AI in Encryption

B L Sunayana
225890048
Manipal Institute of Technology
Bengaluru,India
boppana.mitblr2022@learner.manipal.edu

Aarushi Garg
225890388
Manipal Institute of Technology
Bengaluru,India
aarushi2.mitblr2022@learner.manipal.edu

Ishita Singh
225890344
Manipal Institute of Technology
Bengaluru,India
ishita.mitblr2022@learner.manipal.edu

Vaishnavi D
225890242
Manipal Institute of Technology
Bengaluru,India
vaishnavi1.mitblr2022@learner.manipal.edu

***Abstract*— This paper explores various techniques for image encryption, analyzing methods to enhance data security and maintain image fidelity. By employing algorithms such as chaos-based encryption, line maps, and elliptic curve cryptography (ECC), this study seeks to assess and compare their performance, security robustness, and computational efficiency.**

I. Introduction

In today’s digital landscape, the demand for secure storage and transmission of images is critical, particularly for sensitive data. Image encryption techniques provide a promising approach to maintaining data confidentiality and integrity. By converting images into unintelligible forms, these methods prevent unauthorized access and tampering. This paper focuses on several encryption techniques, comparing their effectiveness in retaining image fidelity and ensuring security.

II. Paper Review

A. *Chaos-Based Image Encryption*

This paper explores a chaos-based approach to image encryption, leveraging chaotic maps to generate keys that are highly sensitive to initial conditions. This sensitivity introduces pseudo-randomness, a fundamental requirement for secure encryption. By employing chaotic systems, the authors create an encryption method where small changes in the input parameters produce entirely different encrypted outputs, thereby enhancing security and making decryption without the correct key extremely difficult. The paper effectively demonstrates the potential of chaotic algorithms for secure image encryption, particularly for scenarios requiring complex, dynamic encryption methods. However, it does not fully address performance limitations, particularly concerning computational efficiency with larger or high-resolution images, which may impact practical usability *[1].*

B. *Line Map Analysis*

This paper proposes a novel image encryption algorithm that leverages chaos theory and a Line map to enhance encryption security. The combination aims to maximize randomness in the encryption process, a critical factor in preventing unauthorized decryption. However, the approach faces challenges in real-time applications, particularly with high-resolution images due to its computational demands. While promising, the paper leaves room for exploring optimization strategies to make it more efficient and secure against various attack types, such as differential attacks *[2].*

C. *Non-Deterministic Symmetric Cryptosystem*

In this study, the authors introduce a non-deterministic symmetric cryptosystem for image encryption, emphasizing randomness to boost security. This method is effective for creating high unpredictability, which is essential for robust encryption. However, the paper doesn’t fully address the scalability issues and computational intensity that might arise with large image datasets. The algorithm could benefit from balancing between randomness and processing speed to improve real-time applicability and performance *[3].*

D. *Elliptic Curve Cryptography (ECC)*

This paper examines the application of elliptic curve cryptography (ECC) in image encryption, highlighting its potential for high security and efficiency due to ECC's smaller key sizes. The authors effectively demonstrate ECC's utility in image encryption, though the analysis lacks an assessment of its performance under different chaotic maps and in resource-constrained environments. Future work could involve exploring ECC's adaptability across various hardware configurations and attack conditions, such as those posed by emerging quantum threats, to gauge its broader applicability *[4].*

III. Research Gap

Despite the strengths of these encryption techniques, each has certain limitations:

- **Chaos-Based Encryption:** The paper by K. Eves and J. Valasek on chaos-based image encryption (2005) addresses an important approach to secure image encryption, but there are still gaps that subsequent research has identified. Key areas for further exploration include the optimization of encryption speed and computational efficiency, as the algorithm may be slower for high-resolution images. Another research gap lies in the robustness of chaotic encryption methods against emerging cryptographic attacks, such as chosen-plaintext or chosen-ciphertext attacks, which exploit weaknesses in the key management or chaotic map sensitivity.

- **Line Map Encryption:** This paper introduces an innovative image encryption algorithm that integrates chaos with a Line map. While effective, it lacks in-depth analysis regarding its computational efficiency and performance under high-resolution data conditions. The method's encryption speed and key sensitivity may not fully meet the requirements of real-time applications. Furthermore, the paper does not thoroughly evaluate the resilience of this combined approach against modern cryptographic attacks, such as differential and chosen-ciphertext attacks.
- **Non-Deterministic Symmetric Cryptosystem:** This study employs a non-deterministic approach to image encryption within a symmetric cryptosystem framework, emphasizing high randomness. While this increases unpredictability, a research gap exists in terms of scalability—especially when handling large volumes of image data. Additionally, the randomness introduced may impact processing time, which could be a limitation for real-time applications or environments requiring high-speed processing.
- **Elliptic Curve Cryptography (ECC):** This paper investigates image encryption using elliptic curve cryptography (ECC), known for its compact key sizes and security. However, while ECC is theoretically efficient, there is limited analysis on its real-world performance, particularly when used in conjunction with chaotic systems. A research gap exists in evaluating ECC's effectiveness under conditions that may involve varying hardware capabilities or under attack models that target specific aspects of chaotic and ECC combinations. Future work could explore optimizing ECC for compatibility with chaotic maps and ensuring its adaptability in embedded systems or resource-constrained environments.

Future work could focus on the lack of effective encryption methods that are specifically tailored to thwart AI models from learning and reproducing protected images. Furthermore, we could explore the usage of various Machine Learning models and how they can help us in encrypting images.

References

[1] K. Eves and J. Valasek, "Chaos-based image encryption algorithm," *ResearchGate*, 2005. [Online]. Available: https://www.researchgate.net/publication/259665875_Chaos-based_image_encryption_algorithm.

[2] Zhou, Guomin & Zhang, Daxing & Liu, Yanjian & Yuan, Ying & Liu, Qiang. (2015). A novel image encryption algorithm based on chaos and Line map. Neurocomputing. 169. 10.1016/j.neucom.2014.11.095. https://www.sciencedirect.com/science/article/abs/pii/S0925231215006785

[3] B. S. Gurubaran, N. Sasikala Devi, E. R. S. Subramanian, and D. Geophilus, "Non-Deterministic Image Encryption Based on Symmetric Cryptosystem," *ScienceDirect*, 2016. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1877050916315423.

[4] L. D. Singh and K. M. Singh, "Image Encryption using Elliptic Curve Cryptography," *ScienceDirect*, 2015. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1877050915013782.