aInternational Academic Institute for Science and Technology

International Academic Journal of Science and Engineering
Vol. 12, No. 2, 2025, pp. 6-10.

ISSN 2454-3896

International Academic Journal of Science and Engineering

www.iaiest.com

Analysis of the Role of Algebraic Structures in Enhancing Cryptographic Security and Encryption Techniques

Tanvi Arora [a], Ajay Naik [b]

[a] *Smart Contracts & Digital Law Lab, Panipat Institute of Technology Law, India*.
[b] *Smart Contracts & Digital Law Lab, Panipat Institute of Technology Law, India*.

Abstract

The arithmetic characteristics of a finite field significantly influence the security attributes of both symmetric and asymmetric encryption systems. Contemporary symmetric-key encryption systems utilize a Galois field with 256 components derived from a singular 8th-degree primitive indeterminate polynomials over Z to construct an S-box, the primary nonlinear factor in AES. The efficacy of S-box-based picture encryption techniques is inferior to that of chaotic system-oriented solutions. This work enhances S-box-based picture encryption methods by using all 16 unique degree 8 fundamental reductive polynomials over Z and using a novel function of the ring Zn of integers times n in the permutations processes. The efficacy of this unique 2-algebraic structures-based encryption of images system is assessed by various statistical analyses, resulting in a notable efficiency level. The comparison of encrypting quality among current chaos-based picture encryption techniques demonstrates that the newly introduced scheme exhibits greater efficiency. This recent advancement in picture encryption techniques offers a replacement for chaos-based encryption of images.

Keywords: Algebraic Structures, Cryptography, Security, Encryption.

DOI: 10.71086/IAJSE/V12I2/IAJSE1211
Received: 05 March 2025/Revised: 17 April 2025/Accepted: 12 May 2025/Published: 27 June 2025

Introduction

The rapid proliferation of digital technologies has rendered interaction swift and casual. People can swiftly interact and share data within seconds via an internet connection (Silvano & Marcelino, 2020). The open nature of wireless systems, such as the web, poses a significant threat to private data security. Cryptography is the discipline concerned with transmitting private data over unsecured channels, encompassing encoding, decoding, and disseminating keys, among other aspects (Banerjee, 2024). Cryptography is categorized into two categories: conventional and asymmetric key encryption. This method of distribution is predicated on the private key. In a symmetric-key security system, the involved parties utilize identical keys. Still, in an asymmetrical-key security system, each party employs distinct keys, precisely standard and secret keys, for safe communications. In symmetric-key encryption, the substitution box (S-box (SB)) is the primary component that generates ambiguity between the key and the data (Zahid et al., 2020). A high-quality S-box is crucial for enhancing the nonlinear nature of block encryption. A multitude of algorithms for the building of S-boxes has been proposed lately. Several pertinent performance indicators have been created to evaluate the worth of an S-box. In recent years, S-boxes have been widely utilized in watermarking, stenography, and audiovisual encryption methods for safe transmission and ensuring the accuracy of received data during communications (Nasr et al., 2024).

Digital imagery is crucial in several social sectors, with applications including defense data, health care advertising, and business, among others. Given the widespread utilization of digital images across various domains, the safety of digital photos has garnered significant attention within the realm of cryptography; thus, the development of novel cryptographic algorithms for encoding images has been a prominent focus for academics (Samiullah et al., 2022).

Several methods for digital security grounded in chaos theories have emerged in the past decade; several have been demonstrated to be vulnerable to various assaults due to flaws in their internal architecture (Joshua, Bhattacharyya, & Rao, 2022). The research analyzed the proposed technique and determined that encryption methods relying solely on pixel location variations and substitutions are vulnerable to chosen-plaintext attacks. The study examined vulnerabilities in the safety of the picture encrypting system based on the perceptron paradigm. The private key can be readily reconstructed if a single pair of plain or encrypted text is known (Abu-Faraj, Al-Hyari, & Alqadi, 2022), (Liu, Li, & Hu, 2021). Researchers developed an image encryption approach employing a hyperchaotic mechanism that generates diffusion in just one iteration. The research identified a flaw in the strategy, indicating it is vulnerable to attacks such as selected texts.

