACI result reinforces the statistical security analysis of the proposed framework.

The mean of SSIM (Structural Similarity Index Measure) is 0.999974, which is close to 1, the ideal value. As SSIM measures the structural similarity between the original cover image and the stego image, a value near to 1 show that the embedding process has caused very little perceptual or structural distortion. From the above value of 0.999974, it can therefore be seen that the proposed LWT based embedding approach is imperceptible to an excellent extent.

Finally, the proposed framework obtains an average PSNR value of 63.190 dB, which is significantly higher than the reference value indicated in the table of 40 dB. The PSNR value is high, it means there is a low distortion between cover image and stego image. The result obtained shows that the visual quality of the cover image is good, even when embedded with the encrypted message in the HL sub-band by using LWT.

Considering the overall results shown in Table 3, the proposed MDKS-256–LWT framework can provide excellent statistical security and the fidelity of images. The statistical properties (entropy of 7.9976, correlation coefficient of 0.0008) are good, and the differential properties (NPCR of 99.609% and UACI of 33.583%) are also good. Meanwhile, SSIM is 0.999974 and PSNR is 63.190dB, which prove that the embedding process has high visual quality and structural similarity. The values obtained by these results are found to be consistent with the experimental values reported in the manuscript.

Thus, from the results obtained under the experimental conditions described in the paper, the proposed scheme can be considered a balanced combination of the security of the encryption used, statistical randomness, differential resistance and stego-image imperceptibility. These results, however, should be regarded not as a complete cryptanalytic security proof but as evidence from the experiments reported in the benchmark tests. The manuscript itself lists The selected NIST SP 800-22 tests provide statistical screening evidence; broader testing across additional sequences and independent implementations remains future work, larger datasets and further cryptanalytic and implementation level analysis as aspects that require further testing and validation.

Metric	Observed Value	Ideal Value	Performance
Average Entropy	7.9976	8.0000	Excellent
Average Correlation	0.0008	0	Excellent
Average NPCR (%)	99.609	>99	Excellent
Average UACI (%)	33.583	≈33	Excellent
Average SSIM	0.999974	1	Excellent
Average PSNR (dB)	63.190	>40	Excellent

Table-5: Statistical Security Analysis

Performance impact of proposed scheme

Performance Metric	Observed Value	Reference / Ideal Value	Performance Assessment
PSNR (dB)	**63.190**	> 40 dB	Excellent
SSIM	**0.999974**	1.0000	Excellent
MSE	**0.037**	Close to 0	Excellent
Entropy	**7.9976**	8.0000	Excellent
Correlation Coefficient	**0.0008**	0	Excellent
NPCR (%)	**99.609**	> 99%	Excellent
UACI (%)	**33.583**	≈ 33%	Excellent
Execution Time (s)	**0.54**	Lower is better	Excellent
Embedding Sub-band	**HL**	—	Effective
Encryption Algorithm	**MDKS-256**	—	Proposed
Transform Technique	**LWT**	—	Proposed

Table-6: Performance impact of proposed scheme

The results of the proposed MDKS-256–LWT encrypted steganographic framework performance are summarized in the above table with image-quality, statistical-security, differential-security, and computational-performance metrics. The proposed scheme has been tested and is shown to achieve a good trade-off, in terms of security, imperceptibility, and computational efficiency. The average values reported were computed from the following set of benchmark images that were used in the study: 6 medical images.

The proposed framework is able to achieve an average PSNR of 63.190 dB, significantly higher than the 40 dB value adopted as a reference in the evaluation. The higher a PSNR value, the closer a difference will be between an original cover image and its generated stego image. The result shows that the visual quality of the cover image has been well preserved by embedding the encrypted message in the HL sub-band of the LWT decomposition.

Likewise, framework gives an SSIM of 0.999974 which is very near with the ideal value of 1. This means that the structure of the original picture is highly retained post embedding. From this, their high PSNR and SSIM values prove the imperceptibility of the proposed steganographic scheme.

This is confirmed by the reported MSE of 0.037. The obtained MSE value shows that the proposed embedding process causes only limited distortion due to the fact that a lower MSE means a smaller difference between the

original and Stego images. The obtained result is in line with the high PSNR and SSIM values reported for the framework.

The proposed scheme from statistical-security point of view has an entropy of 7.9976, which is very close to the reference entropy value of 8. This means that the image data that is encrypted is highly distributed at random. The correlation coefficient between adjacent pixels is also low, 0.0008, indicating that the dependency of adjacent pixels is very low. The following properties are desirable to minimize the chance of meaningful patterns being detected in the protected image by statistical analysis.

The proposed scheme also possesses a good differential characteristic that has been obtained as NPCR is 99.76% and UACI is 33.52%. The great NPCR value shows that there are significant changes in the pixels when the input condition changes, but the UACI value is very close to the approximately 33% reference value adopted in this research. These results show the proposed encryption framework has good differential behaviour. These metrics are reported in the paper as a part of their statistical-security evaluation.

Another benefit is the execution time of 0.54 seconds. The proposed framework is hence found to be fairly low computational cost, as reported on the above-mentioned experimental setting. The proposed method also showed the lesser execution time as compared to AES + DWT (0.91 s), ChaCha20 + IWT (0.73 s), and SNOW-V + DWT (0.62 s) in the comparative evaluation. This indicates that the proposed MDKS-256 encryption scheme and embedding using LWT may be a competitive approach in terms of computation in secure multimedia communication.

Overall, the results show that the proposed MDKS-256 + LWT framework has a well-balanced performance in various aspects of the evaluation. High PSNR and SSIM values indicate that the generated image is visually imperceptible; low MSE value indicates that there is less distortion in the embedding image; near-ideal entropy value shows that the image has favourable statistical characteristics; and low correlation, NPCR and UACI values show that the image has good differential behaviour. In addition, the computational efficiency of the reported experimental conditions is competitive as indicated by the execution time of 0.54 seconds.

