International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-13 Issue-4, April 2024

# Hybrid Cryptosystem using Lattice Permutation and Chaos Logistic Mapping for Image Security

**Thoti. Sasikala, Kanusu. Srinivasa Rao, Buduri. Reddaiah, Bodi. Susheel Kumar**

***Abstract*: Every business platform uses online services and is increasing. Wired and wireless networks are becoming increasingly popular every day. With this, sensitive data is carried over the internet daily. Due to the rapid growth of networks, information security has become increasingly important. Hence, there is a significant risk of data being misinterpreted or manipulated by unauthorised parties. Therefore, there is a need to provide security for the data, and cryptography is the science that helps in providing this security. The encryption algorithm plays a crucial role in information security. This paper provides a brief description of a new hybrid system designed to enhance security. In this work, in addition to traditional operations, Lattice permutation is employed in the encryption process. For key generation, Chaos Logistic Mapping is used, which exhibits greater resistance to key breaking by unauthorised persons. Services like online transactions may be protected mainly with this type of newly proposed hybrid system.***

***Keywords*: Lattice Permutation, Logistic Map, Encryption, Decryption, Chaotic Key Generation.**

## I. INTRODUCTION

These days, accessing web services has become crucial for both individuals and organizations. Over the past 25 years, internet services have made it easy and practical to contact people anywhere in the world. One industry that leverages this substantial benefit offered by the internet is e-business. In this case, protecting sensitive information becomes crucial. An increasing number of secure apps are needed as the electronic business sector expands. Cryptography is a science that is essential to improving security and is one of the best approaches. This science is more critical for modern systems [7] and has a long and impressive history [3] in data security. By considering mathematical operations and scientific functions that enhance security services, this science provides comprehensive and reliable protection.

**Manuscript received on 30 March 2024 | Revised Manuscript received on 05 April 2024 | Manuscript Accepted on 15 April 2024 | Manuscript published on 30 April 2024.**

**Correspondence Author(s)*
**Thoti. Sasikala**, Department of Computer Science and Technology, Yogi Vemana University, Kadapa, India. Email: sasikala3516@gmail.com, ORCID ID: 0009-0000-0942-2507
**Kanusu. Srinivasa Rao**, Associate Professor, Department of Computer Science and Technology, Yogi Vemana University, Kadapa, India. Email: kanususrinivas@gmail.com. ORCID ID: 0000-0002-5851-2194
**Buduri. Reddaiah***, Department of Computer Science and Technology, Yogi Vemana University, Kadapa, India. Email: prof.reddaiah@yvu.edu.in, ORCID ID: 0000-0002-5851-2194
**Bodi. Susheel Kumar**, Department of Computer Science and Technology, Yogi Vemana University, Kadapa, India. Email: bjayakarunya@gmail.com, ORCID ID: 0000-0002-5851-2194



Since approximately 1900 BC, cryptography has been practised as a scientific method for encoding and decoding data. When a scribe in Egypt first used the traditional methods of communication, this process was started and put into practice [1]. In the past, Julius Ceaser employed similar strategies to conceal information and interact with his military officers [8]. Data can be protected using cryptography to prevent unwanted parties from accessing it. It appears to be a tactic to convert the text from its original, understandable form to an unintelligible one to preserve and send the data securely [5]. Encryption is the process of creating a mechanism that safeguards data, ensuring its confidentiality and integrity. It is challenging to get back the originality of any form of data while using this approach without using a decryption process [4].

One crucial component of cryptography, the key, is used to carry out these hiding and unhiding operations. Information privacy is dependent on computations carried out by encrypting and decrypting data using a private key [6]. This is considered a fundamental component utilised in cryptographic computations, enhancing the system's overall performance. Although encryption and decryption algorithms are potent and practical, it is relatively straightforward for unauthorised individuals to breach security if a key is obtained and made public. There are two primary ways in which keys are utilised in cryptosystems, as they are crucial components. The first is a single-key cryptosystem, which involves a single key used for both encoding and decoding. A public key cryptosystem, or asymmetric cryptosystem, is another type. Here, information is encoded with one key, while its original form is recovered using the other.

