Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 28 (2025), No. 5-B, pp. 1855–1864
DOI : 10.47974/JDMSC-2418

Secure communication framework using lattice-based encryption and image steganography

Ashok Kumar Saini [@]
Department of Computer Science and Engineering
Manipal University Jaipur
Jaipur 303007
Rajasthan
India

Madan Lal Saini [†]
Department of Apex- Computer Science and Engineering
Chandigarh University
Mohali 140413
Punjab
India

Devesh Kumar Srivastava [§]
Department of Information Technology
Manipal University Jaipur
Jaipur 303007
Rajasthan
India

Sandeep Singh [‡]
Department of Computer Science and Engineering
SGT University
Gurugram 122505
Haryana
India

[@] *E-mail:* ashok.saini@jaipur.manipal.edu
[†] *E-mail:* mlsaini@gmail.com
[§] *E-mail:* devesh.srivastava@jaipur.manipal.edu
[‡] *E-mail:* sandeep_feat@sgtuniversity.org

© Taru Publications

Prashant Vats*
Department of Computer Science and Engineering
Manipal University Jaipur
Jaipur 303007
Rajasthan
India

Tan Kuan Tak #
Department of Engineering Research Cluster
Singapore Institute of Technology
Singapore 138683
Singapore

Abstract

Ensuring secure communication in modern digital networks is crucial to safeguarding sensitive information. This paper presents a novel framework that combines lattice-based encryption with image steganography to enhance data security and confidentiality. Lattice-based encryption offers strong resistance against quantum computing attacks, making it a robust choice for cryptographic security. Meanwhile, image steganography effectively conceals encrypted data within multimedia content, adding a layer of protection. The proposed framework leverages mathematical principles to optimize encryption strength while minimizing distortion in the steganographic process.

Subject Classification: *Primary 94A60, Secondary 68P25.*

Keywords: *Lattice-based encryption, Image steganography, Secure communication, Cryptographic security, Data protection, Secure digital transformation, Data integrity, Network security, Smart cities, E-governance, IoT security, Sustainable innovation (SDG 9).*

1. Introduction

The exponential growth in digital communication has transformed global connectivity, enabling rapid information exchange across industries. While this digital expansion has facilitated seamless collaboration, it has also introduced significant risks to data security. Cyber threats, including data interception, unauthorized access, and tampering, have emerged as critical challenges for organizations worldwide. With the growing adoption of technologies such as cloud computing, IoT networks, and smart infrastructure, safeguarding sensitive data against evolving security threats is paramount. Traditional encryption algorithms like AES, RSA, and ECC have been widely employed to protect data confidentiality and integrity. However, these methods are increasingly vulnerable to emerging attack vectors, particularly those enabled by

* *E-mail:* **prashant.vats@jaipur.manipal.edu (Corresponding Author)**
# *E-mail:* **kuantak.tan@singaporetech.edu.sg**

advancements in quantum computing. Quantum computers leverage their inherent ability to solve complex mathematical problems at unprecedented speeds, rendering many conventional encryption methods ineffective. As a result, there is a pressing need to explore advanced cryptographic techniques that offer enhanced security against both classical and quantum threats.

Lattice-based encryption has emerged as a promising solution due to its inherent resistance to quantum attacks. It leverages complex mathematical structures built on high-dimensional lattices, where encryption security is derived from the difficulty of solving lattice-based problems such as the Shortest Vector Problem (SVP) and the Learning with Errors (LWE) problem. These problems are computationally intractable for both classical and quantum adversaries, making lattice-based encryption a robust candidate for next-generation cryptographic systems. At the receiver's end, the embedded ciphertext is extracted from the image and decrypted using the recipient's private key, ensuring secure data recovery. The remainder of this paper is structured as follows: Section 2 discusses related work in encryption and steganography techniques. Section 3 outlines the proposed framework, detailing the integration of lattice-based encryption with image steganography. Section 4 presents experimental results and performance evaluation. Finally, Section 5 concludes the paper with future research directions.