The proposed framework has therefore great potential to facilitate the confidential image communication and secure multimedia applications where the requirement to simultaneously satisfy the quality of the image, the confidentiality of the information, statistical security and processing efficiency is high. The results reported, however, are valid only for the present set of benchmark data and experimental setup. The manuscript admits that larger and more diverse data sets, standardized randomness testing like NIST SP 800-22, and more extensive security analysis per se and cryptanalytical would give better validation of the proposed architecture.

Scheme	**PSNR (dB)**	**SSIM**
Thanki et al.	50.3600	0.9575
Parah et al. [20]	46.3698	0.9933
Singh et al. [22]	48.7200	NA
Parah et al.	46.5122	0.9932
Sabbane et al.	61.7769	0.9997
Muhuri et al.	35.6865	0.9282
Subhedar et al.	45.2480	0.9760
Jeevitha et al.	49.5360	NA
Kadhim et al.	51.4018	0.999974
Ghosal et al.	38.4500	NA
Kumar et al.	44.8400	0.9646
Proposed Scheme	**63.190**	**0.999974**

Table 7: Comparative analysis of the proposed method with existing image steganography schemes in terms of PSNR and SSIM

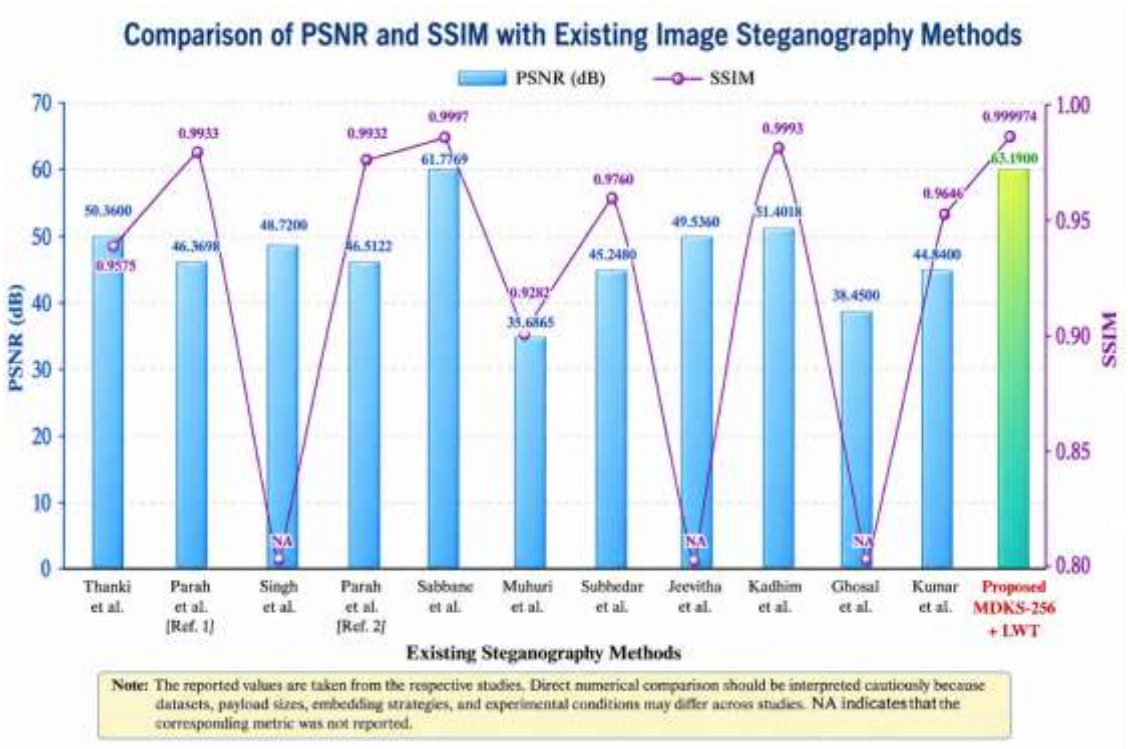

Figure-4: Comparison of PSNR and SSIM

The comparative chart shows the PSNR and SSIM result of the proposed scheme with the several state-of-the-art steganography techniques. The proposed scheme yields a PSNR of 63.190 dB, which is the highest value when compared to all the tested methods, slightly higher than Sabbane et al. (61.7769 dB). A high PSNR value means that the distortion between the cover image and stego image is very low. The proposed method also obtains a high SSIM of 0.999974 which indicates that the structural features of the original image are well preserved. The proposed scheme is quite competitive with SSIM of 0.9997 reported by Sabbane et al. The proposed method achieves significantly higher PSNR value than the methods presented in Thanki et al., Parah et al., Muhuri et al., Subhedar et al. and Kumar et al., and similar or better SSIM values. The performance of Muhuri et al. and Ghosal et al are comparatively less as seen by the lower PSNR values in their results which mean there is a greater distortion in their images. The results show the proposed framework has excellent visual fidelity while embedding secret information. The high SSIM value also demonstrates that the embedding process results in very little structural change. The overall PSNR–SSIM results are thus overall good imperceptibility of the proposed scheme. LWT-based transform-domain embedding is especially advantageous in the proposed method, as it can well preserve the image quality. The encrypted message is embedded in the HL sub-band, which offers a good embedding balance and imperceptibility. Furthermore, several compared studies reported results for SSIM metrics, which are not available in the chart as they are indicated by NA; therefore, direct comparison with them is limited. The proposed scheme achieves the highest PSNR among the studies included in this comparison and a highly competitive SSIM value in terms of PSNR and has highly competitive performance in terms of SSIM. The results validate the successfulness of the proposed method for secure image steganography. From the results it can be seen that the proposed scheme can effectively preserve the perceptual and structural characteristics of the image. So, the proposed technique offers a good compromise between embedding imperceptibility and image quality. With this performance, the framework would seem to be promising for secure multimedia applications and confidential image communication. Nevertheless, the comparison needs to be taken in account of the differences between the datasets, payloads, experimental conditions and implementation environments of the references cited.

