EUROPEAN JOURNAL OF PURE AND APPLIED MATHEMATICS
2025, Vol. 18, Issue 3, Article Number 6323
ISSN 1307-5543 – ejpam.com
Published by New York Business Global

A Novel RGB Image Encryption Scheme using Operations on Residue Classes of Eisenstein Integers $\mathbb{Z}[\omega]_\pi$

Muhammad Sajjad[1], Nawaf A. Alqwaifly[2,*]

[1] *NUTECH School of Applied Science and Humanities, National University of Technology, Islamabad, 44000, Pakistan*
[2] *Department of Electrical Engineering, College of Engineering, Qassim University, Saudi Arabia*

Abstract. This article presents a novel concept for enhancing multimedia security based on Eisenstein integers. The proposed approach is divided into two primary stages. In the first stage, S-boxes are constructed over the residue classes of Eisenstein integers using affine transformations, with all parameters derived from Eisenstein integers. This construction leverages the unique properties of Eisenstein integers, resulting in strong confusion and diffusion characteristics—essential elements of any secure cryptographic system. The second stage incorporates RGB image encryption using a Substitution-Permutation Network (SPN) framework, modified to operate over Eisenstein integers. This modification increases the complexity of image data transformations, thereby enhancing security. A comprehensive analysis of the proposed scheme's security and performance demonstrates its robustness against most known cryptographic attacks, along with greater efficiency in terms of computational and communication costs. The results clearly indicate that the integration of Eisenstein integers into SPN structures is a promising direction for developing effective and secure multimedia encryption methods.

2020 Mathematics Subject Classifications: 16S38, 11T71, 94A60

Key Words and Phrases: Eisenstein Integers, Multimedia Security, S-box Construction, Substitution-Permutation Network (SPN), Cryptography, Image Encryption

1. Introduction

Cryptography is the cornerstone of secure digital communication, ensuring confidentiality, integrity, and authenticity of data across various platforms. It encompasses a range of techniques and algorithms designed to protect information from unauthorized access and tampering. As digital communication expands—from emails to IoT and from cloud services to multimedia content—cryptography's scope broadens to safeguard text,

*Corresponding author.
DOI: https://doi.org/10.29020/nybg.ejpam.v18i3.6323

Email addresses: muhammad.sajjad@nutech.edu.pk (M. Sajjad), nkoiefly@qu.edu.sa (N. A. Alqwaifly)

voice, video, and image data. Classical ciphers such as RSA and AES have laid a strong foundation, yet modern challenges such as quantum computing, real-time image and video processing, and storage-sensitive systems necessitate more robust, efficient, and domain-specific cryptographic tools. Cryptographic primitives such as substitution-permutation networks (SPNs), elliptic curves, lattice-based schemes, and chaos theory are actively researched to meet these evolving challenges [1]. Among these, image encryption using algebraic structures and number theory has emerged as a promising area, especially for multimedia and medical imaging, where traditional schemes fail to meet performance or security thresholds. This article contributes to this domain by integrating Eisenstein integers into the design of nonlinear cryptographic components for RGB image encryption.

Substitution boxes (S-boxes) are fundamental components in symmetric key cryptography, particularly in block ciphers like DES and AES, and are primarily responsible for ensuring the confusion property as defined by Claude Shannon. S-boxes are nonlinear mappings that substitute input bits with output bits, thereby complicating the relationship between the ciphertext and the key. The strength of an S-box lies in its resistance to cryptanalytic attacks such as linear and differential cryptanalysis. Over the years, numerous S-box construction techniques have been developed, from algebraic methods over finite fields [2] to chaos-based and group-theoretic approaches [3–8]. For instance, chaotic systems like Lorenz and Baker maps offer nonlinearity and initial sensitivity, which can be leveraged for S-box generation [3, 5]. More recently, researchers have introduced cryptographic components over exotic number systems like Gaussian [9–12], quaternion [13, 14], and Eisenstein integers [15, 16], utilizing their algebraic richness to construct highly nonlinear and structurally complex S-boxes. This work follows a similar trajectory but uniquely applies affine transformations over the residue classes of Eisenstein integers, thus producing novel and secure S-boxes for RGB image encryption.

Eisenstein integers form a subset of complex numbers defined as $\mathbb{Z}[\omega] = \{a + b\omega \mid a, b \in \mathbb{Z}\}$, where $\omega = e^{2\pi i/3}$ is a primitive cube root of unity. These numbers constitute a unique factorization domain with significant applications in number theory, algebraic geometry, and, more recently, coding and cryptography [15–18]. Their ring structure permits operations analogous to those in $\mathbb{Z}$ and $\mathbb{Z}[i]$ (Gaussian integers), making them suitable for defining residue classes, ideals, and modular arithmetic. This algebraic richness and the underlying hexagonal lattice structure provide unique opportunities for designing cryptographic algorithms with enhanced resistance to linear and differential attacks. In image encryption, Eisenstein integers offer a promising basis for constructing substitution boxes, defining modular transformations, and encoding image pixels with non-standard algebraic operations, thereby increasing entropy and resistance to statistical analysis.

1.1. Literature Review

The field of cryptographic image encryption has witnessed an explosion of innovation, driven by the need for secure transmission and storage of visual data. A foundational perspective is given by Schneier [1], establishing the fundamental principles of cryptographic algorithms. A significant line of work has emerged focusing on the algebraic and

group-theoretic construction of S-boxes and nonlinear cryptographic components. Shah and Qureshi [2], Sajjad et al. [11], and Iqtadar et al. [4] explored Galois fields and group theory for robust S-box design. Recent advancements show a shift toward using Gaussian [9, 10, 12], Eisenstein [15, 16], and quaternion integers [13, 14] for cryptographic primitives, exploiting their nontrivial algebraic strctures. In the domain of Eisenstein integers specifically, Huber [17] introduced early work on coding over Eisenstein-Jacobi integers, while Valmir [18] investigated factor rings and their arithmetic, laying the groundwork for cryptographic application. Sajjad et al. [15, 16] have made critical contributions to the field with the construction and decoding of BCH codes and alternant codes over Eisenstein integers, highlighting their utility in secure communication systems. These works establish the mathematical groundwork for our proposed encryption scheme.

Parallel developments in image encryption have leveraged chaotic maps, dynamic systems, and hybrid techniques for robust encryption. Zhang et al. [19] and Huang et al. [20] demonstrated the use of permutation-diffusion schemes integrated with chaotic maps. Teng et al. [21], Liu et al. [22], and Chen et al. [23] pushed this further with simultaneous permutation-diffusion architectures, while El-Damak et al. [24] and Zefreh [25] employed Fibonacci matrices and Latin squares. Enayatifar et al. [26], Malik and Shah [27], and Zhao et al. [6] integrated DNA sequences and hyperchaotic structures, indicating a trend toward biologically and physically inspired models. Novel applications also include quantum walks [28] and chaotic PRNGs [8], expanding the cryptographic design space. Furthermore, Sajjad and collaborators [10, 12–14] have developed several SPN-based image encryption schemes over complex algebraic structures including Gaussian, quaternion, and Eisenstein integers. Their works demonstrate enhanced security metrics—NPCR, UACI, entropy—through algebraic modifications in SPN structures. Yao et al. [29], Özpolat et al. [8], and Rani [30] add to this with asymmetric encryption, hybrid transformations, and modified encoding schemes, respectively. Alexan et al. [31] and Yakubu et al. [32] underscore the growing need for fast, chaos-based, and scalable encryption solutions. In parallel, Pandian [33, 34] explored code bounds over finite rings, which serve as important theoretical underpinnings for algebra-based encryption schemes.

1.2. Motivation

Despite the rich variety of image encryption techniques, many existing systems suffer from either high computational overhead or weak algebraic foundations. Chaos-based schemes, while effective in achieving high entropy, often lack algebraic transparency and are susceptible to parameter estimation attacks. Conversely, purely algebraic models sometimes fail to provide sufficient nonlinearity or are computationally rigid. There is a strong motivation to bridge this gap by constructing cryptographic primitives—specifically S-boxes—within a well-structured, mathematically rigorous algebraic system. Eisenstein integers present a compelling candidate due to their unique factorization, modular structure, and suitability for residue class construction. Integrating these with SPN architectures, which are proven frameworks for strong encryption, provides an opportunity to design a secure, efficient, and mathematically elegant image encryption scheme. Furthermore, the

cryptographic potential of Eisenstein residue classes remains underexplored in multimedia security, warranting a detailed investigation.