Algebraic Structures in Enhancing Cryptographic Security

An algebraic framework, denoted as $< X, Y, \cdots, ., *, \cdots, k_1, k_2 \cdots, x, y >$, is an n-tuple in which the components x ∈ X and y ∈ Y are different; it encompasses domains and limits of operations and n-ary actions. The Cartesian counterparts of the sets are denoted as $k_1 \; and \; k_2$, which represent binary relationships established on these collections. Non-associative algebra presupposes the vector spaces on an area, wherein the multiplication action interacts with the adding operation according to the standard distributive law. The multiplication process is not inherently circular or associated. A quasigroup, unlike finite categories, lacks associativity and an identity component.

An algebraic framework, represented as (R,*), is classified as a quasigroup if, for any two components a, b ∈ R, both equations a * i = b and j * a = b possess a distinct answer in Q. A quasigroup is defined as a set R equipped with a binary action *, such that for any pair of elements in R, the action * satisfies a specific rule.

$$(\forall a, b \; \in R) a * i = b, j * a = b \tag{1}$$

According to the means, if a quasigroup is a bounded non-empty collection, then every cell of its table constitutes a permutation of l. This study introduces a method for generating quasigroup-based streams of ciphers applicable to developing both asymmetric and asymmetric public-key encryption methods. A recent work presents a taxonomy for cryptographic methods derived from the issue of multidimensional quadratic formulas over quasigroups. A quasigroup is an algebraic structure with three steps that adhere to four specific characteristics.

$$j = x * \left(\frac{i}{j}\right), j = \frac{x}{(i*j)}, j = \left(\frac{j}{i}\right) * i, j = \frac{j+i}{i} \tag{2}$$

A quasigroup (R, *) and associated paragraphs (R, /) and (R, \) exhibit a reciprocal reverse combination according to the following circumstances:

$$i(i * j) = j, i * \left(\frac{i}{j}\right) = j \tag{3}$$

A left self-distributive equation (R, *) that adheres to the principle of $i * (j * k) = (i * j) * (i * k)$for all $i, j, k \in R$, and where the action * is self-distributive, represents a non-associative variant of the more recognized non-abelian finite sets. The structure was characterized by examining the conjugator searching issues (CSP) within noncommutative groupings.

Let Q be a non-empty collection, and let F $R \times R \to R$be a well-defined function. Should the subsequent formula be valid,

$$F_q\big(F_p(t)\big) = F_{F_q(p)}\big(F_q(t)\big) \tag{4}$$

The formula F is referred to as a left self-distributive network. If F, (Q) is seen as a binary action q*p, then the equation (1) transforms into

$$q * (p * t) = (q * p) * (q * t) \tag{5}$$

The procedure * exhibits left self-distributivity about itself. The toughness of a left self-distributed structure indicates the one-wayness or pre-image susceptibility of that system, precisely the difficulty of obtaining s from the pair $(p;\ F, (p))$.

The theoretical foundations of the suggested homomorphic mappings indicate the potential application of left self-distributed non-abelian structures, including quasigroups, in developing symmetric and public key cryptography methods.

Considering that two distinct algebraic frameworks exhibit analogous properties, with one structure stated on a group R and a corresponding framework on a set R', it is possible to find a homomorphic connecting from R to R' that maintains specific attributes of the foundational domain buildings.

Algebraic Structures-based Encryption Algorithm

The research provides the proposed method. The suggested strategy is appropriate for color picture encryption and consists of four phases. In the initial phase, the research separated the red, green, and blue components of the RGB image. The research alters the row-wise R, G, and B streams using a 2 × 2 matrix with elements from the unit grouping U(Zm) intersecting U(ZN), where M and N denote the number of lines and columns, accordingly, in the plain picture. This change yields three modified channels. To achieve significant nonlinearity in the technique, the research employed the S-box building approach, which will be discussed in section 3.1, along with a set of all level 8 basic reductive polynomials with coefficients from the range of Zz to produce sixteen S-boxes. The research partitioned each shuffled color component into 16 segments, substituting each segment with a distinct S-box before amalgamating the substituted segments.

Upon obtaining three replaced matrices, the research constructs a random matrix of dimensions M x N using the number ring Z256 and the polynomial addition modulo, an indestructible polynomial of level 8 over the space Zz. The research then performs a bitwise XOR function on each randomly produced array and each replaced matrix, resulting in three turned matrix structures. The research amalgamates the color modification channels in the last phase to obtain the encoded image. The sequential process of the novel encrypting system is illustrated in Fig. 1.