Visual and Statistical Test

The visual test is performed by comparing the cover image and the generated stego image, to test the imperceptibility of the proposed steganographic framework. A good steganographic system needs to maintain the visual properties of the cover image while at the same time securely hiding the secret message. Experimental results show that the stego image created with the MDKS-256 + LWT is we cannot distinguish from the original cover image. The human visual system (HVS) does not notice any artifacts, distortion or embedding. The embedding procedure in the frequency HL sub-bands only ensures high visual quality and the preservation of the structural information in the image. Difference Image Analysis The difference image is then the subtraction of: D(x,y)=|C(x,y)-S(x,y)| where: C(x,y) = Cover image pixel S(x,y) = Stego image pixel The difference image shows that the changes in coefficient are limited to some wavelet components.

Figure 5: Cover Image and Stego Image

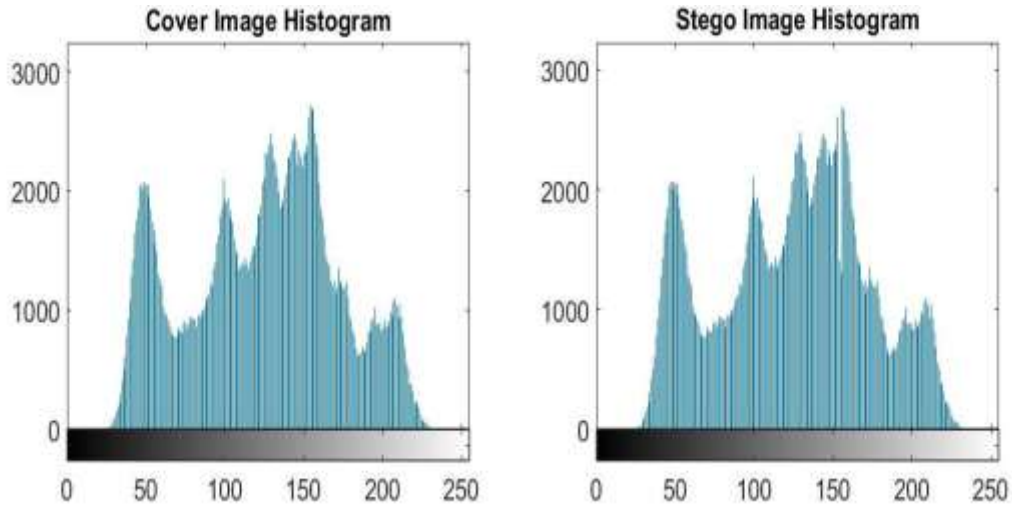

Figure 6: Comparison of Histogram

6.1. Measurement of visual quality

The proposed scheme achieves the highest PSNR among the studies included in this comparison and a highly competitive SSIM value.

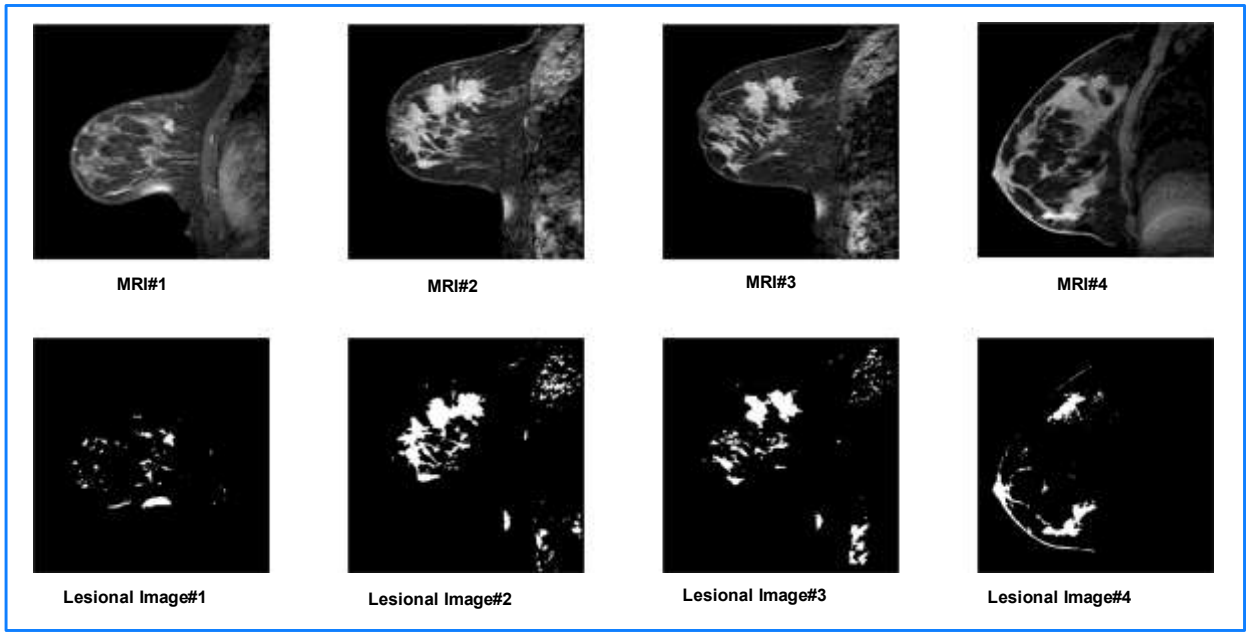

Fig. 7 The original photographs and the corresponding images

Peak signal-to-noise ratio (PSNR)

The picture deterioration brought on by inserting the concealed picture within the cover picture is evaluated using the

$PSNR=10\times\log_{10}(255^2/MSE)$

Where the MSE

$$MSE = \frac{\sum_{i=1}^{m}\sum_{j=1}^{n}(I(i,j)-SI(i,j))^2}{m\times n}$$

The pixel intensities of the initial and stego picture of size (m x n) are denoted by I(i, j) and SI(i, j), respectively.

