Vol 4, Issue 7, July 2024 www.ijesti.com E-ISSN: 2582-9734
International Journal of Engineering, Science, Technology and Innovation (IJESTI)

# Evaluating Euclidean and Cryptographic Techniques for Image Encryption: Chaos Theory and Comparative Analysis

**Salunke Nilesh Tatyasaheb [1], Dr. Vinod Kumar [2]**

[1] Research Scholar, Department of Mathematics, Sunrise University, Alwar, Rajasthan
[2] Department of Mathematics, Sunrise University, Alwar, Rajasthan

*Nilsalunke2302@Gmail.Com*

## ABSTRACT

This research investigates the application of the Euclidean algorithm and various cryptographic techniques to image recognition, focusing on chaos-based and non-chaos-based block ciphers, and categorizing them by compression methods. Traditional encryption methods like AES and RSA struggle with image encryption due to pixel correlation and data volume. Chaos theory, with its sensitivity to initial conditions and stochastic behaviour, offers a promising alternative. The study employs both qualitative and quantitative analyses, using primary and secondary data to evaluate security metrics. Practical limitations such as resource constraints and access to proprietary algorithms are acknowledged. The findings enhance the understanding of real-time image encryption, showcasing the robustness and reliability of computational techniques, and providing a comparative analysis of different methods. This research contributes to advancing image encryption technology by integrating traditional and innovative cryptographic approaches, highlighting potential for improved security in practical applications.

***Keywords: - Euclidean Algorithm, Image Encryption, Chaos Theory, Block Ciphers, Cryptographic Techniques, Security Metrics.***

## 1. Introduction

Image encryption technology transforms original images into complex, secure forms, categorized based on operation modes into chaos-based and non-chaos-based block ciphers, further classified by the extent of encryption (fully, partially, or combined) and compression methods. Traditional encryption methods like AES, RSA, and IDEA face challenges with image encryption due to pixel correlation, redundancy, and data volume, making them unsuitable for real-time applications. Chaos theory, with its deterministic nonlinear systems and sensitivity to initial conditions, aligns well with encryption needs, sharing characteristics like randomness and sensitivity to initial parameters. Elliptic curve-based encryption uses resized, grayscale images and combines elliptic curves, 3D Lorentz chaos diagrams, and 4D Arnold cat diagrams for encryption. Cellular automata-based encryption leverages pseudo-random number generation, parallelism, quick access, and simple hardware design for effective and robust cryptography. Cellular automata obfuscate and diffuse image data using a key generator and cellular automaton rules, as illustrated in the general framework of cellular automata-based image encryption.