1.3. Contribution

This article proposes a novel RGB image encryption scheme based on the residue classes of Eisenstein integers $\mathbb{Z}[\omega]_\pi$, combining the strengths of algebraic number theory with the proven architecture of Substitution-Permutation Networks (SPNs). Our contributions are multi-fold. First, we construct cryptographically secure S-boxes using affine transformations over Eisenstein residues, ensuring high nonlinearity and the avalanche effect. Second, we design a modified SPN framework tailored to RGB images, where both substitution and permutation stages operate over Eisenstein integers, thereby enhancing confusion and diffusion. Third, we evaluate the proposed scheme using a comprehensive suite of cryptographic tests—NPCR, UACI, entropy, PSNR, MSE, histogram uniformity, correlation coefficients, and the NIST randomness test suite—demonstrating superior security and efficiency. Finally, our approach generalizes to a broader class of algebraic rings, offering a versatile template for future multimedia encryption applications. This work not only introduces a novel technique but also expands the mathematical toolkit available to cryptographic engineers.

2. Eisenstein Integers an Their Properties [15–18]

The Eisenstein integers are a special class of complex numbers defined as $\mathbb{Z}[\omega] = \{a+b\omega : a, b \in \mathbb{Z}\}$, where ω is a primitive cube root of unity given by $\omega = e^{2\pi i/3} = \frac{-1+\sqrt{3}i}{2}$. These numbers form a commutative ring under addition and multiplication, which is closed under these operations. One of the fundamental properties of Eisenstein integers is their norm function, defined as

$$N(a + b\omega) = (a + b\omega)(\overline{a + b\omega}) = a^2 - ab + b^2,$$

which is multiplicative, meaning

$$N(z_1 z_2) = N(z_1)N(z_2).$$

This norm plays a crucial role in defining divisibility and prime elements within this number system.

The Eisenstein integers form a Euclidean domain, which means that division with remainder is possible, allowing the use of the Euclidean algorithm. As a result, $\mathbb{Z}[\omega]$ is also a Unique Factorization Domain (UFD), ensuring that every element can be uniquely factored into Eisenstein prime numbers, similar to the prime factorization of integers. The units (invertible elements) in this ring are the elements whose norm equals 1, which include $\pm 1, \pm\omega, \pm\omega^2$, forming a cyclic group of order 6. A number in $\mathbb{Z}[\omega]$ is considered Eisenstein prime if either it remains prime in the rational integers $\mathbb{Z}$ and is congruent to 2 (mod 3) (i.e., of the form $3k-1$, such as 2, 5, 11, etc.), or if it has a norm that is a rational prime.

Due to their algebraic structure, Eisenstein integers form a triangular (hexagonal) lattice in the complex plane, which is denser than the square lattice of Gaussian integers. This makes them useful in fields such as cryptography, coding theory, and signal processing. Modular arithmetic in $\mathbb{Z}[\omega]$ follows principles similar to those in $\mathbb{Z}$, with moduli taken from Eisenstein integers. These numbers have applications in algebraic number theory, cryptography, error-correcting codes, algebraic geometry, and even physics, where they appear in problems involving tiling, lattice-based security protocols, and number-theoretic cryptographic constructions.

Theorem 1. *[17, 18] For each odd rational prime $p \in \mathbb{N}$, there exists a prime $\pi \in \mathbb{Z}[\omega]$ such that*

$$N(\pi) = p = \pi\overline{\pi}.$$

In particular, p is not a prime element in $\mathbb{Z}[\omega]$.

Theorem 2. *[17, 18] An element $\pi \in \mathbb{Z}[\omega]$ is prime in $\mathbb{Z}[\omega]$ if and only if its norm $N(\pi)$ is a prime number in $\mathbb{Z}$.*

2.1. Residue Class of Eisenstein Integers [17, 18]

Let $\mathbb{Z}[\omega]_\pi$ denote the residue class ring of Eisenstein integers modulo π, where $\pi \in \mathbb{Z}[\omega]$. Then, the modulo function f is defined as:

$$f : \mathbb{Z}[\omega] = \{a + b\omega : a, b \in \mathbb{Z}\} \to \mathbb{Z}[\omega]_\pi,$$

$$f(x) = y \pmod{\pi} = x - \left[\frac{x\bar{\pi}}{\pi\bar{\pi}}\right]\pi,$$

where $y \in \mathbb{Z}[\omega]_\pi$, and $\bar{\pi}$ denotes the complex conjugate of π. This equation involves rounding the quotient $[\cdot]$ to the nearest Eisenstein integer. To perform Eisenstein integer (EI) rounding, the real and imaginary components (i.e., the non-ω part and the coefficient of ω) are independently rounded to the nearest integers.

2.2. Eisenstein Mannheim Weight and Eisenstein Mannheim Distance [17, 18]

Let $\alpha, \beta \in \mathbb{Z}[\omega]_\pi$, and define $\gamma = \alpha - \beta = a_1 + b_1\omega \pmod{\pi}$. Then, the **Eisenstein Mannheim (EM) weight** of γ is given by:

$$W_{\mathrm{EM}}(\gamma) = |a_1| + |b_1|.$$

Accordingly, the Eisenstein Mannheim distance between α and β is defined as:

$$d_{\mathrm{EM}}(\alpha, \beta) = W_{\mathrm{EM}}(\gamma).$$

Theorem 3. *[17] Indeed, the Eisenstein Mannheim weight W_{EM} defines a metric on the residue class ring $\mathbb{Z}[\omega]_\pi$.*

Theorem 4. *[17] If* $\gcd(a,b)=1$*, then the quotient ring* $\mathbb{Z}[\omega]/\langle a+b\omega\rangle$ *is isomorphic to the finite field* $\mathbb{Z}_{a^2-ab+b^2}$*.*

Theorem 5. *[17] Let* $\pi_k = a_k + b_k\omega$ *be distinct primes in* $\mathbb{Z}[\omega]$*, and let* $p_k = \mathbb{Z}_{a_k^2-a_kb_k+b_k^2}$ *be the corresponding distinct rational primes in* $\mathbb{Z}$*, where* $k=1,2,3,\ldots,m$*. If* α *is a generator of the multiplicative group* $\mathbb{Z}[\omega]/\langle\pi_k\rangle$*, then*

$$\alpha^{\frac{\varphi(p_k)}{2}} \equiv -1 \pmod{\pi_k}.$$

Theorem 6. *[17, 18] Let* $\pi = a+b\omega$ *be an Eisenstein prime in* $\mathbb{Z}[\omega]$*, where the norm of* π *is* $N(\pi)=a^2-ab+b^2=p$*, a prime in* $\mathbb{Z}$*. If* $\mathbb{Z}[\omega]_\pi$ *is a finite field generated by* α*, then*

$$\alpha^{\varphi(p)} \equiv 1 \pmod{\pi},$$

where $\varphi(p)$ *is Euler's totient function.*

3. Algorithm for Proposed $n \times n$ S-boxes over Eisenstein Integers Residue Class

The construction of $n \times n$ S-boxes over the Eisenstein integers residue class involves leveraging the algebraic properties of Eisenstein integers to design nonlinear substitution functions for cryptographic applications. An S-box, or substitution box, is a fundamental component in block ciphers, ensuring security by introducing confusion, which helps protect against various cryptanalytic attacks. When defined over the Eisenstein integers residue class—where numbers are taken modulo a specific Eisenstein integer—the S-box elements form a structured yet complex arrangement that enhances security. Unlike traditional S-boxes based on finite fields, the use of Eisenstein integers introduces additional algebraic properties that improve resistance to differential and linear cryptanalysis. The design process begins by selecting a suitable modulus, defining a nonlinear transformation function, and ensuring that the S-box remains bijective, meaning every input maps uniquely to an output. Subsequent steps involve computing the residue class elements, applying a permutation strategy, and validating key cryptographic properties such as nonlinearity, differential uniformity, and the avalanche effect. By leveraging Eisenstein integers in this manner, the resulting S-box achieves a higher level of security, making it particularly useful in encryption algorithms, secure communication protocols, and lightweight cryptographic systems. The following steps describe the algorithm for constructing $n \times n$ S-boxes over the Eisenstein integers residue class. A method to construct S-boxes using Eisenstein integers proceeds as follows:

(i) **Generation of Residue Class R Using the Modulo Function:** The first step involves generating a residue class R using the modular function defined by

$$f(x) = y \pmod{\pi} = x - \left\lfloor \frac{x\overline{\pi}}{\pi\overline{\pi}} \right\rfloor \pi,$$

where x is an element of the given algebraic structure, π is a prime element in that structure, and $\overline{\pi}$ denotes the conjugate of π. The floor operation $\lfloor \cdot \rfloor$ represents the integer quotient of $\frac{x\overline{\pi}}{\pi\overline{\pi}}$. This operation ensures the result remains within a defined fundamental domain, producing a well-structured set of residue classes. This step establishes a finite and controlled set of elements for subsequent processing.