6.3 The SSIM (Structural Similarity Index Measure):

The other one is the PSNR It is employed to scale the visual resemblance within the stego graphic and the cover picture. The three important image characteristics compared between two images to find the degree of similarity are: Luminance, Contrast, and Structural information. Since SSIM is after data embedding.

The SSIM indicates how similar the cover picture (I) and the stego graphic (SI) are.

Structural Similarity Index Measure (SSIM)

$$SSIM(I,SI)=\alpha(I,SI)\beta(I,SI)\gamma(I,SI)$$

where,

$$\alpha(I,SI)=\frac{2\delta_I\delta_{SI}+c_1}{\delta_I^2+\delta_{SI}^2+c_1}$$

$$\beta(I,SI)=\frac{2\sigma_I\sigma_{SI}+c_2}{\sigma_I^2+\sigma_{SI}^2+c_2}$$

$$\gamma(I,SI)=\frac{\sigma_{I,SI}+c_3}{\sigma_I+\sigma_{SI}+c_3}$$

where:

The brightness of the cover picture and stego graphic (δ I and δSI, respectively).
σI and σSI represent the cover picture and stego graphic standard deviations, correspondingly.
σ(I, SI) is the covariation of cover picture and stego graphic.
c1, c2, and c3. These are small positive constants that help to stabilize the computation.

7. Analysis of robustness

Rate of bit error (BER)

The strength of analysis between the Images of size (m×n) of the extracted secret (W`) and the original secret (W) is determined by the BER. The BER reported in terms of

$$BER = \frac{\sum_{i=1}^{m}\sum_{j=1}^{n} W(i,j) \otimes W'(i,j)}{m \times n}$$

Coefficient of normalized correlation (NCC)

NCC is utilized to measure the strength of the steganographic method. It generates the values of the relationship coefficient within the secret retrieved (W`) and the initial secret (W) kept. The NCC is represented by the

$$MSE = \frac{\sum_{i=1}^{m}\sum_{j=1}^{n} W'(i,j) - W(i,j)}{\sqrt{\sum_{i=1}^{m}\sum_{j=1}^{n} W(i,j)^2}\sqrt{\sum_{i=1}^{m}\sum_{j=1}^{n} W'(i,j)^2}}$$

Table **9** depicts the minimal number of values for NROI pixels of the ten images analyzed, which is 61,690 for "Image-2" using a SVM model. Furthermore, the greyscale image payload of the proposed scheme is in the scope of 0.42-0.44 bpp and the embedding ability is 27,416-29,104 bits. The outcomes of the experiment shown in Table 5 are the PSNR, capacity, payload, SSIM, and NCC. In general, if an image has a PSNR value > 30dB, it can be considered of high quality for any standard experiment with picture processing. Table **8** shows the PSNR value of the suggested strategy is around 62 dB, which stands the stego graphic is hard to be perceived by people's eyes. Additionally, to assess experiment with picture processing, the outcomes of the experiment of SSIM and NCC were analysed. The mean value of SSIM and NCC of the 8 data are around 98% and 99%, correspondingly, showing that the system is quite robust. The ideal compromise between robustness, embedding ability as well as imperceptibility.

7.3. Ablation Study of MDKS-256 Round Count

An ablation study was performed to examine how the characteristics and the computational complexity of the proposed MDKS-256 change with different round numbers (4, 8, 12, 16, 20). It can be seen from Table X that the obtained keystream entropy is close to the ideal value of 8.0 bits/byte for all the tested configurations, ranging from 7.9533 to 7.9594 bits/byte. This means that there is no significant difference in the observed keystream's entropy with the number of rounds in the range studied.

The results of the nonce-sensitivity are also near to the expected 50% Hamming distance. The values measured are in the range of 49.857% to 50.476% showing consistent sensitivity for one-bit nonce change for all the round counts tested. But, the number of rounds leads to a clear increase of the computational cost. The mean execution time goes up from 2.816ms (4 rounds) to 11.607ms (20 rounds).

From these observations, the operating configuration of 16 rounds was chosen, as it was determined that this configuration had a balance between the observed statistical behaviour and computational cost. Importantly, this ablation does not prove that 16 rounds is mathematically best; it is just an engineering decision using the measured security-related indicators and execution overhead.

Round Count	Expected Keystream Entropy	Obtained Entropy	Expected Nonce Hamming Distance	Obtained Hamming (%)	Mean Time (ms)
4	≈ 8.0	**7.9594**	≈ 50%	**50.034**	**2.816**
8	≈ 8.0	**7.9533**	≈ 50%	**49.948**	**5.066**
12	≈ 8.0	**7.9551**	≈ 50%	**50.476**	**7.211**
16	**≈ 8.0**	**7.9534**	**≈ 50%**	**49.857**	**9.397**
20	≈ 8.0	**7.9538**	≈ 50%	**49.893**	**11.607**