2. Related Work

Aparna and Madhumitha [1] have presented their work on the combined Image Encryption and Steganography Technique for Enhanced Security. This study introduces a dual-layer encryption approach utilizing DNA cryptography, followed by embedding the encrypted image into a cover image using steganographic methods.

Mohades, Kadkhoda, and Mohades, [2] have proposed their work on the application of the Löwner-John Ellipsoid in the Steganography of Lattice Vectors. This research presents a novel method for transmitting secret information by embedding lattice vectors within cover media.

Kurniawan and Satrya [3] have presented their work on analyzing Futuristic ID Cards using Lattice-Based Cryptography along with the Steganographic algorithm. This work proposes a secure identity card system that combines lattice-based cryptographic schemes with digital steganography. Li, Ng, and Purcell [4] proposed their work on Homomorphic Encryption used in Lattice-Based Cryptography and thus provided an investigative overview by elucidating the principles of lattice-based cryptography, emphasizing its applications in constructing homomorphic encryption schemes. The work underscores the relevance of lattice problems in developing secure cryptographic protocols resistant to quantum attacks.

Raiyan and Kabir [5] proposed the Screed Solo framework, integrating random shuffling, symmetric encryption, and error correction coding to enhance the robustness and security of LSB-based image steganography. This approach

is designed to improve the resilience of embedded data against diverse attack scenarios.

Johnson and Vijayakumar [6] have proposed their work on Image Steganography Combined with Cryptography, where there is an infinite delay in the Helper asymmetrical unbiased stochastic integral-differential structures. Rajan and Ganesh [7] proposed their work on the Random RC4 Encrypting and Dynamic Pixel shuffling for Hash LSB Steganography, essentially by proposing a novel framework that integrates dynamic pixel shuffling, hash-based LSB steganography, and RC4 encryption.

Wang, Xu, and Yu [8] have proposed their work on Lattice-Based Cryptography by offering a comprehensive survey. This paper reviews the state-of-the-art lattice-based cryptographic schemes.

3. Proposed Work

In this research, we propose a Secure Communication Framework that integrates Lattice-Based Encryption (LBE) with Image Steganography to ensure robust and secure data transmission.

3.1 *Key Generation using Lattice-Based Cryptography*

The framework begins with the generation of cryptographic keys using Lattice-Based Encryption (LBE) techniques such as NTRU (Nth Degree Truncated Polynomial Ring) Encryption [9]. These encryption mechanisms provide high security against quantum computing attacks, making them suitable for next-generation secure communication.

NTRU Key Generation → Given $f(x)$ *and* $g(x)$be random polynomials where:

$$f(x) = \sum_{i=0}^{N-1} a_i x^i , g(x) = \sum_{i=0}^{N-1} b_i x^i \quad (1)$$

where $ai, bi \in -1,0,1$

Generate the Public Key h(x)

$$h(x) = \frac{1}{f(x)} \cdot g(x) \ modq \quad (2)$$

The public key is h(x), which is derived from the random polynomials f(x) and g(x).

In lattice-based encryption, key exchange protocols such as Kyber and Frodo enable secure communication by allowing both parties to generate key pairs and exchange public keys over an insecure channel [10, 11]. Each party then computes a shared secret using their private key and the other's public key [12]. In the NTRU scheme, the public key is defined by Equation (2).

Kyber (Module-LWE Based Key Exchange)

Choose→ public matrix A from a predefined distribution.
Generate→ small secret key s and an error vector e.
Compute the public key→ p=A·s+e
The public key is (A,p), and the secret key is s.
Define parameters→