(ii) **Reduction of Elements Using Modulo p to Obtain R^*:** Once the residue class R is generated, it undergoes further reduction by applying modulo p to all its elements, resulting in a new set denoted as R^*. This step confines the elements of R within a finite field $\mathbb{Z}/p\mathbb{Z}$ or an analogous structure in higher-dimensional number systems. By performing this reduction, the elements are mapped into a smaller, more manageable set used for further mathematical transformations. This process is essential for uniformity and computational efficiency in the cryptographic construction of the S-box.

(iii) **Application of Affine Transformation:** In this step, two elements

$$a = (x_1, y_1) \quad \text{and} \quad b = (x_2, y_2)$$

are selected from the multiplicative group R^*. Here, x_1 and x_2 are the non-ω parts, while y_1 and y_2 are the ω parts of elements in R^*. The affine transformation is then applied to all elements x_i in R^* as

$$g(x) = ax_i^{-1} + b,$$

where x_i^{-1} represents the modular inverse of x_i, and a must be nonzero to ensure invertibility. This transformation introduces both diffusion and confusion properties, which are critical for cryptographic strength. It also provides nonlinearity, enhancing resistance against linear and differential cryptanalysis.

(iv) **Restriction of Values Using Modulo 256:** Since cryptographic S-boxes typically operate within an 8-bit space (values ranging from 0 to 255), all elements obtained from the affine transformation must be restricted to this range. To achieve this, a modulo 256 operation is applied to the transformed values, ensuring that all outputs fall within the permissible 8-bit range. This step aligns the generated values with standard cryptographic block sizes, enabling their direct use in encryption algorithms. Additionally, this restriction helps maintain uniformity in the final S-box structure.

(v) **Transformation of Elements into Matrices:** After restricting the values within the 8-bit range, the resulting elements are structured into matrices to form S-boxes. The values obtained in the previous step are arranged into two 16×16 matrices, which correspond to two separate 8×8 S-boxes. These 8×8 S-boxes serve as the final substitution boxes, essential components in block ciphers such as SPN-based cryptographic systems. This structured arrangement ensures efficient substitution operations during encryption and decryption.

(vi) **Iterative Process to Generate Multiple S-Boxes:** To obtain a diverse set of S-boxes with strong cryptographic properties, the affine transformation process (Step iii) is repeated for all possible values of a and b selected from R^*. Each unique pair (a, b) produces a distinct pair of 8×8 S-boxes. This iterative process results in a large number of different S-boxes, each possessing unique nonlinearity and diffusion properties. The diversity of these S-boxes enhances security by making cryptanalysis more difficult, as different keys or settings can use different S-boxes within the same cryptographic system. This step ensures flexibility and robustness in the encryption algorithm by providing multiple cryptographically strong S-box options.

Significance of the Pair of S-boxes

The S-boxes generated through this algorithm play a crucial role in modern cryptographic systems, ensuring the security and robustness of encryption techniques. Their primary function is to introduce confusion in substitution-permutation networks (SPNs) and block ciphers, making them resistant to various forms of cryptanalysis. By carefully selecting elements from a residue class and applying a series of transformations, the algorithm constructs S-boxes with desirable cryptographic properties such as strong diffusion and resistance to differential and linear attacks. The modular reduction in the early steps ensures that the generated elements belong to a controlled finite set, leading to well-distributed and structured S-boxes. The affine transformation step significantly enhances the unpredictability of the S-boxes, making it difficult for attackers to exploit algebraic structures or patterns. Moreover, the application of modulo 256 ensures that the resulting values conform to standard 8-bit encryption formats, essential for practical implementation in secure communication systems. The final transformation of these values into structured 8×8 matrices allows direct integration into cryptographic frameworks such as AES-like ciphers. Additionally, the iterative generation of multiple S-boxes through varying parameters ensures flexibility and adaptability, allowing different encryption settings to use distinct S-boxes, thereby increasing complexity for attackers attempting to decipher the encryption scheme. The construction process also guarantees that each generated S-box exhibits a strong avalanche effect, meaning that a small change in input results in a significant and unpredictable change in output, further strengthening its cryptographic strength. As a result, these S-boxes provide an essential layer of security in encryption protocols, contributing to the overall integrity, confidentiality, and robustness of modern digital communication and data protection systems.

4. Applications and Analysis of 8×8 S-boxes over the Residue Classes of Eisenstein Integers

This approach is specifically applied to the Eisenstein prime $E = 84 + 25\omega$, with a prime modulus of 5581, in order to compare its performance with S-boxes derived from elliptic curves, chaotic maps, and Gaussian primes. In this construction, the non-ω and ω components of the Eisenstein integers are treated as the x and y coordinates, respectively.

Using the proposed algorithm, S-boxes S_1 and S_2 are generated based on the prime 5581 and are systematically presented in Tables 1 and 2. These S-boxes are developed following the structured steps of the algorithm, ensuring a rigorous transformation process that maintains cryptographic strength and enhances security properties such as diffusion and resistance to attacks. This comparative approach allows for a deeper understanding of how Eisenstein primes contribute to the design of secure S-boxes in modern encryption systems.

Table 1: S-box of X-coordinates S_1

120	249	56	89	114	234	116	21	79	152	143	176	75	142	226	163
232	15	126	39	254	62	153	244	190	245	184	233	117	210	208	9
175	136	235	88	135	32	177	154	201	204	119	169	2	158	35	31
46	207	43	181	5	124	246	65	160	187	60	230	111	214	241	82
213	4	110	14	223	173	179	134	215	242	13	168	148	137	224	138
198	203	28	180	182	45	228	253	172	220	27	41	24	104	146	165
26	59	209	42	54	98	171	86	85	83	248	188	90	128	121	76
161	81	100	227	57	132	115	73	66	25	12	34	112	18	193	84
196	155	191	159	178	255	71	95	64	47	94	127	16	237	141	218
77	55	229	101	44	33	91	205	250	217	197	49	78	145	97	251
216	36	99	231	162	147	199	87	23	8	7	183	70	129	170	102
125	105	211	186	103	157	52	144	156	247	240	58	225	67	38	131
189	92	107	50	11	221	130	174	236	48	68	239	22	29	185	133
61	69	106	194	150	222	19	212	195	151	80	238	0	252	40	149
200	113	167	202	166	108	206	192	20	6	219	63	164	53	122	109
96	37	93	17	1	118	140	72	3	30	51	123	74	243	10	139

4.1. Security Analysis of the Proposed S-boxes

Once the S-boxes have been constructed, it is essential to evaluate their effectiveness. In this section, we perform a comprehensive security analysis of the newly designed S-boxes to assess their cryptographic strength. Specifically, the proposed S-boxes are analyzed with respect to several key parameters: nonlinearity, strict avalanche criterion (SAC), bit independence criterion (BIC), linear approximation probability (LAP), and differential approximation probability (DAP). These criteria are widely employed to measure the robustness and resistance of S-boxes against various cryptanalytic attacks.

4.1.1. Bijectivity of S-Boxes Generated by Eisenstein Integers

The S-boxes generated from the residue classes of Eisenstein integers are bijective since both the residue class construction and the applied transformations are bijections. Consequently, the inverses of the proposed S-boxes shown in Tables 1 and 2 exist.