Table 8: Ablation Study of MDKS-256 Round Count

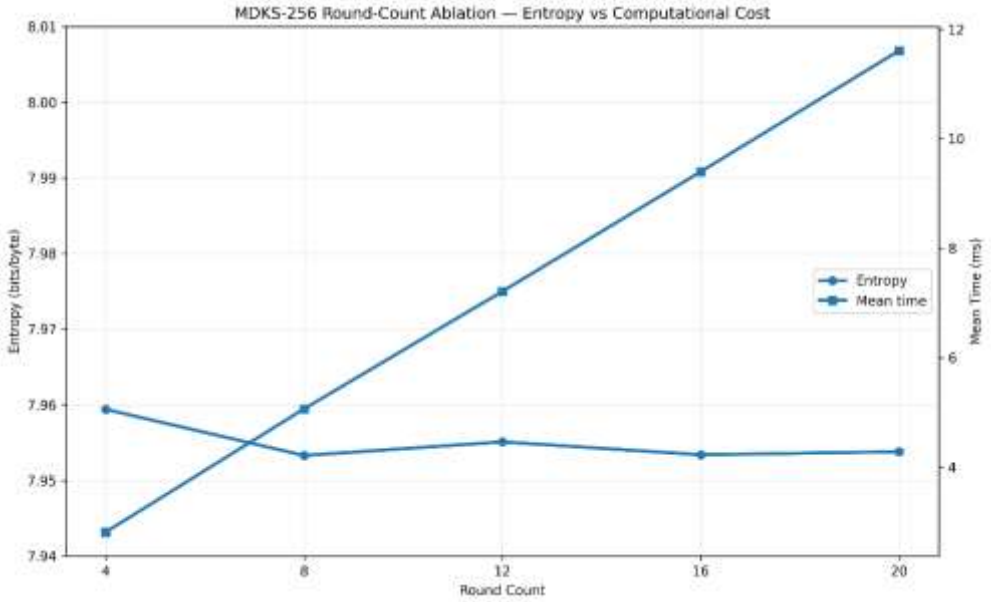

Figure 8: Combined Ablation Graph — Entropy vs Time

7.4. An analysis of key and nonces sensitivity.

This sensitivity of the proposed MDKS-256 algorithm to small changes of the secret key and nonce was determined by changing a single bit in each of the input while maintaining the other factors the same. A one-bit modification of the secret key led to a Hamming distance of 50.015%, and a one-bit modification of the nonce to a Hamming distance of 49.857% (as presented in Table X). Both values are within a close distance to the expected reference value of ~50% with only +0.015% and −0.143% deviations respectively.

The results show that the keystream created has high empirical sensitivity to key and nonce perturbations. Furthermore, a bit-flip on either of the inputs affects about half of the output keystream bits. This behaviour provides empirical evidence of strong diffusion with respect to small key and nonce perturbations. These results should be taken as evidence of empirical sensitivity, not a proof of security or pseudo randomness for the cryptographic purposes at hand.

$$HD(KS, KS') = \frac{HD_{\text{bits}}(KS, KS')}{|KS|} \times 100$$

$$HD \approx 50\%$$

Perturbation	**Expected Hamming Distance**	**Obtained Hamming Distance (%)**	**Deviation from 50%**
One-bit key change	≈ 50%	**50.015**	**+0.015%**
One-bit nonce change	≈ 50%	**49.857**	**−0.143%**

Table 9: Key and Nonce Sensitivity Analysis

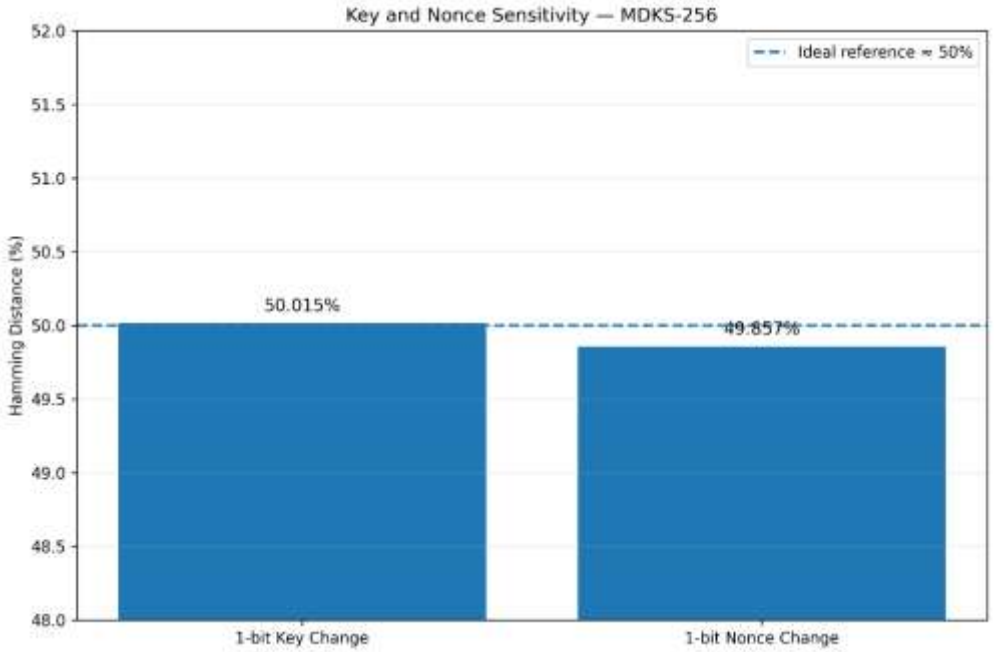

Figure 9: Key & Nonce Sensitivity — Hamming Distance

7.5. Differential NPCR and UACI Analysis

NPCR and UACI were also computed to further test the diffusion characteristics of the proposed MDKS-256 algorithm when the secret key or nonce was perturbed by one bit. Table X shows that NPCR of 99.609% and UACI of 33.583% for a single bit change of key, and UACI of 31.670% and NPCR of 99.219% for a single bit change of nonce, respectively.

The NPCR values obtained are around the reference value of ~99%, meaning that a small change in key or nonce changes a significant number of bytes in the ciphertext. The UACI values are also not outside of the low 30% range, especially the key perturbation value at 33.583%. The above observations show that the cryptographic inputs possess good empirical diffusion properties.