Prime modulus q
Polynomial ring:
Rq= $\boldsymbol{Zq[x]/(x^n+1)}$*;* $\forall$ *Dimension* $\in$ *k, where k*$\rightarrow$*2k for Kyber-768.*
Secret key s and error term e are sampled from a discrete Gaussian distribution χ*.*

$$\boldsymbol{\chi k = i = 1 \sum k(bi - bi')}$$

Generate$\rightarrow$*public random matrix A,*

$$\boldsymbol{A \in Zqn \times m},$$

A $\forall$ *sampled using a cryptographic PRF;*

$$\text{PRF} \rightarrow \boldsymbol{F}: \{\boldsymbol{0,1}\}\boldsymbol{n} \times \{\boldsymbol{0,1}\}\boldsymbol{m} \rightarrow \{\boldsymbol{0,1}\}\boldsymbol{m}$$

$$\boldsymbol{PRFExpansion \rightarrow Ai,j = H\big(seed,(i,j)\big)}.$$

So the Public Key Equation $\rightarrow \boldsymbol{t = A \cdot s + emodq}$
Sample the secret key and error vector:

$$s,\ e \leftarrow \chi k$$

Compute the public key polynomial:

$$t = A \cdot s + e \bmod q$$

where:

- *A is the public random matrix.*
- *S is the private key polynomial.*
- *E is the error term ensuring security.*

Final public and private keys:
Public key$\rightarrow (\boldsymbol{A,t})$; $\boldsymbol{Private\ Key = s}$
Private Key$\rightarrow \boldsymbol{B = A \cdot S + Emodq}$

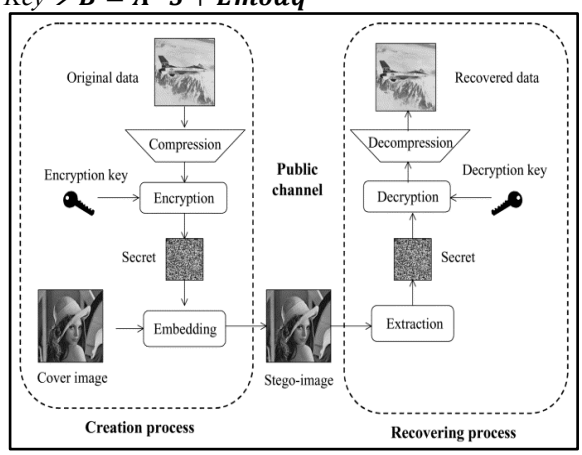

Figure 1
Public-Private Key Generation and Usage in Lattice-Based Encryption

3.2 *Data Encryption*

Once the cryptographic keys are generated, the confidential message is encrypted using Lattice-Based Encryption to ensure its security before embedding it into an image. The encryption process transforms the plaintext message into an unintelligible ciphertext, preventing unauthorized access. This step adds a layer of security, ensuring that even if the hidden data is detected, it remains unreadable without the decryption key. Figure 1 illustrates the process of public-private key generation in lattice-based encryption, where the public key is used for encryption, and the private key is securely kept for decryption at the receiver's end.

$\boldsymbol{Z_q}$*: integers modulo q*

$A \in \boldsymbol{Z_q^{n*m}}$*: public matrix*

$S \in \boldsymbol{Z_q^n}$ *: secret key*

$e \in \boldsymbol{Z_q^m}$*: small error vector*

$b = \boldsymbol{A^T}.\boldsymbol{S} + \boldsymbol{e}$*: public key*

Encryption

For message $\boldsymbol{m} \in \{\boldsymbol{0}, \boldsymbol{1}\}\boldsymbol{m}$ *:* $\boldsymbol{EncA}, \boldsymbol{b}(\boldsymbol{m}) = \left(\boldsymbol{u} = \boldsymbol{A} \cdot \boldsymbol{r},\ \boldsymbol{v} = \boldsymbol{b} \cdot \boldsymbol{r} + \left\lfloor \frac{\boldsymbol{q}}{\boldsymbol{2}} \right\rfloor \cdot \boldsymbol{m}\right)$

Where:

$$\boldsymbol{r} \in \boldsymbol{0}, \boldsymbol{1}\boldsymbol{m}: \boldsymbol{random\ binary\ vector}$$

Decryption → $\boldsymbol{v} - \boldsymbol{sT} \cdot \boldsymbol{u} = \lfloor \boldsymbol{q/2} \rfloor \cdot \boldsymbol{m} + (\boldsymbol{noise})$

recover m by rounding.