## II. CRYPTOGRAPHY AS BACKGROUND

Encryption, also known as enciphering, is the process of transforming plaintext into a scrambled form. Decryption, also known as deciphering, is the process of recovering the original text from a scrambled form [2]. Two encryption methods are usually used when processing text. One strategy is substitution, when every element of plain text is substituted with text that is challenging to comprehend and will become difficult for those who are not permitted. The second method is called transposition, in which the original text's components are rearranged in a way that differs from the original and makes it harder to read and comprehend. Additionally, a combined method known as a product cypher can be employed. It is accomplished by combining multiple techniques. The primary constraint when applying these algorithms to the original text is that no plaintext data should be lost. The next is that every word in the text must be reversible.

## III. PROPOSED SCHEME

This proposed hybrid system is primarily based on a lattice-based permutation that rearranges the values generated from the input image. In the encryption process, a lattice permutation is applied to the image, and in decryption, the inverse Lattice permutation is used. To generate the key for the encryption and decryption processes, the Chaos key generation method is used in conjunction with logistic mapping.

### A. Lattice-based Cryptography

There are numerous known secure lattice-based cryptography systems. A significant component of lattice-based cryptography is group theory, which provides a sound mathematical background for the analysis and design of cryptographic systems. Group theory is used in lattice-based cryptography to improve the efficiency of digital signatures, encryption, and key exchange security. A cryptography paradigm based on the difficulty of specific issues related to mathematical structures known as lattices. Michael N. John and O. G. Udoaka have worked on algebraic methods for cryptography [7].

Juan Gonzalez-Meneses, Volker Gebhardt, and Joan S. Birman worked on cube-based lattice cryptography [10]. J. Gryak and D. Kahrobaei [11] conducted research on cryptography based on polycyclic groups. This paper investigates the formation of additive abelian groups using lattice structures defined by basis vectors, offering a flexible framework for cryptographic operations. Due to its reputation for withstanding attacks from quantum computers, lattice-based cryptography is a good option for post-quantum cryptography [12].

### B. Chaos and Logistic Map

The Latency Challenges of symmetric key algorithms are addressed through the use of chaos. There have been many difficulties in using the symmetric-key technique to provide security [13][15], including potentials and opportunities. A completely exploited chaos is found in chaos-based cryptography. A one-dimensional logistic map makes information transport secure and straightforward [16][17][18]. The essential features of chaos include its ability to produce a variety of complex patterns, which leads to the mathematical model making a significant amount of data. Secret keys can be created with this data [19]. Many logistic map forms have been suggested, and they are effective. The well-known characteristic of logistic maps is their unpredictable and random nature, which is frequently anticipated to be utilized in dynamic key propagation in combination with chaotic and scheduling techniques to ensure data integrity.

However, it must possess three qualities, such as a significant parameter, robust chaos, and mixing property, to be selected [14]. By evaluating all the properties, this work utilises the traditional logistic map. The equation is

$$x_{n+1} = r.x_n.(1 - x_n)$$

In this work, a novel key scheduling mechanism is designed that optimises encryption for images, based on the chaos concept aligned with the logistic map. Compared to general cryptosystems, chaos-based cryptosystems are more suitable for handling large amounts of data, including images, audio, and video. Several authors have attempted to introduce chaos into the current cryptosystem [9] [20].

## IV. PROPOSED CRYPTOSYSTEM

### A. Framework of Encryption Process

In this process, the original image is converted to an encrypted image using Lattice permutation and Chaos key generation with logistic mapping, as shown in Figure 1.

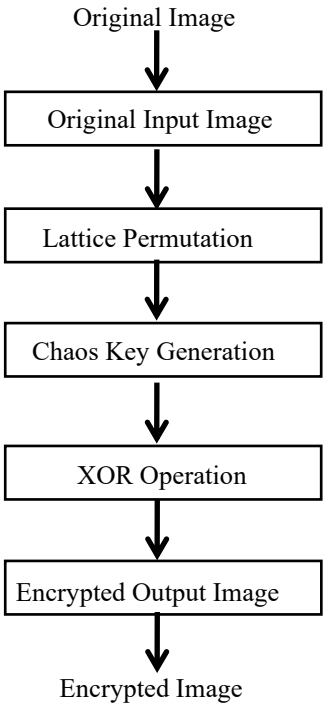


**Fig. 1. Block Diagram of Encryption Process**

### B. Encryption Algorithm

The proposed algorithm (Figure 1) outlines a step-by-step procedure for encryption, which involves converting the original image into an encrypted image.