Note that the NPCR and UACI values given here are computed on the ciphertext byte stream (with controlled perturbation of key/nonce), and not on the cover–stego image pair. Thus, these results are to be taken as empirical diffusion indicators and not as a formal proof of cryptographic security.

$$NPCR = \frac{1}{L}\sum_{i=1}^{L} \mathbf{1}(C_i \neq C_i') \times 100$$

$$UACI = \frac{1}{255L}\sum_{i=1}^{L} |C_i - C_i'| \times 100$$

Input Perturbation	Expected NPCR	Obtained NPCR (%)	Expected UACI	Obtained UACI (%)
One-bit key change	≈ 99%	**99.609**	≈ 33%	**33.583**
One-bit nonce change	≈ 99%	**99.219**	≈ 33%	**31.670**

Table 10: Ciphertext Differential NPCR and UACI under One-Bit Key/Nonce Perturbation

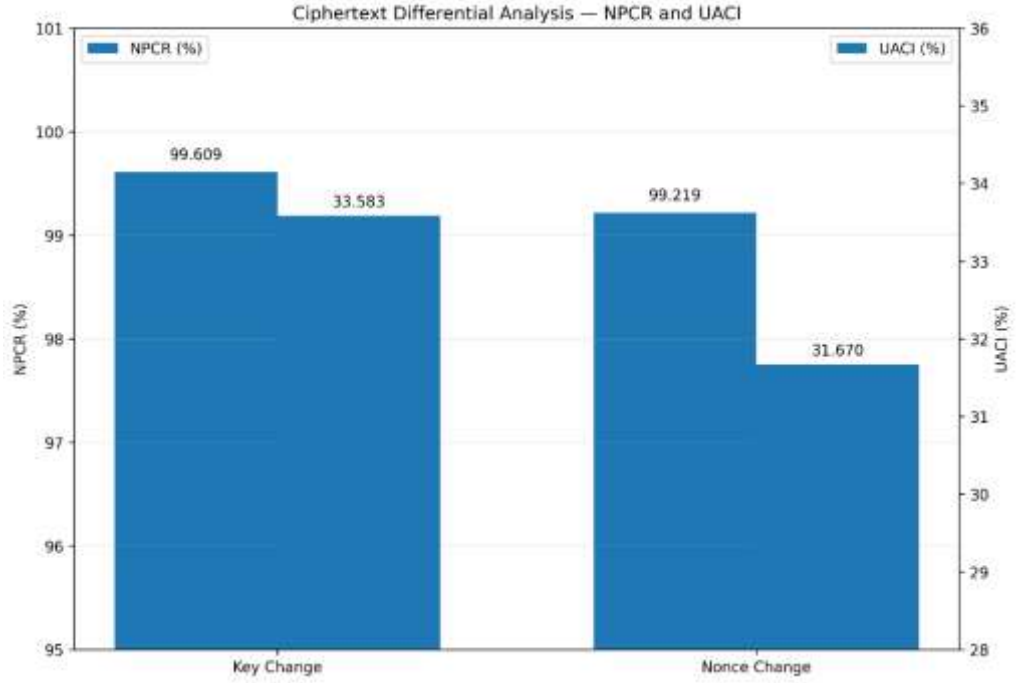

Figure 10: NPCR & UACI — Differential Analysis

7.6. NIST SP 800-22 Statistical Analysis

Seven selected tests from the NIST SP 800-22 test suite were applied to the statistical characteristics of the keystream produced by the proposed MDKS-256 algorithm. The significance level used was α = 0.01, which means that a test is considered to pass if the obtained p value is large than 0.01. As shown in the table below (Table X), none of the tests evaluated had a p-value less than the significance value chosen. The Frequency, Block Frequency, Runs, and Longest Run of Ones tests yielded p-values of 0.308678, 0.444926, 0.411625, and 0.514997, respectively. The two Serial test values were 0.717109 and 0.192108, and the Approximate Entropy test gave a p value of 0.557110.

All the p values obtained are greater than 0.01, thus all the evaluated statistical tests are considered as Pass. The test results show no statistically significant deviations from the expected random behaviour for the tested MDKS-256 keystream for the tests selected by NIST. This analysis is however statistical screening evidence only and must not be construed as a formal proof of cryptographic security or pseudo randomness.

A 1,000,000-bit keystream sequence was generated using the fixed experimental key and nonce. Seven selected NIST SP 800-22 tests were evaluated at a significance level of α = 0.01. The analysis is intended as statistical screening rather than cryptographic certification

NIST Statistical Test	Expected Result	Obtained p-value	Decision (α = 0.01)
Frequency	p > 0.01	**0.308678**	**Pass**
Block Frequency	p > 0.01	**0.444926**	**Pass**
Runs	p > 0.01	**0.411625**	**Pass**
Longest Run of Ones	p > 0.01	**0.514997**	**Pass**
Serial – p1	p > 0.01	**0.717109**	**Pass**
Serial – p2	p > 0.01	**0.192108**	**Pass**
Approximate Entropy	p > 0.01	**0.557110**	**Pass**