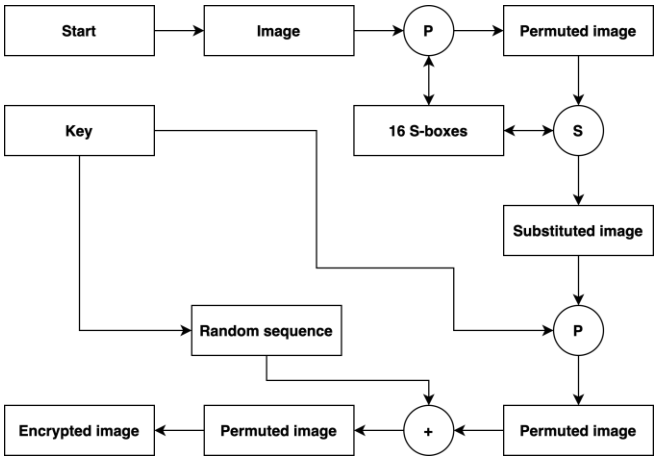


Fig. 1: Architecture of the design

Results

A practical cryptosystem must possess the capacity to withstand all conventional assaults, including statistical and mathematical methods.

4.1 Study of Entropy

This study is a statistical evaluation to assess disorder. The entropy examination of the data that has been encrypted indicates unpredictability, with resultant values around eight if all numbers possess equal likelihood; thus, the data entropy as of the effective encryption system ought to be 8. The study's findings are presented in Fig. 2. The findings indicate that the mean outcomes of the encrypted image utilizing the suggested scheme are approximately 8, surpassing the method documented in the survey research, demonstrating the suggested technique's efficacy in countering this possibility.