3.3 *Image-Based Steganographic Embedding*

The encrypted message is then embedded into a cover image using a steganographic technique. We utilize Least Significant Bit (LSB) steganography, Discrete Wavelet Transform (DWT), or a combination of both to ensure minimal image distortion while maintaining high security. To enhance robustness, a chaotic encryption scheme such as the Arnold Cat Map is applied before embedding, providing a random and secure distribution of data within the image.

$\boldsymbol{I}(\boldsymbol{x}, \boldsymbol{y})$: $\boldsymbol{intensityvalueofpixelat}(\boldsymbol{x}, \boldsymbol{y})$

$\boldsymbol{Mi}$: $\boldsymbol{i^{th}\ bit\ of\ message}$

$\boldsymbol{LSB}\big(\boldsymbol{I}(\boldsymbol{x}, \boldsymbol{y})\big)$: $\boldsymbol{leastsignificantbitofthepixel}$

$\boldsymbol{B^k}$ **be the** $\boldsymbol{k^{th}}$ **bit of the binary representation of** $\boldsymbol{I}(\boldsymbol{i}, \boldsymbol{j})$,

such that: → *I(i,j)=* $\sum_{k=0}^{T} \boldsymbol{B^k}.\boldsymbol{2^k}$

$\boldsymbol{M}(\boldsymbol{n}) \in \boldsymbol{0}, \boldsymbol{1}\boldsymbol{bethen^{th}bitofthemessagebitstreamtohide}.$

$\boldsymbol{I}{\sim}(\boldsymbol{i}, \boldsymbol{j})\boldsymbol{bethestegopixelvalueafterembedding}.$

Embedding Single Bit LSB $\boldsymbol{B_0}$ *with the message bit M(n):* →

$$\boldsymbol{I}{\sim}(\boldsymbol{i}, \boldsymbol{j}) = (\boldsymbol{I}(\boldsymbol{i}, \boldsymbol{j})\boldsymbol{AND254})\boldsymbol{ORM}(\boldsymbol{n})$$

For embedding r LSBs → $\boldsymbol{I}{\sim}(\boldsymbol{i}, \boldsymbol{j}) = \big(\boldsymbol{I}(\boldsymbol{i}, \boldsymbol{j})\boldsymbol{AND}(\boldsymbol{255} \ll \boldsymbol{r} \gg \boldsymbol{r})\big)\boldsymbol{ORMr}(\boldsymbol{n})$

Where $\boldsymbol{Mr}(\boldsymbol{n})$ → *Mr(n)* ∈ *{0,1,…,2r−1} be the r-bit chunk of the message.*

3.4 *Transmission Over an Insecure Channel*

After embedding the encrypted message, the stego image is transmitted over an insecure communication channel such as the internet or wireless networks. Since the message is embedded within an image, it appears as normal image data, making it difficult for adversaries to detect the presence of hidden information.

Given
$\boldsymbol{C \rightarrow cover\ image}$,
$\boldsymbol{M \rightarrow message\ bits}$,
$\boldsymbol{S = Embed(C, M) be\ the\ stego\ image}$,
$\boldsymbol{M' = Extract(S) be\ the\ extracted\ message\ at\ the\ receiver'send}$.

$$S = C \oplus E(M) \xrightarrow{\text{Insucure Channe}} M' = D(S)$$

Where:
$\boldsymbol{E(M)}$: $\boldsymbol{embedding\ function}$ ($\boldsymbol{LSB\ embedding}$),
$\boldsymbol{D(S)}$: $\boldsymbol{extraction\ function}$.