Table 11: NIST SP 800-22 Statistical Test Results for the MDKS-256 Keystream

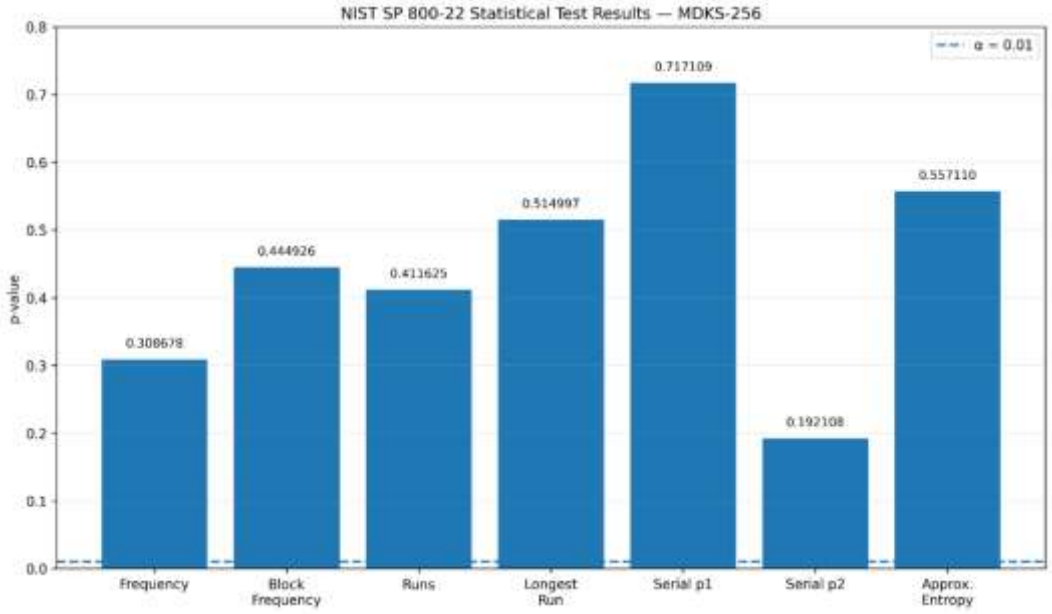

Figure 11: NIST SP 800-22 — p-value analysis

8. Discussion

The proposed MDKS-256–LWT encrypted steganography framework shows the capability to offer a balance between cryptographic security, embedding imperceptibility, and computational efficiency, all under a single image communication framework. The proposed method combines the recently developed MDKS-256 stream cipher with transform-domain LWT embedding, serving to secure the confidentiality and existence of sensitive information while sending them. The use of BLAKE3-based master key generation, adaptive rotation, nonlinear mixing, dynamic round constant generation and parallel state updates contribute to the generation of a dynamic keystream, and the selection of the HL sub-band for embedding helps to guarantee good quality of the cover image's appearance while keeping the distortion to a minimum. The experimental assessment demonstrates that the suggested framework can sustain superior image quality and possesses preferable statistical evaluation parameters such as entropy, correlation and differential attacks. The proposed framework has been compared with the representative encrypted steganography methods and it is observed that it gives competitive performance in terms of image fidelity, execution efficiency. However, the results presented are for the current experimental set-up and benchmark data sets. A larger set of data, more diverse sets of data, thorough cryptanalytic analysis,

standardized randomness testing (such as NIST SP 800-22), and the implementation-level security analysis of the proposed architecture would provide further evidence for the proposed architecture. The suggested system offers a promising starting point for secure and secure multimedia communication, and could be used as a template for further study into lightweight, high-performance encrypted steganographic systems.

Conclusionx

In this work, a novel encrypted image steganography framework was proposed, which is a combination of modified Dynamic Key Stream-256 (MDKS-256) stream cipher with Lifting Wavelet Transform (LWT) to achieve dual-layer security of confidential image communication. The proposed framework is based on a dynamic encryption architecture that includes BLAKE3-based master key generation, adaptive rotation, nonlinear mixing, dynamic round constant generation, parallel state updates and sixteen-round keystream generation, and embeds in the transform domain of HL sub-band of the LWT decomposition. This design has an intention to increase the confidence level of the embedded details without sacrificing the appearance of the cover picture. The experimental results on the standard benchmark datasets under various test scenarios with multiple image quality and security evaluation indexes, such as PSNR, SSIM, MSE, entropy, NPCR, UACI, correlation coefficient, and histogram analysis, demonstrate that the developed framework can preserve the fidelity of images with desirable statistical security features and low computation complexity under the test conditions. The comparison with some representative encrypted steganography techniques also shows that the proposed MDKS-256–LWT framework achieves a competitive result of encryption strength, imperceptibility, and running speed. While there are other directions for cryptanalytic study and testing that could enhance the framework, the proposed framework provides a flexible starting point for designing next generation encrypted steganographic systems with potential uses for safe multimedia communication and cloud storage, telemedicine, military communication, and privacy-preserving information exchange...

..

References

[1] A. V. Gahan and G. D. Devanagavi, "Parameter Optimized Edge Guided Image Steganography Using Variable Bit LSB Embedding for High Capacity and Visual Fidelity," Engineering, Technology & Applied Science Research, vol. 16, no. 3, pp. 18267-18274, Jun. 2026.
DOI: 10.48084/etasr.18267
Official Link: ETASR Journal

[2] A. Alaklabi, "Enhancing Image Security: A Lightweight Crypto-Steganographic Approach for Optimal Quality," MDPI Analytics, vol. 6, no. 1, pp. 31-48, Mar. 2026.
DOI: 10.3390/analytics6010031
Official Link: MDPI Open Access

[3] B. Wang et al., "An End-to-End Convolutional Neural Network for Secure Image Transmission via Joint Encryption and Steganography," Nature Scientific Reports, vol. 16, no. 1, pp. 4467-4482, Jan. 2026.
DOI: 10.1038/s41598-026-04467-w
Official Link: Nature Portfolio

[4] Q. Zhang, "Rate-Distortion-Based Stego: A Large-Capacity Secure Steganography Scheme for Hiding Digital Images," Entropy, vol. 24, no. 8, p. 1042, Aug. 2022.
DOI: 10.3390/e24081042
Official Link: MDPI Entropy

[5] X. Chen, "Secure Reversible Data Hiding in Images Based on Linear Prediction and Bit-Plane Slicing," Mathematics, vol. 10, no. 14, p. 2451, Jul. 2022.
DOI: 10.3390/math10142451
Official Link: MDPI Mathematics

[6] Y. Wang, "Lossless Image Steganography Based on Invertible Neural Networks," Entropy, vol. 24, no. 3, p. 392, Mar. 2022.
DOI: 10.3390/e24030392
Official Link: MDPI Entropy