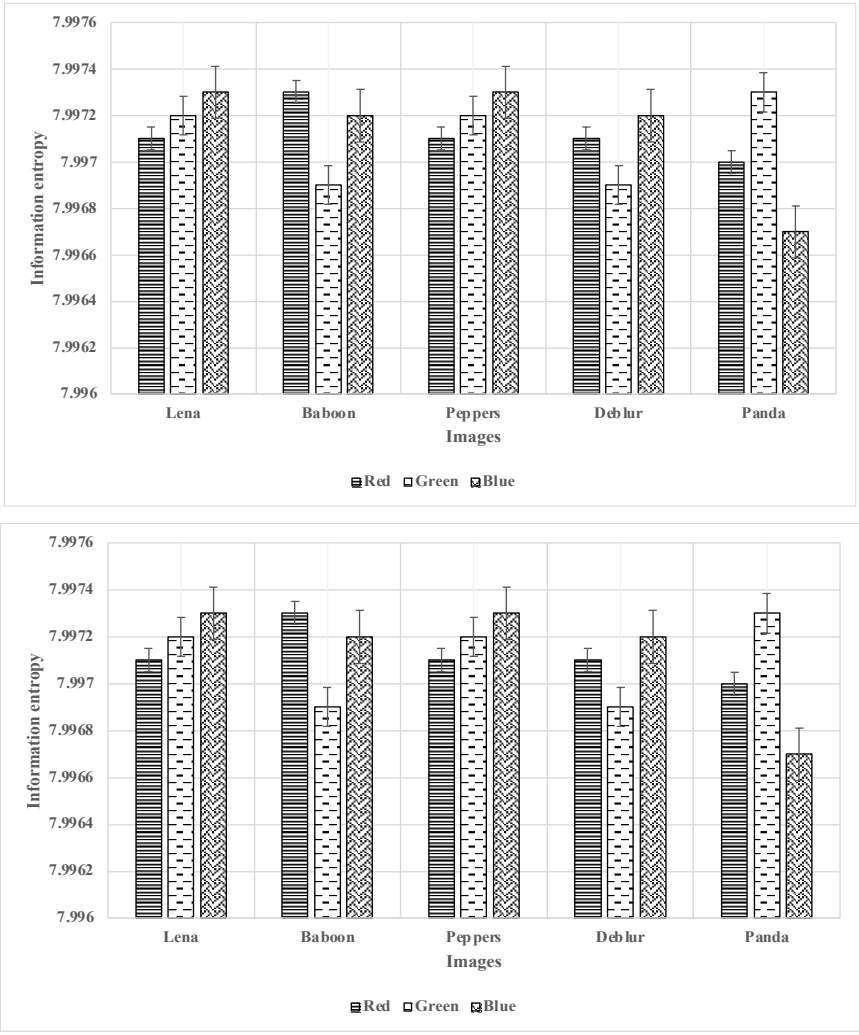


Fig. 2: Information entropy analysis (a) Original (b). Ciphered image

4.2 Randomness Assessment for Cipher

The safety of a cryptosystem encompasses several attributes, including longevity, evenly distributed complexity, and efficiency. To meet these requirements, the research assesses the unpredictability of the encrypted pictures. A segment of these tests consists of multiple subsets. The distorted Lena 24-bit digital picture is utilized to fulfill all evaluations. Numerous initial keys are used to assess the unpredictability of the figures. The secret information is a colorful picture of Lena measuring 256 × 256 pixels. These results indicate that the proposed digital image encryption technique meets standards. Based on the results, the encryption method's generated random encryption algorithms can be characterized as very unequal in their outputs.

Conclusion

This study presents an innovative image encryption method utilizing 256 components from 16 Galois domains and Zn, a circle of integers multiplied by n. A substitution-permutation arrangement is employed to create a novel encryption system. The ambiguity among the principal flows, and the cipher picture has intensified. Incorporating the diffusion level enhanced the security degree of the suggested strategy. The robustness of the algorithm for encryption is assessed using several statistical techniques. The picture quality checks for the proposed encryption technique applied to the Lena picture yielded results that met the established standards. Thus, upon contrast, it is determined that the suggested 2-algebraic structures-based picture security method significantly outperforms other current chaos-based picture encryption algorithms. From a futuristic standpoint, the research expands this study to encompass many data formats, including speech, message, sound, and visual.

References

Silvano, W. F., & Marcelino, R. (2020). Iota Tangle: A cryptocurrency to communicate Internet-of-Things data. *Future generation computer systems*, *112*, 307-319. https://doi.org/10.1016/j.future.2020.05.047

Banerjee, S. (2024). Exploring Cryptographic Algorithms: Techniques, Applications, and Innovations. *International Journal of Advanced Research in Science, Communication and Technology,* 607-620. https://doi.org/607-620. 10.48175/ijarsct-18097

Zahid, A. H., Al-Solami, E., & Ahmad, M. (2020). A novel modular approach based substitution-box design for image encryption. *IEEE Access*, *8*, 150326-150340. https://doi.org/10.1109/ACCESS.2020.3016401

Nasr, M. A., El-Shafai, W., El-Rabaie, E. S. M., El-Fishawy, A. S., El-Hoseny, H. M., Abd El-Samie, F. E., & Abdel-Salam, N. (2024). A robust audio steganography technique based on image encryption using different chaotic maps. *Scientific Reports*, *14*(1), 22054. https://doi.org/10.1038/s41598-024-70940-3

Samiullah, M., Aslam, W., Khan, M. A., Alshahrani, H. M., Mahgoub, H., Abdullah, A. M., ... & Chen, C. M. (2022). Rating of Modern Color Image Cryptography: A Next-Generation Computing Perspective. *Wireless Communications and Mobile Computing*, *2022*(1), 7277992. https://doi.org/10.1155/2022/7277992

Joshua, E. S. N., Bhattacharyya, D., & Rao, N. T. (2022). Managing information security risk and Internet of Things (IoT) impact on challenges of medicinal problems with complex settings: a complete systematic approach. In *Multi-chaos, fractal and multi-fractional artificial intelligence of different complex systems* (pp. 291-310). Academic Press. https://doi.org/10.1016/B978-0-323-90032-4.00007-9

Abu-Faraj, M. A., Al-Hyari, A., & Alqadi, Z. (2022). A complex matrix private key to enhance the security level of image cryptography. *Symmetry*, *14*(4), 664. https://doi.org/10.3390/sym14040664

Liu, S., Li, C., & Hu, Q. (2021). Cryptanalyzing two image encryption algorithms based on a first-order time-delay system. *IEEE Multi Media*, *29*(1), 74-84. https://doi.org/10.1109/MMUL.2021.3114589