Table 2: S-box of Y-coordinates S_2

248	121	184	217	242	106	244	149	207	24	15	48	203	14	98	35
104	143	254	167	126	190	25	116	62	117	56	105	245	82	80	137
47	8	107	216	7	160	49	26	73	76	247	41	130	30	163	159
174	79	171	53	133	252	118	193	32	59	188	102	239	86	113	210
85	132	238	142	95	45	51	6	87	114	141	40	20	9	96	10
70	75	156	52	54	173	100	125	44	92	155	169	152	232	18	37
154	187	81	170	182	226	43	214	213	211	120	60	218	0	249	204
33	209	228	99	185	4	243	201	194	153	140	162	240	146	65	212
68	27	63	31	50	127	199	223	192	175	222	255	144	109	13	90
205	183	101	229	172	161	219	77	122	89	69	177	206	17	225	123
88	164	227	103	34	19	71	215	151	136	135	55	198	1	42	230
253	233	83	58	231	29	180	16	28	119	112	186	97	195	166	3
61	220	235	178	139	93	2	46	108	176	196	111	150	157	57	5
189	197	234	66	22	94	147	84	67	23	208	110	128	124	168	21
72	241	39	74	38	236	78	64	148	134	91	191	36	181	250	237
224	165	221	145	129	246	12	200	131	158	179	251	202	115	138	11

4.1.2. Nonlinearity

Nonlinearity is one of the key parameters that determines how effectively a cryptographic S-box can mask data to enhance security. In the context of an S-box defined over the Galois field $GF(2^8)$, nonlinearity measures the confusion capability, indicating how difficult it is for an adversary to deduce the input-output mapping. The nonlinearity of an S-box, denoted by $N(L)$, is defined as:

$$N(L) = \min_{\phi,\mu\in GF(2^8),\tau\in GF(2)} \left\{ y \in GF(2^8) : \phi \cdot L(x) \neq \mu \cdot y \oplus \tau \right\},$$

where $\phi, \mu \in GF(2^8)$ and $\tau \in GF(2)$.

A high nonlinearity value implies that the input-output transformation of the S-box is highly complex and non-linear, which is desirable for cryptographic security. Meier and Staffelbach (1990) identified nonlinearity as a critical parameter; however, they noted that it alone is insufficient, and other security properties must also be considered. They also showed that for an S-box over $GF(2^n)$, the nonlinearity $N(f)$ can be calculated by the formula:

$$N(f) = 2^{n-1} - 2^{\frac{n}{2}-1}.$$

Accordingly, it has been established that the optimal nonlinearity value for S-boxes over $GF(2^8)$ is 120. Tables 3, and 4 shows the NL results of the proposed study. And NL comparison between the proposed results and existing works is given in Table 11.

4.2. Bit Independent Criteria

The bit independence criterion (BIC) is a crucial security metric used to evaluate the strength of S-boxes in cryptographic applications. It ensures that changes in a single input

Table 3: NL of the S-box functions

S-boxes	$\mathbf{f_1}$	$\mathbf{f_2}$	$\mathbf{f_3}$	$\mathbf{f_4}$	$\mathbf{f_5}$	$\mathbf{f_6}$	$\mathbf{f_7}$	$\mathbf{f_8}$
S_1	106.0	108.0	106.0	108.0	106.0	106.0	110.0	108.0
S_2	106.0	108.0	106.0	108.0	106.0	106.0	110.0	108.0

Table 4: Nonlinearity values of the proposed S-boxes for Eisenstein prime 5581

S-boxes	**Prime**	**Parameters** (a, b)	**Minimum**	**Maximum**	**Average**
S_1	5581	$(7, 18), (12, 9)$	106	110	107.25
S_2	5581	$(8, 23), (16, 5)$	106	110	107.25

bit result in independent and unpredictable changes in the output bits, thereby increasing resistance to differential cryptanalysis. For the proposed $n \times n$ S-boxes constructed over the residue classes of Eisenstein integers, the BIC is analyzed to assess their robustness against various attacks. Specifically, BIC requires that for any pair of output bits y_i and y_j, their correlation should be minimal when a single input bit x_k is flipped. Mathematically, BIC can be tested using the strict avalanche criterion (SAC), which ensures that

$$p(y_i : x_k \text{ flipped}) \approx 0.5, \quad \text{for all } i \neq j \text{ and any input bit } x_k.$$

The Eisenstein integer-based residue class structure introduces additional algebraic complexity, leading to more unpredictable bit transformations within the S-box. The computed BIC values for the proposed S-boxes are compared with those of existing cryptographic S-boxes, demonstrating enhanced robustness against statistical and differential attacks. Tables 5, and 6 shows the SAC results of the proposed study. And SAC comparison between the proposed results and existing works is given in Table 11.

Table 5: BIC of S_1

0.0000	0.5254	0.4863	0.5059	0.5000	0.5020	0.4941	0.5000
0.5254	0.0000	0.4902	0.5137	0.4980	0.4785	0.5059	0.5020
0.4863	0.4902	0.0000	0.5215	0.5313	0.5000	0.5195	0.4863
0.5059	0.5137	0.5215	0.0000	0.4746	0.4824	0.5254	0.4922
0.5000	0.4980	0.5313	0.4746	0.0000	0.5156	0.4863	0.5098
0.5020	0.4785	0.5000	0.4824	0.5156	0.0000	0.4824	0.4980
0.4941	0.5059	0.5195	0.5254	0.4863	0.4824	0.0000	0.5195
0.5000	0.5020	0.4863	0.4922	0.5098	0.4980	0.5195	0.0000

4.3. Strict Avalanche Criterion

The strict avalanche criterion (SAC) is an essential property for evaluating the security of cryptographic S-boxes. It ensures that a small change in the input, such as flipping a single bit, results in significant and unpredictable changes in the output. A strong SAC property is critical for resistance against differential and linear cryptanalysis, as it

Table 6: BIC of S_2

0.0000	0.5254	0.4863	0.5059	0.5000	0.5020	0.4941	0.5000
0.5254	0.0000	0.4902	0.5137	0.4980	0.4785	0.5059	0.5020
0.4863	0.4902	0.0000	0.5215	0.5313	0.5000	0.5195	0.4863
0.5059	0.5137	0.5215	0.0000	0.4746	0.4824	0.5254	0.4922
0.5000	0.4980	0.5313	0.4746	0.0000	0.5156	0.4863	0.5098
0.5020	0.4785	0.5000	0.4824	0.5156	0.0000	0.4824	0.4980
0.4941	0.5059	0.5195	0.5254	0.4863	0.4824	0.0000	0.5195
0.5000	0.5020	0.4863	0.4922	0.5098	0.4980	0.5195	0.0000

enhances the diffusion characteristics of the S-box. For the proposed $n \times n$ S-boxes over the residue classes of Eisenstein integers, SAC is assessed by analyzing the probability that each output bit changes when a single input bit is flipped. Ideally, this probability should be close to 0.5, meaning that each output bit is equally likely to change, regardless of the input modification. Mathematically, SAC can be expressed as:

$$P(y_i : x_k \text{ flipped}) \approx 0.5, \quad \forall i, \quad \forall k,$$

where y_i is the i-th output bit and x_k is the k-th input bit. The unique algebraic properties of Eisenstein integers contribute to improved randomness and diffusion in the generated S-boxes. The SAC values obtained for the proposed S-boxes are compared with those of traditional S-boxes, demonstrating their effectiveness in cryptographic applications. Detailed SAC evaluation results are presented in the tables, confirming the robustness of the proposed method in achieving strong avalanche effects. Tables 7, and 8 shows the SAC results of the proposed study. And SAC comparison between the proposed results and existing works is given in Table 11.