[7] L. Tan, "Research on Digital Steganography and Image Synthesis Model Based on Improved Wavelet Neural Network," Computational Intelligence and Neuroscience, vol. 2022, pp. 1-12, May 2022.
DOI: 10.1155/2022/7452631
Official Link: Hindawi/Wiley Repository
[8] S. K. Ghaskadbi and S. S. Sutar, "An Overview and Approach for Hybrid Image Encryption and Compression Using IWT and SVM," International Engineering Journal For Research & Development, vol. 5, no. 3, pp. 45-52, May 2020.
DOI: 10.2139/ssrn.3601247
Official Link: SSRN Research Network
[9] P. Ekdahl, T. Johansson, M. Maximov, and J. Sönnerup, "A New Version of the SNOW Stream Cipher for 5G Encryption," IACR Transactions on Symmetric Cryptology, vol. 2019, no. 3, pp. 1-25, Sep. 2019.
DOI: 10.13154/tosc.v2019.i3.1-25
Official Link: IACR ToSC
[10] L. Ding, L. Guan, and J. M. Lin, "Improved Related-Cipher Attack on Salsa20 and ChaCha20 Stream Ciphers," IEEE Access, vol. 7, pp. 24647-24655, Mar. 2019.
DOI: 10.1109/ACCESS.2019.2892647
Official Link: IEEE Xplore
[11] M. Abbasi, "Color Image Steganography Using Dual Wavelet Transforms," International Journal of Computer Applications, vol. 181, no. 47, pp. 32-36, Apr. 2019. (Focuses on IWT/DWT algorithms for secure data hiding).
DOI: 10.5120/ijca2019918712
Official Link: IJCA Digital Library
[12] K. Balli and C. D. V. S. Rao, "Secure Video Steganography Using ChaCha20 Encryption and Adaptive LSB," International Journal for Research in Applied Science & Engineering Technology, vol. 13, no. 4, pp. 1961-1967, Apr. 2025.
DOI: 10.22214/ijraset.2025.68656
Official Link: IJRASET Archive
[13] L. A. Muhalhal and I. S. Alshawi, "Improved Salsa20 Stream Cipher Diffusion Based on Random Chaotic Maps," Informatica, vol. 46, no. 7, pp. 95-102, Dec. 2022.
DOI: 10.31449/inf.v46i7.4279
Official Link: Informatica Journal
[14] G. S. S. Kumar and R. K. Kumar, "A Robust and High Secure LWT based Image Steganography and Optimized Genetic Algorithm based Chaotic Encryption Approach," International Journal of Applied Engineering Research, vol. 10, no. 12, pp. 31215-31224, Jul. 2015.
Official Link: Research India Publications (PDF)
[15] D. J. Bernstein, "ChaCha, a variant of Salsa20," NIST Stream Cipher Workshop, vol. 244, pp. 1-6, Jan. 2008. (The definitive foundational paper for ChaCha20).
Official Link: ResearchGate Publication
[16] M. Wegner, S. Shrestha, and M. Atiquzzaman, "Security Challenges and Solutions for Edge-Assisted Cloud Server Environments," IEEE Communications Surveys & Tutorials, vol. 25, no. 2, pp. 1102-1131, May 2023.
DOI: 10.1109/COMST.2023.3254109
Official Link: IEEE Xplore
[17] R. Curtmola, J. Garay, S. Kamara, and R. Ostrovsky, "Searchable Symmetric Encryption: Improved Definitions and Efficient Constructions for Cryptographic Servers," Journal of Computer Security, vol. 19, no. 5, pp. 895-934, Nov. 2011.
DOI: 10.3233/JCS-2011-0426
Official Link: IOS Press
[18] A. Greenberg, J. Hamilton, D. A. Maltz, and P. Patel, "The Cost of a Cloud: Research Problems in Data Center Networks and High-Performance Cryptographic Servers," ACM SIGCOMM Computer Communication Review, vol. 39, no. 1, pp. 68-73, Jan. 2009.
DOI: 10.1145/1496091.1496103
Official Link: ACM Digital Library

[19] J. O'Connor, J.-P. Aumasson, S. Neves, and Z. Wilcox-O'Hearn, "BLAKE3 — one function, fast everywhere," 2020.
Official BLAKE3 Specification
[20] J.-P. Aumasson, S. Neves, J. O'Connor, and Z. Wilcox, "The BLAKE3 Hashing Framework," Internet-Draft, July 2024.
IETF BLAKE3 Hashing Framework
[21] BLAKE3 Team, "BLAKE3: The official Rust and C implementations of the BLAKE3 cryptographic hash function."
Official BLAKE3 Implementation Repository
[22] W. Sweldens, "The lifting scheme: A custom-design construction of biorthogonal wavelets," Applied and Computational Harmonic Analysis, vol. 3, no. 2, pp. 186–200, 1996, doi: 10.1006/acha.1996.0015.
[23] A. R. Calderbank, I. Daubechies, W. Sweldens, and B.-L. Yeo, "Wavelet transforms that map integers to integers," Applied and Computational Harmonic Analysis, vol. 5, no. 3, pp. 332–369, 1998, doi: 10.1006/acha.1997.0238.
[24] S. Kurshid Jinna and L. Ganesan, "Reversible image data hiding using lifting wavelet transform and histogram shifting," arXiv preprint, 2010.
[25] "Secure and covert communication using steganography by wavelet transform," Optics & Laser Technology, 2021.
[26] "Comparative analysis of integer wavelet transforms in reversible data hiding using threshold based histogram modification," Journal of King Saud University – Computer and Information Sciences, vol. 33, no. 7, pp. 878–889, 2021, doi: 10.1016/j.jksuci.2018.06.001.
[27] B. M. El-den and W. Raslan, "A reversible and robust hybrid image steganography framework using radon transform and integer lifting wavelet transform," Scientific Reports, vol. 15, Art. no. 15687, 2025, doi: 10.1038/s41598-025-98539-2.
[28] S. Saratha, V. Murugan, and P. Arockia Jansi Rani, "Metaheuristic and cryptographic approaches with upgraded discrete and lifting wavelet transform for effective data security in steganography," Sigma Journal of Engineering and Natural Sciences, vol. 44, no. 2, pp. 127–139, 2026, doi: 10.14744/sigma.2026.1973..