**Proposed Encryption Algorithm-1**

1. Original Input Image
   a. Read the grey-scale image and convert it into an ASCII pixel representation.
   b. Then build a 3x3 matrix.
2. Lattice Permutation
   a. Select an image and build a 3x3 matrix from the ASCII pixel values
   b. Determine the size of the lattice considered key.
   c. Divide the image into blocks of size key x key. If the size of the image is not divisible by the key, apply zero padding
   d. For each block, apply lattice permutation by shifting pixels according to the permutation rule

      **New position = (i + j) % key**

   e. Save the permutated blocks to obtain the permutated image.

3. Chaos Key Generation
   a. Read the permutated image for encrypting the image using the Chaos key image
   b. Initialize parameters
      I. Chaos, a logistic map parameter 'r' (commonly between 3.5 and 4)
      II. Select an initial condition '$x_o$' (seed) for the logistic map.
      III. Select a specific number of iterations to iterate.
   c. Iterate through the logistic map equation for a specific number of iterations.
      ie., $\boldsymbol{x_{n+1} = r.x_n.(1 - x_n)}$
   d. Apply the round function to convert logistic values into pixel values according to the Grayscale image (0-255).
      **Pi=round (255.Xi)**
      Where, Pi=pixel values
      Xi=logistic value
   e. Save the logistic mapping key image to encrypt the permutated image.
4. XOR Operation
   a. Convert the pixel values of the permutated image and the key image into binary value representation.
   b. Perform an XOR operation between them.
   c. Convert binary values to decimal values.
5. The result of the XOR operation is the encrypted image

### C. Framework Decryption Process

In this process, the encrypted image is converted to the original image by using inverse Lattice permutation and Chaos key generation with logistic mapping, as shown in Figure 2.

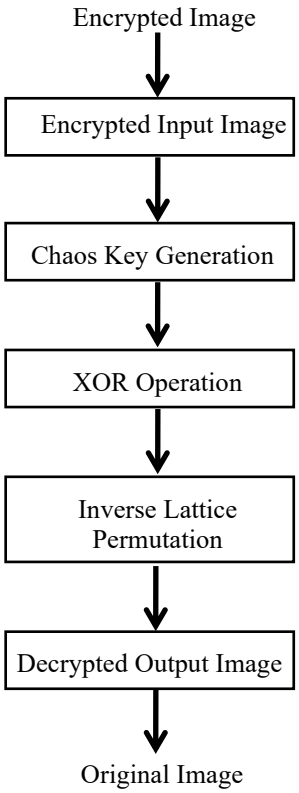


**Fig. 2. Block Diagram of Decryption Process**

### D. Decryption Algorithm

The proposed algorithm 2 illustrates a step-by-step procedure for decryption that involves converting the encrypted image into the original image, as shown in Figure 2.

**Proposed Decryption Algorithm-2**

1. Read the encrypted image as input for decryption.
2. Chaos Key Generation: Regenerate the chaotic key sequence using the same Chaos-based algorithm used in encryption.
   a. Read the encrypted image
   b. Initialize parameters
      I. Chaos, a logistic map parameter 'r' (commonly between 3.5 and 4).
      II. Select an initial condition '$x_o$' (seed) for the logistic map.
      III. Select a specific number of iterations to iterate.
   c. Iterate through the logistic map equation for a specific number of iterations.
      ie., $\boldsymbol{x_{n+1} = r.x_n.(1 - x_n)}$
   d. Apply the round function to convert logistic values into pixel values according to the Grayscale image (0-255)
      **Pi=round (255.Xi)**
      Where, Pi=pixel values
      Xi=logistic value
   e. Save the logistic mapping key image to decrypt the encrypted image
3. XOR Operation
   a. Convert the pixel values of the encrypted image and the key image into binary value representation.
   b. Perform an XOR operation between them.
   c. Convert binary values to decimal values
4. Inverse Lattice Permutation
   a. Read the image that is generated as a result of the XOR operation.
   b. Use the same key size as used in the encryption process.
   c. Divide the resultant of the XOR operation image into blocks of size key x key. If the image size is not divisible by the key, apply zero padding.
   f. For each block, apply inverse lattice permutation by shifting pixels back to their original position
      **Original position = ((j - i) + key) % key**
5. The result of the inverse Lattice permutation is the original image

## V. RESULTS

The encryption algorithm used on the original image, where the ASCII code of the image is considered in a 3x3 matrix, is shown in Table I to produce the encrypted image.