Table 7: SAC Analysis of Proposed S-box S_1 over the Non-Omega Part of Eisenstein Integers

0.5625	0.40625	0.5	0.5	0.53125	0.515625	0.484375	0.484375
0.5	0.484375	0.53125	0.5625	0.46875	0.515625	0.5	0.5
0.484375	0.4375	0.40625	0.515625	0.515625	0.546875	0.546875	0.515625
0.421875	0.5625	0.515625	0.421875	0.453125	0.515625	0.5	0.453125
0.46875	0.53125	0.5	0.53125	0.5	0.4375	0.53125	0.53125
0.5	0.484375	0.546875	0.53125	0.515625	0.421875	0.515625	0.484375
0.46875	0.5	0.5	0.546875	0.484375	0.40625	0.4375	0.484375
0.53125	0.515625	0.453125	0.453125	0.53125	0.46875	0.5625	0.453125

4.4. Linear Approximation Probability

Some of the important aspects measured in S-boxes and cryptographic functions, with respect to linear cryptanalysis, include the *linear approximation probability* (LAP). LAP is used to estimate the dependence between linear combinations of input and output bits of a

Table 8: SAC Analysis of Proposed S-box S_2 over the Omega Part of Eisenstein Integers

0.5625	0.40625	0.5	0.5	0.53125	0.515625	0.484375	0.484375
0.5	0.484375	0.53125	0.5625	0.46875	0.515625	0.5	0.5
0.484375	0.4375	0.40625	0.515625	0.515625	0.546875	0.546875	0.515625
0.421875	0.5625	0.515625	0.421875	0.453125	0.515625	0.5	0.453125
0.46875	0.53125	0.5	0.53125	0.5	0.4375	0.53125	0.53125
0.5	0.484375	0.546875	0.53125	0.515625	0.421875	0.515625	0.484375
0.46875	0.5	0.5	0.546875	0.484375	0.40625	0.4375	0.484375
0.53125	0.515625	0.453125	0.453125	0.53125	0.46875	0.5625	0.453125

cryptographic function. Larger values of LAP indicate higher amounts of non-linearity in the function, which in turn implies a higher complexity for an attacker to solve. Therefore, larger LAP values mean it is easier to protect against linear cryptanalysis. Mathematically, for a cryptographic function $f : \{0,1\}^n \to \{0,1\}^m$, the LAP is defined as:

$$\mathrm{LAP}(f) = \max_{a,b\in\{0,1\}^n\setminus\{0\}} \left| \frac{1}{2^n} \sum_{x\in\{0,1\}^n} (-1)^{a\cdot x\oplus b\cdot f(x)} \right|,$$

where a and b are binary vectors, $a\cdot x$ and $b\cdot f(x)$ represent the dot products modulo 2, and $\oplus$ denotes the exclusive XOR operation. The LAP value reveals the degree of maximum correlation between the approximate local linear fit and the ideal uniform distribution. The closer the LAP value of an ideal cryptographic function or S-box is to zero, the more independent the output is from any linear function of the input. This property is crucial to counteract top attacking strategies that exploit linear dependencies.

The LAP values for both proposed S-boxes are the same, equal to 0.140625. LAP comparison between the proposed results and existing works is given in Table 11.

4.5. Differential Approximation Probability

The *differential approximation probability* (DAP) is a fundamental criterion for evaluating the resistance of an S-box against differential cryptanalysis. It quantifies the maximum probability that a specific input difference will result in a particular output difference when processed through the S-box. A lower DAP value indicates stronger security, as it reduces an attacker's ability to predict the propagation of differences through the cipher. For an S-box S, the DAP is defined as:

$$\mathrm{DAP}(S) = \max_{(\Delta x,\Delta y)\neq(0,0)} P\big(S(x)\oplus S(x\oplus\Delta x) = \Delta y\big),$$

where Δx represents the input difference, Δy represents the corresponding output difference, and $\oplus$ denotes the bitwise XOR operation. The proposed $n\times n$ S-boxes, constructed over the residue classes of Eisenstein integers, exhibit well-distributed differential behavior due to the algebraic structure of the Eisenstein field. The nonlinearity and affine

transformations incorporated in the design further enhance resistance against differential cryptanalysis. A comparative analysis of the DAP values of the proposed S-boxes with those of conventional S-boxes—such as those based on chaotic maps, elliptic curves, and Gaussian primes—is provided in tables. The results demonstrate that the proposed S-boxes achieve low DAP values, ensuring robustness against differential attacks and reinforcing their applicability in secure cryptographic systems. Tables 9, and 10 shows the DAP results of the proposed study. And DAP comparison between the proposed results and existing works is given in Table 11.

Table 9: DAP Analysis of Proposed S-box S_1 over the Non-ω Part of Eisenstein Integers

0.02344	0.02344	0.03125	0.03906	0.02344	0.02344	0.02344	0.03125	0.02344	0.03125	0.02344	0.03125	0.02344	0.02344	0.02344	0.02344
0.02344	0.03906	0.02344	0.02344	0.02344	0.03125	0.02344	0.03125	0.03125	0.02344	0.02344	0.02344	0.02344	0.02344	0.03125	0.02344
0.02344	0.03125	0.02344	0.03125	0.03125	0.02344	0.02344	0.02344	0.02344	0.03125	0.02344	0.02344	0.02344	0.03125	0.02344	0.03125
0.02344	0.02344	0.03125	0.03125	0.02344	0.03125	0.03125	0.02344	0.03906	0.02344	0.03906	0.03125	0.02344	0.02344	0.03125	0.03125
0.03125	0.02344	0.02344	0.02344	0.02344	0.02344	0.03125	0.02344	0.02344	0.02344	0.02344	0.02344	0.02344	0.02344	0.02344	0.02344
0.02344	0.02344	0.03125	0.03125	0.02344	0.02344	0.02344	0.02344	0.02344	0.02344	0.02344	0.02344	0.02344	0.02344	0.02344	0.02344
0.02344	0.03125	0.03125	0.02344	0.03125	0.03125	0.03125	0.02344	0.02344	0.03906	0.02344	0.02344	0.03125	0.02344	0.02344	0.03125
0.02344	0.03125	0.02344	0.03125	0.03125	0.02344	0.02344	0.02344	0.03125	0.03125	0.02344	0.02344	0.03125	0.02344	0.03125	0.03125
0.02344	0.02344	0.03125	0.03125	0.03906	0.02344	0.03125	0.03125	0.03125	0.02344	0.03906	0.02344	0.02344	0.02344	0.02344	0.02344
0.02344	0.02344	0.02344	0.02344	0.03125	0.02344	0.03125	0.02344	0.02344	0.02344	0.02344	0.03125	0.02344	0.03125	0.02344	0.02344
0.02344	0.02344	0.03125	0.02344	0.02344	0.01562	0.03125	0.02344	0.03906	0.03125	0.03125	0.03125	0.02344	0.02344	0.02344	0.02344
0.02344	0.03125	0.03125	0.02344	0.03125	0.02344	0.02344	0.02344	0.02344	0.03125	0.02344	0.03125	0.03906	0.02344	0.03125	0.02344
0.02344	0.03125	0.03125	0.03125	0.03125	0.02344	0.03125	0.02344	0.02344	0.03125	0.02344	0.02344	0.03125	0.02344	0.03125	0.03125
0.02344	0.02344	0.03125	0.03125	0.03125	0.03125	0.02344	0.02344	0.03906	0.03125	0.03125	0.03125	0.02344	0.02344	0.02344	0.02344
0.02344	0.02344	0.02344	0.02344	0.03125	0.02344	0.02344	0.02344	0.02344	0.02344	0.03125	0.02344	0.02344	0.02344	0.02344	0.02344
0.03906	0.02344	0.02344	0.03125	0.02344	0.02344	0.02344	0.03125	0.02344	0.03125	0.03125	0.03125	0.03906	0.03125	0.03125	0

Table 10: DAP Analysis of the Proposed S-box S_2 over the ω-Component of Eisenstein Integers