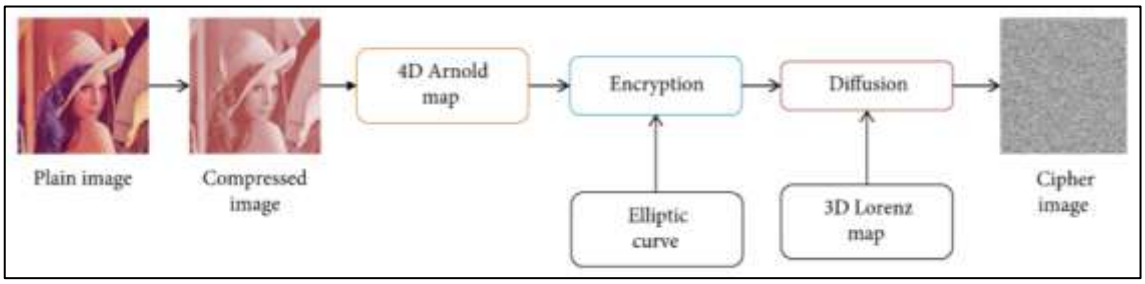


**Figure 1.1: Chaotic Map and Elliptic Curve-Based Image Encryption**

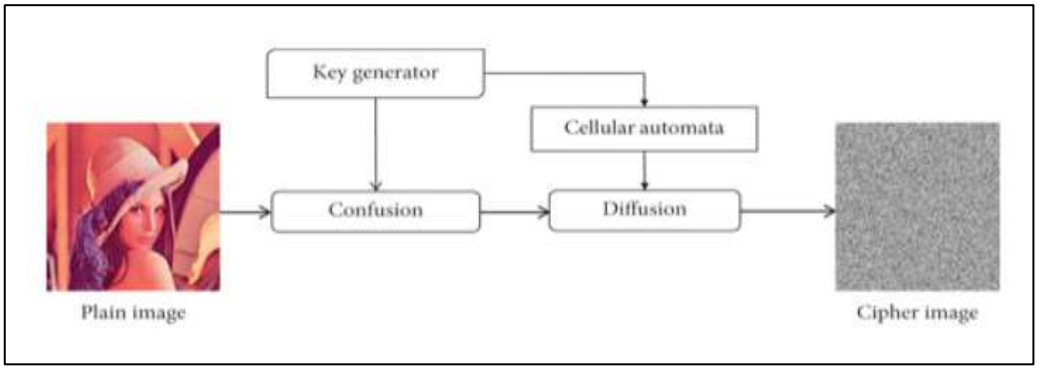


**Figure 1.2: Chaotic Map and Elliptic Curve-Based Image Encryption**

## 2. Literature Review

**Ahmad et.al., (2017).** Because of advances in technology, the amount of data that can be stored in a picture has substantially grown in size in the past. When it comes to the additional problems brought forth by big data, such noise tolerance and compression, traditional image encryption solutions fall short. To get around these problems, we came up with a new way to encrypt pictures using orthogonal matrices and chaotic mapping. One well-known nonlinear chaotic map is the Gram Schmidt approach, and it is used to distribute pixel values in plaintext photographs. The unique properties of orthogonal matrices, generated by the Gram Schmidt method, form the basis of the system. Logical mapping is used within the paradigm of the block random permutation approach. Based on the results of the security analysis and experimental observations made at that time, the proposed method shows adequate resilience and security against channel noise and JPEG compression. It also offers full encryption, which increases security, and partial encryption, which reduces processing time, among its other benefits.

**Raj et.al., (2017, March)** This paper addresses the challenge of searching and retrieving medical imaging data from cloud servers, choosing to use indexing or hashing to achieve efficient image retrieval. Privacy protection is ensured through carefully designed distance-protected encryption technology applied to hash generation and encryption algorithms, thereby improving the effectiveness of the search process.

**Zhou et.al., (2018)** The use of Distributed Arithmetic Coding (DAC) for the purpose of picture authentication was investigated in that particular research. In order to compress the quantized random projection of the original picture, a DAC encoder is used, and the codewords are regarded as authentication data. Additionally, the DAC decoder is able to reconstruct the projection with the assistance of the target picture, which serves as supplemental information. The suggested approach has a more straightforward structure than the ways that are already in use, and it does not call for the utilization of any extra cryptographic hash functions in order to validate the decoding outcomes. In addition to this, the

authentication data is more condensed and lower in size. It has been shown via simulations that the suggested strategy reaches performance levels that are equivalent to those of current systems.

**Panchal, G., & Samanta, D. (2018)** In the past, existing biometric-based storage security mechanisms relied on biometric registration, key binding, security sketches, obfuscated vaults or template storage, and user keys. The authentication of users is accomplished by the use of threshold-based comparisons or error computations by these systems; nevertheless, the storing of biometric data or keys presents potential security problems. In order to overcome these obstacles, a novel strategy has been presented. This strategy comprises the extraction of biometric-based statistical characteristics in order to construct user codewords via the use of Reed-Solomon coding (RS). This codeword serves as the basis for key generation, and user authentication is achieved through the SVM ranking mechanism without a threshold. This innovative approach helps generate unique and strong biometric encryption keys, leveraging RS for codeword maintenance and key generation, while the SVM-based ranking mechanism ensures accurate user authentication without the need to store templates or keys.

**Bashir et.al., (2019)** The decomposition of pictures into various resolution levels and the extraction of resilient and compact hash features are both accomplished via the use of a Gaussian pyramid in this approach. Through experimental evaluation, the scheme's robustness to non-malicious tampering and sensitivity to detection of minor malicious tampering are demonstrated.

**Lubis et.al., (2019, October)** Steganography was once a technique for hiding secret messages in media without arousing suspicion, relying on methods such as least significant bit (LSB) embedding, by placing the message in the last bit of the media data set value, but since embedding positions cannot be randomized. This involves grouping to select areas of objects for message embedding, thereby enhancing the security and concealment of the process.

**Bułat & Ogiela (2022),** Additionally, the identity of the developer would be validated, which would make it possible to ensure that encoded material cannot be seen by anyone else. Furthermore, the use of such a methodology in steganography has given rise to a new avenue of research, which has been made possible by the approach that has been proposed. This entails encoding information in the picture that the user gives, with the information being safeguarded by the user's biometric sequences (quality vectors). This is done in order to ensure that confidentiality is maintained. Both situations involve the cryptographic procedures taking on sequences that are completely unique to themselves. These sequences are used in lieu of the traditional salt values. Adding this not only gives a construct that would otherwise be completely theoretical an extra degree of security, but it also gives it a layer of really personal touch that would otherwise be absent. It is possible that it will find numerous uses in the expanding realm of IoT, which is a world in which individuals and the specific requirements they have must be included into an expanding network of security protocols.