3.5 *Data Extraction and Decryption*

At the receiver's end, the stego image undergoes steganographic extraction, where the hidden data is retrieved using the corresponding extraction algorithm. The extracted ciphertext is then decrypted using the private key from the lattice-based cryptographic scheme, restoring the original message.

$$\boldsymbol{C = Extract(S)}$$
$$\boldsymbol{C = (x, y) \cup (S(x, y) mod 2)}$$

Decryption Equation:

$$\boldsymbol{v - sT \cdot u = \lfloor q/2 \rfloor \cdot m + e}$$

Where *e* is small noise. Now, recover *m* using:

$$\boldsymbol{m = Round(\lfloor q/2 \rfloor v - sT \cdot u)}$$

Combined (Extraction + Decryption) → $\boldsymbol{m = Decrypt(Extract(S), s) = Round(\lfloor q/2 \rfloor v - sT \cdot u)}$.

4. Experimental Results.

To evaluate the proposed Secure Communication Framework based on Lattice-Based Encryption (LBE) and Image Steganography (IS), a prototype was developed using Python. The experimental setup consisted of a machine running Windows 10 on an Intel Core i7-11800H processor with 16 GB RAM. In the encryption phase, plaintext messages were transformed into ciphertext using the LWE scheme. The encryption parameters included a public matrix $A \in Zqm \times nA$, where q=1024q = 1024q=1024, n=512n = 512n=512, and m=1024m = 1024m=1024. A secret key $s \in Zqn$ was randomly generated to ensure cryptographic strength. The given table 1 shows the Performance Evaluation of

Lattice-Based Encryption with Image Steganography for Secure Communication.

Table 1

Performance Evaluation of Lattice-Based Encryption with Image Steganography for Secure Communication

Metric	Grayscale Image	Color Image
Encryption Time (avg)	2.13 seconds	2.15 seconds
Decryption Time (avg)	3.38 seconds	3.41 seconds
Payload Capacity	512 bits	1024 bits
PSNR	48.21 dB	45.67 dB
Message Retrieval Accuracy	100%	100%
Security Strength	High	High
Standard Deviation (Time)	±0.04 sec	±0.05 sec

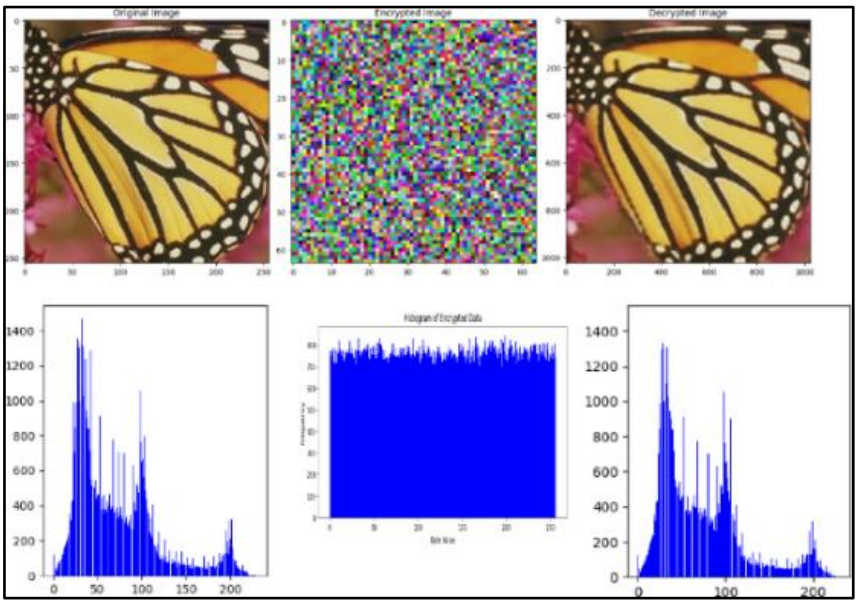

Figure 2

Lattice-Based Encryption Algorithm Leveraging Optimized 3D Chaotic Maps for Secure Image Communication

The decrypted message was then recovered from the ciphertext using the lattice-based decryption algorithm, which involved solving the LWE instance with the same secret key. Figure 2 demonstrates a lattice-based encryption algorithm that utilizes optimized 3D chaotic maps to enhance the security and efficiency of image communication, providing robust protection for transmitted image data.