0.02344	0.02344	0.03125	0.03906	0.02344	0.02344	0.02344	0.03125	0.02344	0.03125	0.02344	0.03125	0.02344	0.02344	0.02344	0.02344
0.02344	0.03906	0.02344	0.02344	0.02344	0.03125	0.02344	0.03125	0.03125	0.02344	0.02344	0.02344	0.02344	0.02344	0.03125	0.02344
0.02344	0.03125	0.02344	0.03125	0.03125	0.02344	0.02344	0.02344	0.02344	0.03125	0.02344	0.02344	0.02344	0.03125	0.02344	0.03125
0.02344	0.02344	0.03125	0.03125	0.02344	0.03125	0.03125	0.02344	0.03906	0.02344	0.03906	0.03125	0.02344	0.02344	0.03125	0.03125
0.03125	0.02344	0.02344	0.02344	0.02344	0.02344	0.03125	0.02344	0.02344	0.02344	0.02344	0.02344	0.02344	0.02344	0.02344	0.02344
0.02344	0.02344	0.03125	0.03125	0.02344	0.02344	0.02344	0.02344	0.02344	0.02344	0.02344	0.02344	0.02344	0.02344	0.02344	0.02344
0.02344	0.03125	0.03125	0.02344	0.03125	0.03125	0.03125	0.02344	0.02344	0.03906	0.02344	0.02344	0.03125	0.02344	0.02344	0.03125
0.02344	0.03125	0.02344	0.03125	0.03125	0.02344	0.02344	0.02344	0.03125	0.03125	0.02344	0.02344	0.03125	0.02344	0.03125	0.03125
0.02344	0.02344	0.03125	0.03125	0.03906	0.02344	0.03125	0.03125	0.03125	0.02344	0.03906	0.02344	0.02344	0.02344	0.02344	0.02344
0.02344	0.02344	0.02344	0.02344	0.03125	0.02344	0.03125	0.02344	0.02344	0.02344	0.02344	0.03125	0.02344	0.03125	0.02344	0.02344
0.02344	0.02344	0.03125	0.02344	0.02344	0.01562	0.03125	0.02344	0.03906	0.03125	0.03125	0.03125	0.02344	0.02344	0.02344	0.02344
0.02344	0.03125	0.03125	0.02344	0.03125	0.02344	0.02344	0.02344	0.02344	0.03125	0.02344	0.03125	0.03906	0.02344	0.03125	0.02344
0.02344	0.03125	0.03125	0.03125	0.03125	0.02344	0.03125	0.02344	0.02344	0.03125	0.02344	0.02344	0.03125	0.02344	0.03125	0.03125
0.02344	0.02344	0.03125	0.03125	0.03125	0.03125	0.02344	0.02344	0.03906	0.03125	0.03125	0.03125	0.02344	0.02344	0.02344	0.02344
0.02344	0.02344	0.02344	0.02344	0.03125	0.02344	0.02344	0.02344	0.02344	0.02344	0.03125	0.02344	0.02344	0.02344	0.02344	0.02344
0.03906	0.02344	0.02344	0.03125	0.02344	0.02344	0.02344	0.03125	0.02344	0.03125	0.03125	0.03125	0.03906	0.03125	0.03125	0

4.5.1. Comparison of Proposed S-boxes with Existing Methods

The overlapping tests were conducted using well-known S-boxes derived from elliptic curves (EC), chaotic maps (CM), and other methods as described in [3, 5–8, 14]. These tests aimed to evaluate the efficacy of the proposed S-boxes, which are based on residue classes of Eisenstein integers (EI), in comparison to existing S-box designs. The results of the analysis for EC-, CM-, and EI-based S-boxes are summarized in Table 11, considering various cryptographic parameters. The findings indicate that the proposed S-boxes exhibit higher nonlinearity values than those derived from EC, CM, and several other schemes, implying stronger resistance to linear attacks. A unique feature of the proposed technique is its ability to generate a pair of S-boxes simultaneously by fixing three parameters:

a, b, and p. In contrast, other methods typically generate only a single S-box for a given set of parameter values. Table 11 further demonstrates that all proposed S-boxes in this study exhibit relatively high nonlinearity. This indicates improved capability in inducing confusion, thereby enhancing immunity against linear attacks. The SAC (Strict Avalanche Criterion) and BIC (Bit Independence Criterion) results for the proposed S-boxes are comparable to those of the S-boxes reported in [3, 5–8, 14]. This confirms that the diffusion properties of the proposed S-boxes are on par with those of well-established designs. Finally, the Differential Approximation Probability (DAP) analysis shows that the proposed S-boxes maintain competitiveness with those discussed in the aforementioned references. Therefore, it is reasonable to conclude that the proposed technique is effective in generating S-boxes with high resistance to differential cryptanalysis when compared to conventional approaches.

Table 11: Comparison of Proposed S-boxes with Existing Methods

S-box	**Type**	**NL**	**LAP**	**DAP**	**SAC Max**	**SAC Ave**	**SAC Min**	**BIC Max**	**BIC Ave**	**BIC Min**
S_1	EI	107.25	0.1406	0.0391	0.5625	0.4951	0.4063	0.6094	0.5017	0.4063
S_2	EI	107.25	0.1406	0.0391	0.5625	0.4951	0.4063	0.6094	0.5017	0.4063
[3]	EC	104.00	0.148	0.047	0.610	0.516	0.422	0.543	0.503	0.463
[5]	CM	106.00	0.148	0.023	0.609	0.500	0.391	0.525	0.499	0.473
[14]	QI	107.00	0.133	0.039	0.406	0.504	0.594	0.375	0.505	0.609
[6]	CM	104.25	0.133	0.039	0.594	0.498	0.406	0.5273	0.4990	0.4648
[7]	CM	104.00	0.148	0.039	0.625	0.508	0.391	0.531	0.501	0.471
[8]	CM	105.50	0.140	0.047	0.578	0.498	0.391	...	0.4976	...

5. RGB Image Algorithm over the Residue Classes of Eisenstein Integers

Encrypting images using Eisenstein integers enhances security due to the unique algebraic properties of these numbers. This method transforms pixel values or groups thereof into Eisenstein integers, allowing encrypted image data to be manipulated efficiently through mathematical operations. The encryption technique exploits specific characteristics of Eisenstein integers, enabling operations such as rotations, translations, and other arithmetic transformations that effectively distort the image. The densification and symmetry properties of Eisenstein integers increase resilience against various cryptographic attacks. Consequently, the proposed image encryption method ensures that encrypted image data remains secure and can be efficiently decrypted by the legitimate key holder without compromising image quality. The detailed steps of the proposed encryption process are outlined below:

(i) **Separation of RGB Channels:** An RGB image is first separated into its three constituent channels: Red, Green, and Blue. Let x represent the red channel, y the green channel, and z the blue channel. Each pixel is associated by combining coordinates in the form of (x, y) and (y, z).

(ii) **Separation of RGB Channels:** In this step, RGB pixel values are transformed

into Eisenstein integers. Confusion is achieved by utilizing the novel arithmetic properties of Eisenstein integers to permute pixel values in a non-linear and random manner. The Eisenstein integer system complicates basic operations like addition and multiplication, thereby strengthening encryption. Converting RGB pixel values into Eisenstein integers and performing mathematical operations such as multiplication in the residue classes significantly obscures the relationship between the original and encrypted pixel values. This ensures that even a minor alteration in the image results in a substantial difference in its encrypted form, enhancing overall security.

(iii) **Affine Transformation and Modulo Operations:** The pixel pairs (x, y) and (y, z) are multiplied using the result of an affine map under modulo 2^n, with residues taken as Eisenstein integers. The resulting transformed values are denoted as (x', y') and (y'', z''). The use of Eisenstein integers ensures that an attacker cannot easily reverse-engineer the altered image to recover the original.

(iv) **Diffusion Using S-Boxes:** The diffusion process is designed to propagate the effect of a single pixel change across the entire image, thereby eliminating the statistical characteristics of the original image. S-boxes (Substitution Boxes) are employed to transform values in a highly non-linear manner. This transformation is applied to RGB pixel values to produce new encrypted values. By applying two S-boxes to the pixel values and then performing operations such as permutation or bitwise mixing, the algorithm ensures that even a small change in the input results in a significant and unpredictable change in the encrypted image.

(v) **Final Permutation and Encryption Layers:** To further enhance diffusion, the outputs (x_i', y_i') are permuted using S-box 1, and (y_i'', z_i'') using S-box 2. The final encrypted values are obtained as follows:

- R = Encrypted red layer
- G_1 = First transformed green layer
- G_2 = Second transformed green layer
- B = Encrypted blue layer

The encrypted green layer is then calculated using the XOR operation: $G = G_1 \oplus G_2$.

(vi) **Assembly of Encrypted Image:** Finally, the complete encrypted image is assembled using the encrypted Red (R), Green (G), and Blue (B) layers. The resulting encrypted image is highly resistant to cryptographic attacks and retains its integrity under various conditions.

(vii) **Decryption Process:** The decryption process involves performing the reverse operations of the encryption process. By applying the inverse affine transformations, inverse S-box operations, and modular arithmetic, the original pixel values can be accurately recovered. This ensures that the image can be decrypted efficiently and reconstructed precisely by the authorized key holder.