**Table I: Outcome of Encryption Process**

| Original Image | Lattice Permutation (New position = (i+ j)%key (here, key =lattice key)] | Chaos key generation (Apply Logistic mapping) $x_{n+1}=r.\ x_n.\ (1-x_n)$ | XOR b/w Resultants of Lattice permutation and Chaos key generation | Encrypted Image |
|---|---|---|---|---|
| 100 150 200<br>50 75 125<br>25 180 60 | 100 150 200<br>125 50 75<br>180 60 25 | 127 249 24<br>85 222 113<br>245 36 121 | 27 111 208<br>40 236 58<br>65 24 96 | 27 111 208<br>40 236 58<br>65 24 96 |

The decryption algorithm used on the encrypted image is considered in a 3x3 matrix, as shown in Table II, to obtain the original image.

**Table II: Outcome of Decryption Process**

| Encrypted Image | Chaos key generation (Apply Logistic mapping) $x_{n+1}=r.\ x_n.\ (1-x_n)$ | XOR b/w Resultants of Encrypted Image and Chaos Key Generation | Inverse Lattice Permutation (Original position = ((j-i)+key)%key (here, key =lattice key)] | Original Image |
|---|---|---|---|---|
| 27 111 208<br>40 236 58<br>65 24 96 | 127 249 24<br>85 222 113<br>245 36 121 | 100 150 200<br>125 50 75<br>180 60 25 | 100 150 200<br>50 75 125<br>25 180 60 | 100 150 200<br>50 75 125<br>25 180 60 |

## VI. CONCLUSION

Group theory integration turns out to be a strong and flexible method in lattice-based cryptography. Lattices and their subgroups form abstract algebraic structures that provide a strong basis for creating cryptographic methods that withstand both conventional and quantum attacks. The security of lattice-based protocols is influenced by the hardness of lattice problems that are formulated using group-theoretic principles.

This work described a lattice-based group theory-based cryptography technique. A unique key scheduling mechanism has been created to encrypt vast amounts of data, and it is also built and demonstrated using the lattice chaos concept in conjunction with the logistic map. As illustrated, the suggested method requires an appropriate chaotic map that reduces the likelihood of it breaking.

As part of future enhancements with continued development, the robustness and effectiveness of lattice-based cryptographic systems should be improved, making them competitive options in the rapidly changing field of secure communications and data security.

## DECLARATION STATEMENT

| | |
|---|---|
| Funding | No, I did not receive. |
| Conflicts of Interest | No conflicts of interest to the best of our knowledge. |
| Ethical Approval and Consent to Participate | No, the article does not require ethical approval or consent to participate, as it presents evidence. |
| Availability of Data and Material/ Data Access Statement | Not relevant. |
| Authors Contributions | All authors have equal participation in this article. |