5. Conclusion

This study presents a robust and efficient secure communication framework that integrates Lattice-Based Encryption (LBE) with Image Steganography (IS) to ensure confidentiality and imperceptibility in message transmission. The use of LWE-based encryption offers strong resistance against both classical and quantum attacks, addressing future security concerns.

References

[1] H. Aparna and J. Madhumitha, "Combined image encryption and steganography technique for enhanced security using multiple chaotic maps," *Comput. Electr. Eng.*, vol. 110, p. 108824 (2023), doi: 10.1016/j.compeleceng.2023.108824.

[2] H. Mohades, M. Kadkhoda, and M. M. Mohades, "Application of the Lowner-John ellipsoid in the steganography of lattice vectors and a review of the Gentry's FHE," arXiv preprint, arXiv:1804.10246 (2018).

[3] F. Kurniawan and G. B. Satrya, "Future identity card using lattice-based cryptography and steganography," in Advances in Computer, Communication and Computational Sciences, S. K. Bhatia, S. Tiwari, R. Sui, M. C. Trivedi, and K. K. Mishra, Eds. Singapore: Springer, vol. 1158, *Advances in Intelligent Systems and Computing*. (2021) doi: 10.1007/978-981-15-4409-5_4.

[4] Y. Li, K. S. Ng, and M. Purcell, "A tutorial introduction to lattice-based cryptography and homomorphic encryption," arXiv preprint, arXiv:2208.08125 (2022). [Online]. Available: https://arxiv.org/abs/2208.08125

[5] S. R. Raiyan and M. H. Kabir, "SCReedSolo: A secure and robust LSB image steganography framework with randomized symmetric encryption and Reed-Solomon coding," arXiv preprint, arXiv:2503.12368 (2025). [Online]. Available: https://arxiv.org/abs/2503.12368

[6] M. Johnson and V. Vijayakumar, "An investigation on the optimal control for Hilfer fractional neutral stochastic integrodifferential systems with infinite delay," *Fractal Fract.*, vol. 6, no. 10, p. 583 (2022), doi: 10.3390/fractalfract6100583.

[7] J. G. Rajan and R. S. Ganesh, "Dynamic pixel shuffling and hash LSB steganography with RC4 encryption: A robust data security framework," *Expert Syst. Appl.* (2025), doi: 10.1016/j.eswa.2025.127403.

[8] X. Wang, G. Xu, and Y. Yu, "Lattice-based cryptography: A survey," *Chin. Ann. Math. Ser. B*, vol. 44, pp. 945–960 (2023), doi: 10.1007/s11401-023-0053-6.

[9] K. Sharma, S. Bhatt, and M. Khari, "Empirical study on network exploitation tools and vulnerability detection tool," *J. Inf. Optim. Sci.,* vol. 46, no. 5, pp. 1439–1458 (2025), doi: 10.47974/JIOS-1508.

[10] M. Jain, R. Verma, S. Kumar, A. Srivastava, A. Pillai, and V. S. Sharma, "Securing the future of wireless communications: Utilizing a blend of deep learning techniques for identifying risks in advanced communication networks," *J. Inf. Optim. Sci*., vol. 46, no. 4-A, pp. 939–948 (2025), doi: 10.47974/JIOS-1819.

[11] A. F. Mutar, L. M. Khanli, and H. Emami, "A hybrid cryptographic and deep learning approach for IoT device security," *J. Discrete Math. Sci. Cryptogr.,* vol. 28, no. 4-B, pp. 1437–1449 (2025), doi: 10.47974/JDMSC-2289.

[12] L. S. Reddy and I. Kumar, "Inside adversary combinatorial attacks in secret sharing scheme via linear system of equations when n = 5," *J. Discrete Math. Sci. Cryptogr.,* vol. 28, no. 3, pp. 715–732 (2025), doi: 10.47974/JDMSC-1866.

Received November, 2024