5.1. Significance of RGB Image Encryption over the Residue Classes of Eisenstein Integers

The RGB image encryption algorithm over the residue classes of Eisenstein integers offers a highly secure approach to protecting digital images. By leveraging the unique algebraic properties of Eisenstein integers—a special set of complex numbers—this method enhances both the security and efficiency of image encryption, while providing resistance to various cryptographic attacks. One of the primary advantages of this technique is its ability to achieve strong confusion and diffusion: pixel values are permuted unpredictably, and small changes in the original image result in significant changes in the encrypted image. The encryption process involves modular arithmetic within the residue classes of Eisenstein integers. Operations such as modular multiplication and affine transformations render the reverse-engineering of the original image extremely difficult for potential attackers. The non-trivial multiplicative structure of Eisenstein integers increases the complexity of cryptanalytic methods such as brute-force, differential, and statistical attacks. Furthermore, this encryption method utilizes non-linear pixel transformations, moving beyond traditional encryption schemes that often rely on linear operations or simple XOR mappings. As a result, the encrypted pixel distribution becomes unpredictable, providing additional resistance against mathematical attacks. Another critical feature is its sensitivity to input variations, known as the avalanche effect: even a single-pixel change in the original image leads to a substantial difference in the encrypted result. This property ensures robust security and prevents attackers from deducing any meaningful patterns from the ciphertext. Despite its strong security attributes, the algorithm remains computationally efficient due to the rapid processing of modular arithmetic. This makes it suitable for real-time applications, including secure medical imaging, military communications, and confidential satellite image transmission. Moreover, the algorithm is robust against noise, compression artifacts, and transmission errors, maintaining its protective properties under adverse conditions such as lossy compression or network-based distortions. In summary, the RGB image encryption algorithm based on the residue classes of Eisenstein integers provides a powerful combination of complexity, robustness, and computational efficiency. It guarantees that encrypted image data remains unintelligible without the correct decryption key, while supporting practical deployment in modern digital security systems.

All steps of the proposed study are illustrated in Flowchart Figure 1.

6. Applications of RGB Image Encryption over the Residue Classes of Eisenstein Integers

The applications of RGB image encryption over the residue classes of Eisenstein integers span multiple fields where image security, confidentiality, and integrity are critical. The primary goal of this encryption approach is to transform visually meaningful images into noise-like encrypted images, ensuring that unauthorized users cannot extract any useful information. This technique is particularly valuable in medical imaging, where sensitive data such as MRI scans, CT scans, and X-rays must be securely stored and transmitted to

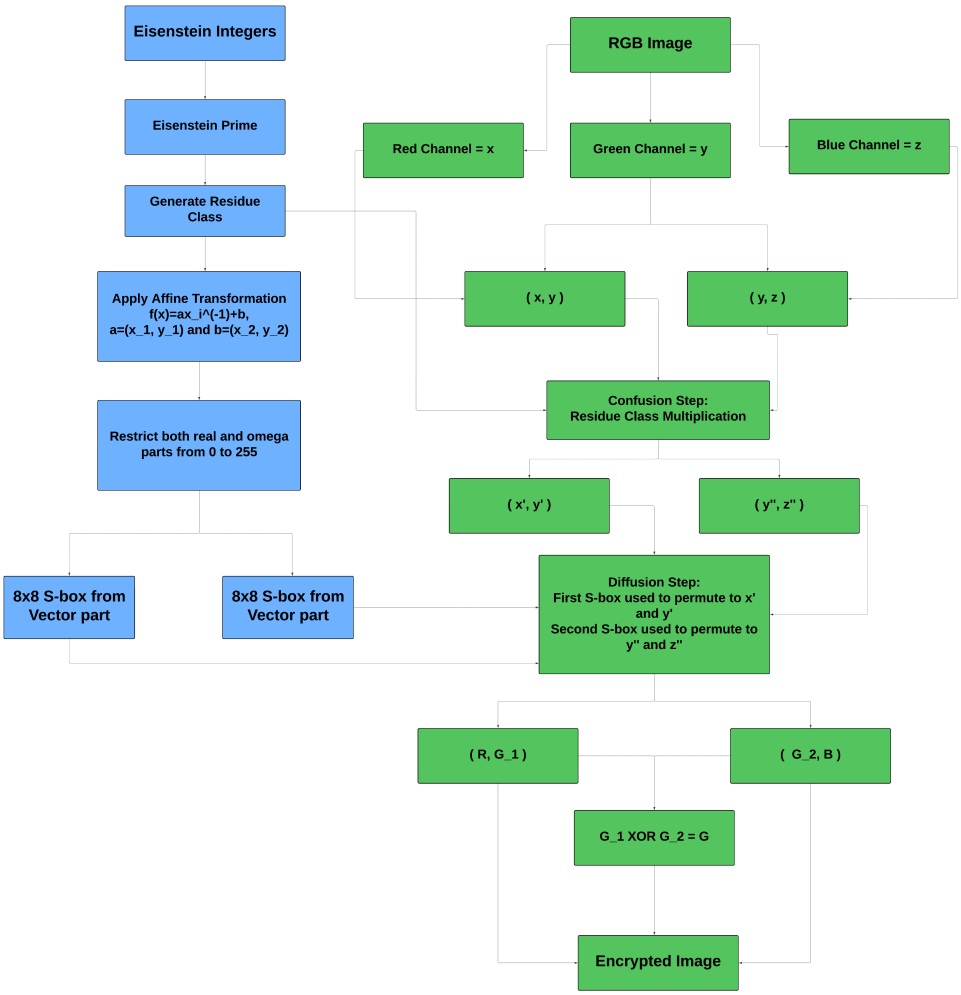

Figure 1: Flowchart of the Proposed Study

prevent unauthorized access or data breaches. Similarly, in military and defense applications, encrypted satellite images, reconnaissance photographs, and classified surveillance footage require robust protection against cyber threats and espionage. Financial institutions also rely on such encryption methods to secure documents containing sensitive graphical data, such as digital signatures, confidential reports, and transaction records. Digital forensics further benefits from this encryption approach, as it enables the secure storage of crime scene photographs and forensic evidence, preventing unauthorized modifications or leaks. The proposed encryption technique undergoes rigorous statistical analysis to verify its effectiveness in generating noise-like images. Key sensitivity analysis ensures that even a slight modification in the encryption key results in a completely different encrypted image, strengthening security against brute-force attacks. Key space analysis confirms that the algorithm has a sufficiently large key space, making it computationally infeasible for attackers to guess the correct key. Histogram analysis demonstrates how the

encryption process removes identifiable patterns by uniformly distributing pixel intensity values. Correlation analysis evaluates the independence between adjacent pixels, ensuring that no visual relationships remain in the encrypted image. Entropy analysis measures the randomness in encrypted images, validating their unpredictability. Figure 2 illustrates the transformation of original images, such as Earth, House, Sailboat on Lake, and Pepper, into encrypted versions, highlighting the effectiveness of this approach in securing digital images.