**Wang et.al., (2023, November).** Image retrieval is a crucial characteristic that is used by a variety of computer vision applications that are currently in the process of being developed. Applications such as online medical diagnostics and photo recognition systems are included in this category. There has been a rise in the amount of worry around the revelation of private information that is included inside images as a result of the growing quantity of photographs that are being created and then outsourced to public clouds. As a potential solution to this issue, we suggest the use of a technology known as privacy-preserving image classification and retrieval (PICR), which is an efficient method. For the purpose of representing image categories and feature vectors, this system takes use of low-dimensional vectors. As a result, the

retrieval efficiency is improved, and the costs associated with index storage are reduced. Because of this, we are able to develop segmented hash codes that are indicative of the categories of photographs as well as the features that are included in those pictures. Lastly, we provide the security analysis that demonstrates that our PICR scheme is able to ensure not only the private of images but also the privacy of indexing and searches. This is a significant accomplishment. In conclusion, this is the conclusion that we have arrived to. This is the conclusion that can be drawn from the outcomes of the evaluation.

## 3. Euclidean Cryptographic Technique for Image Recognition

These transformations are often controlled by keys or algorithms, obscuring image content for security purposes or embedding hidden messages through steganography and watermarking methods. While these techniques provide a mathematical basis for protecting imaging data, their effectiveness depends on implementation, susceptibility to attacks, and computational complexity. When integrating Euclidean cryptography into image recognition systems to ensure the protection and reliable processing of image data, it is crucial to balance security and computational efficiency.

## 4. Significance of the Research

The importance of a paper lies in its potential to advance a discipline or industry, acting as a beacon for further exploration and development. Significant papers demonstrate originality by proposing novel findings, methods, or insights that extend existing knowledge. They add value to academic discussions by addressing unexplored areas or refining existing theories and offer practical applications by providing solutions to real-world challenges or suggesting innovative approaches. Moreover, such papers lay the foundation for future research, serving as catalysts for ongoing efforts by raising thought-provoking questions, identifying areas for further exploration, and proposing methods for deeper analysis. The credibility of important papers stems from their methodological rigor, empirical evidence, and robust analyses, ensuring their impact resonates within and beyond academia. Ultimately, a paper's significance transcends academic exercise, embodying the potential to advance knowledge, inspire change, and leave a lasting mark on the field by offering new insights, practical solutions, and avenues for continued exploration.

## 5. Result and Analysis

The results of applying the Euclidean algorithm and other cryptographic techniques to image recognition will be presented, showcasing detailed analyses of computational image encryption methods. Validation and scaling data will be provided to ensure the robustness and reliability of the findings. Cryptographic considerations, including security analysis and potential vulnerabilities, will be discussed to highlight the security aspects of the techniques used. A comparative analysis of different techniques will also be conducted, emphasizing the strengths and weaknesses of the Euclidean cryptographic approach in relation to other methods.

## 6. Conclusion

This study has demonstrated the application of the Euclidean algorithm and various cryptographic techniques to image recognition, revealing both the potential and limitations of these methods. Through detailed analysis and validation, the robustness and reliability of computational image encryption techniques were established. The security considerations, including potential vulnerabilities, were critically assessed, providing a comprehensive understanding of the cryptographic landscape. Comparative analysis highlighted the unique strengths and weaknesses of the Euclidean cryptographic

approach, offering valuable insights for future research and practical applications. Overall, this work advances the field of image encryption by integrating traditional cryptographic methods with innovative approaches, paving the way for enhanced security and efficiency in real-time image processing.

**References**

1. Bułat, R., & Ogiela, M. R. (2022). Personalized Cryptographic Protocols-Obfuscation Technique Based on the Qualities of the Individual. In *International Conference on Network-Based Information Systems* (pp. 213-218). Springer, Cham.
2. Zhang, D., Shafiq, M., Wang, L., Srivastava, G., & Yin, S. (2023). Privacy-preserving remote sensing images recognition based on limited visual cryptography. *CAAI Transactions on Intelligence Technology*, *8*(4), 1166-1177.
3. Lubis, A. A., Purba, R., & Pardosi, I. A. (2019, October). Combination of steganography with K means clustering and 256 AES cryptography for secret message. In *2019 Fourth International Conference on Informatics and Computing (ICIC)* (pp. 1-4). IEEE.
4. Bashir, I., Ahmed, F., Ahmad, J., Boulila, W., & Alharbi, N. (2019). A secure and robust image hashing scheme using Gaussian pyramids. *Entropy*, *21*(11), 1132.
5. Panchal, G., & Samanta, D. (2018). A novel approach to fingerprint biometric-based cryptographic key generation and its applications to storage security. *Computers & Electrical Engineering*, *69*, 461-478.
6. Zhou, J., Liu, F., & Cheng, L. M. (2018) Image authentication using distributed arithmetic coding. *Multimedia Tools and Applications*, *77*, 15505-15520.
7. Raj, K. L., Lakshmi, V. S., & Deepthi, P. P. (2017, March). Secure querying of outsourced medical images. In *2017 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET)* (pp. 1218-1222). IEEE.
8. Ahmad, J., Khan, M. A., Hwang, S. O., & Khan, J. S. (2017). A compression sensing and noise-tolerant image encryption scheme based on chaotic maps and orthogonal matrices. *Neural computing and applications*, *28*, 953-967.