## REFERENCES


1. S. Herbert, “A brief History of Cryptography”, An article available at hhtp://cybercrimes.net/aindex.html.
2. B. Reddaiah, R. Pradeep kumar Reddy, S. Hari Krishna, “Enciphering using Bit-wise logical operators and pairing function with text generated hidden key”, IJCA 90975-88870, vol. 121, No. 8, July 2015: pp. 30-35. https://doi.org/10.5120/21562-4597
3. S. Tanenbaum, “Modern Operating Systems”, Prentice Hall, 2003.
4. Basic Cryptographic Algorithms”, an article available at www.itsc.state.md.us/oldsite/info/InternetSecurity/Crypto/CryptoIntro.html#Alogrithms.
5. P.P. Charles & P. L. Shari, “Security in Computing: 4th edition”, Prentice-Hall, Inc., 2008.
6. Behrouz A. Forouzan, Cryptography and Network Security, Special Edition, Tata McGraw-Hill.
7. KHAN, “The Codebreakers”, Macmillan Publishing Company, New York, 1967.
8. S. William, Cryptography and Network Security: Principles and Practice, 2nd edition, Prentice-Hall, Inc., 1999. Pp 23-50
9. Sehgal, A., Perelman, V., Kuryla, S. and Schonwalder, J.: Management of resource-constrained devices in the Internet of Things. IEEE Communications Magazine, 50(12). (2012). https://doi.org/10.1109/MCOM.2012.6384464
10. John S. Birman, Volker Gebhardt and Juan Gonzalez-Meneses, Conjugacy in Garside groups 1: cycling, powers and rigidity, Groups Geom, Dynamics, 1(2007), 221-279. https://doi.org/10.4171/ggd/12
11. Gryak and D. Kahrobaei, The status of polycyclic group-based cryptography: A survey and open problems, Groups Complexity Cryptology, 8(2016), 171-186. https://doi.org/10.1515/gcc-2016-0013
12. D. Kahrobaei and V. Shpilrain, Using semidirect product of (semi) groups in public key cryptography, Computability in Europe, LNCS, (2016), 132-141. https://doi.org/10.1007/978-3-319-40189-8_14
13. Mukhopadhyay, S.C. and Suryadevara, N.K.: Internet of things: Challenges and opportunities. In Internet of Things (pp. 1-17). (2014). Springer, Cham. https://doi.org/10.1007/978-3-319-04223-7_1
14. Yao, X., Chen, Z. and Tian, Y.: A lightweight attribute-based encryption scheme for the Internet of Things. Future Generation Computer Systems, 49, (2015). Pp.104-112. https://doi.org/10.1016/j.future.2014.10.010
15. Ion, M., Zhang, J. and Schooler, E.M.: August. Toward content-centric privacy in ICN: Attribute-based encryption and routing. In Proceedings of the 3rd ACM SIGCOMM workshop on Information-centric networking (pp. 39-40). ACM. (2013). https://doi.org/10.1145/2491224.2491237
16. Baptista, M.S.: Cryptography with Chaos. Physics Letters A, 240(1-2), (1998). Pp. 50-54. https://doi.org/10.1016/S0375-9601(98)00086-3
17. Kocarev, L.: Chaos-based cryptography: a brief overview. IEEE Circuits and Systems Magazine, 1(3), (2001). Pp. 6-21. https://doi.org/10.1109/7384.963463
18. Kotulski, Z., SZCZEPANSKI, J., Gorski, K., Paszkiewicz, A. and Zugaj, A.: Application of discrete chaotic dynamical systems in cryptography-DCC method. International Journal of Bifurcation and Chaos, 9(06), (1999). Pp. 1121-1135. https://doi.org/10.1142/S0218127499000778
19. Alvarez, G., Montoya, F., Romera, M. and Pastor, G.: Breaking parameter modulated chaotic secure communication system. Chaos, Solitons & Fractals, 21(4), (2004). Pp. 783-787. https://doi.org/10.1016/j.chaos.2003.12.041
20. Kocarev, L.: Chaos-based cryptography: a brief overview. IEEE Circuits and Systems Magazine, 1(3), (2001). Pp. 6-21. https://doi.org/10.1109/7384.963463


## AUTHORS PROFILE

**Thoti. Sasikala** is studying M.C.A. in the Department of Computer Science and Technology at Yogi Vemana University, Kadapa, Andhra Pradesh. She is passionate about learning new technologies and developing new methods. She aims to become a comprehensive security service provider and is eager to conduct security-related research with practical applications. She also wants to work in the security industry as a software engineer. Her leadership demonstrates her dedication to resource management and the advancement of technical breakthroughs in various initiatives. Sasikala's contributions to this research offer a thorough comprehension of the security industry's scalability issues.

**Kanusu. Srinivasa Rao** is working as an Associate Professor in the Department of Computer Science and Technology at Yogi Vemana University, Kadapa, Andhra Pradesh. He has published 40 papers related to Image Processing and Security. His research interests include Image Processing, Cryptography, and Network Security. Kanusa's commitment to investigating the nexus between security and technology is essential to the creation of reliable solutions. His research highlights the value of using systematic techniques to create models for security and upkeep. He symbolizes the collaborative attitude of this study team as the corresponding author.

**Buduri. Reddaiah** is working as an Associate Professor in the Department of Computer Science and Technology at Yogi Vemana University, Kadapa, Andhra Pradesh. His research interests are in security and Artificial Intelligence. With a focus on network security and Artificial Intelligence, his research endeavours to enhance data integrity and access control mechanisms. Reddaiah's dedication to exploring the intersection of technology and security plays a crucial role in the development of robust systems. His work emphasises the importance of methodical approaches to developing models in security and maintenance. As the corresponding author, he embodies the collaborative spirit of this research team.

**Bodi. Susheel Kumar** is working as an Academic Consultant in the Department of Computer Science and Technology, Kadapa, Andhra Pradesh. His research areas include cryptography and Network Security, and he has published many papers in these areas. He is a significant contributor to this study due to his expertise and commitment to programming with new technologies, as well as his efforts to promote a deeper understanding of the role of technology in this work. He has a strong desire to work as a developer. His dedication to his career is evident in his leadership of various activities. Susheel's contributions to this work provided a thorough understanding of the scalability issues associated with security-related online applications.