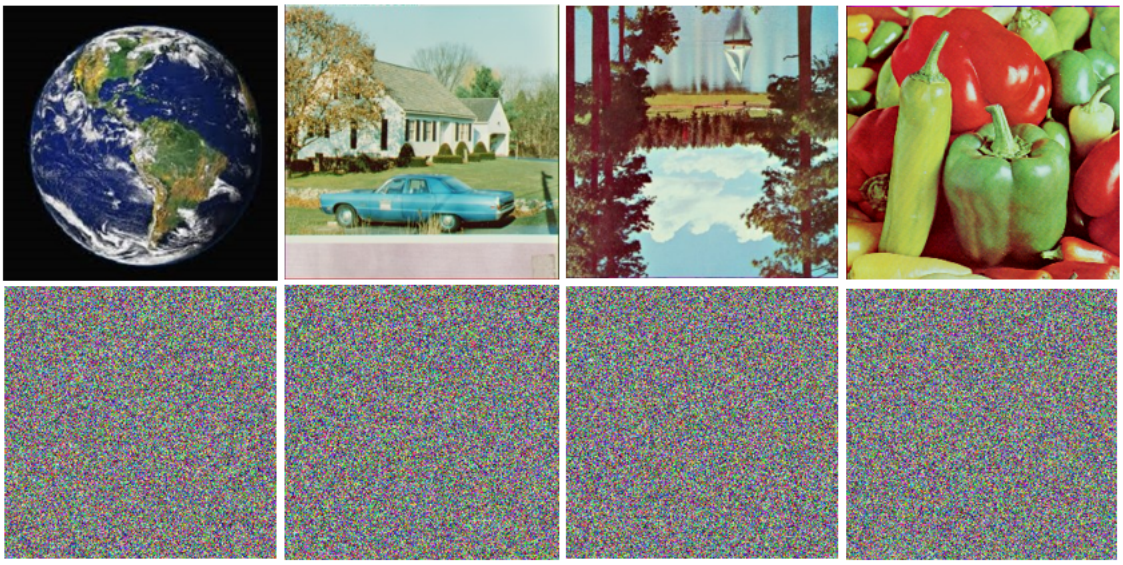

Figure 2: Eisenstein Integers based Original and Encrypted RGB Images

6.1. Histogram Analysis (HA)

Histogram analysis is a crucial statistical method used to evaluate the effectiveness of RGB image encryption over the residue classes of Eisenstein integers. In image encryption, a well-secured algorithm should ensure that the pixel intensity distribution of the encrypted image significantly differs from that of the original image, making it appear random and noise-like. The histogram of an image represents the frequency distribution of pixel intensities across its red, green, and blue channels. In an unencrypted image, the histogram typically exhibits distinct patterns corresponding to the visual characteristics of the image, such as variations in brightness and contrast. However, after encryption using the Eisenstein integer-based method, the histogram should become uniformly distributed, indicating that the encrypted image lacks recognizable patterns. This uniformity makes it nearly impossible for attackers to extract meaningful information through statistical analysis. The encryption process, which involves modular arithmetic and affine transformations over Eisenstein integers, ensures that pixel values are non-linearly transformed, leading to a more randomized histogram. Additionally, the diffusion properties of the encryption scheme contribute to equalizing the frequency of pixel intensities, further

eliminating correlations present in the original image. A well-distributed histogram also prevents attackers from utilizing frequency-based cryptanalysis techniques to reconstruct the original image. By comparing histograms of the original and encrypted images, the effectiveness of the encryption method can be validated. A highly uniform histogram confirms that the algorithm has successfully concealed the structural characteristics of the original image, ensuring strong security. The results of histogram analysis demonstrate that the encryption scheme significantly alters the statistical distribution of pixel intensities, making it a robust method for protecting digital images against unauthorized access and cryptographic attacks. The histogram analysis of original and Encrypted different images have been given in Figure 3.

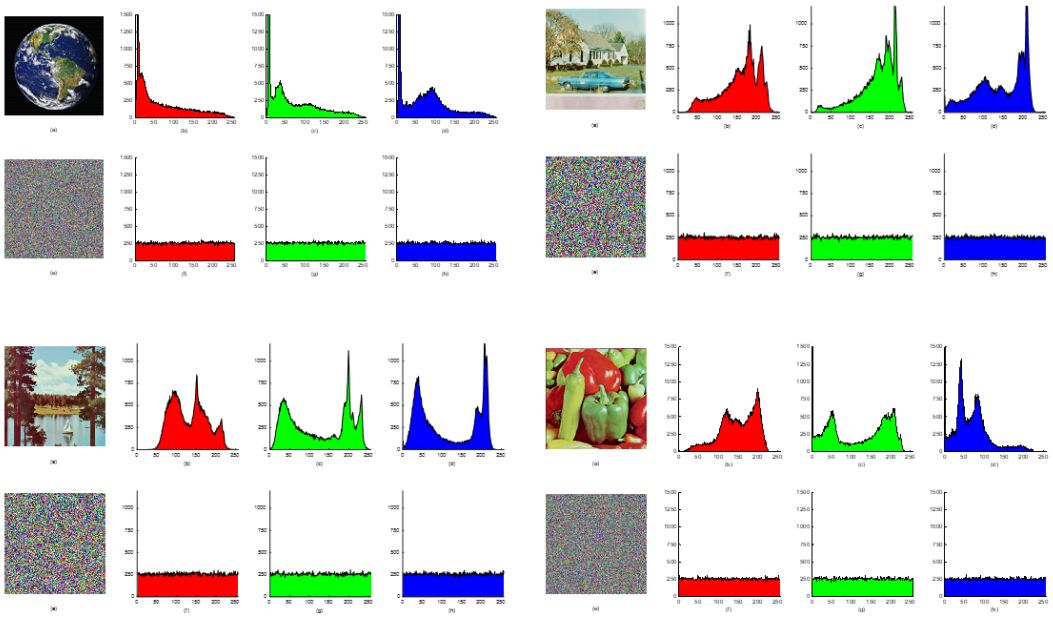

Figure 3: Histogram of Earth, House, Sailboat on Lake and Pepper Original and Encrypted Images

6.2. 3D Plotting Histogram Analysis

When examining the results of 3D histograms of the original and encrypted images for analysis it is possible to notice that the histogram of the original image demonstrates a clearly defined structure and mostly has several peaks which correspond to the most frequent shades of color. These peak represents the nature and distribution of the content and color of the image further having distinguishable pattern between the red, green and the blue channel. However, the encrypted images 3D histogram shows no clear peaks and correlation between the pixels and looks more scattered and well distributed. The fairly consistent values point to the fact that the pixel has been adequately randomized and it is almost impossible differentiates any structure from the original image. The change from a 2D-structured bin to a bin that is arranged randomly re-endorses the ability of the encryption in protecting the image data since the attacks aim at referencing

recognizable patterns within the color channels. Based on this analysis, it can be concluded that histogram examination is crucial in evaluating the effectiveness of image encryption strategies since it depicts the changes to the original images data distribution. The 3D plotting histogram of different original and RGB images is given in Figures 4 and 5.

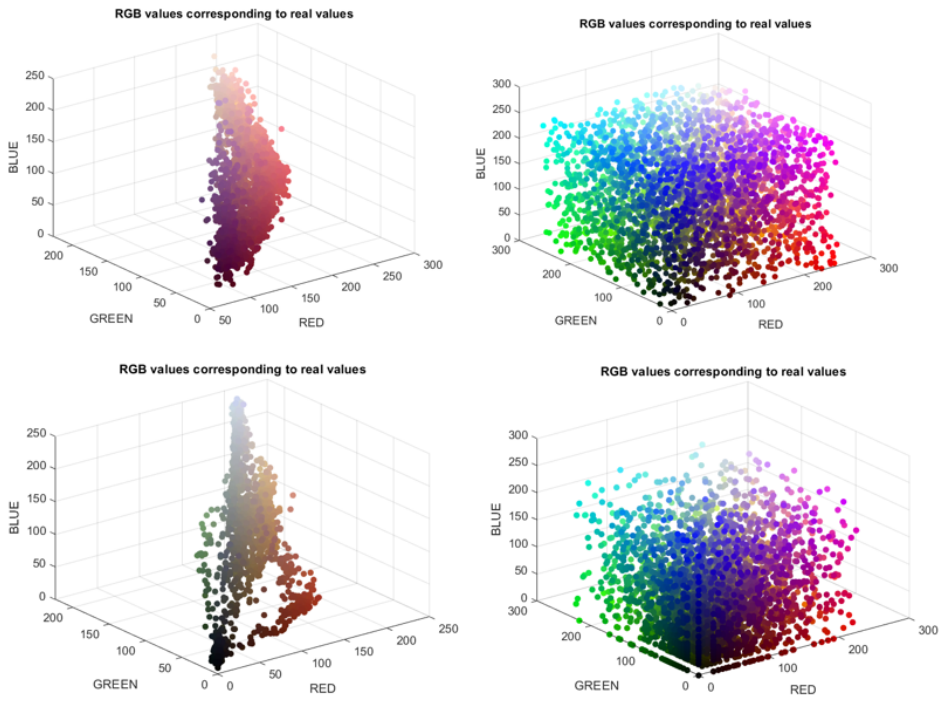

Figure 4: Original and Encrypted 3D Histogram of Earth and House Images

6.3. NPCR and UACI

NPCR (Number of Pixels Change Rate) is a crucial metric used to evaluate the sensitivity of an encryption algorithm to minor changes in the original image. In an effective image encryption scheme, even a single pixel modification in the input image should lead to a significant alteration in the encrypted image, ensuring strong security against differential attacks. NPCR measures the percentage of pixel values that change between two encrypted images when their corresponding original images differ by only one pixel. A high NPCR value, ideally close to 99% , indicates that the encryption method exhibits strong diffusion properties, meaning that a minor modification in the input spreads throughout the entire encrypted image. In the context of RGB image encryption over the residue classes of Eisenstein integers, NPCR is enhanced by the inherent algebraic properties of Eisenstein integers, which introduce non-linearity in the encryption process. The combination of modular arithmetic and affine transformations ensures that changes in pixel values are propagated unpredictably across all color channels, making it difficult

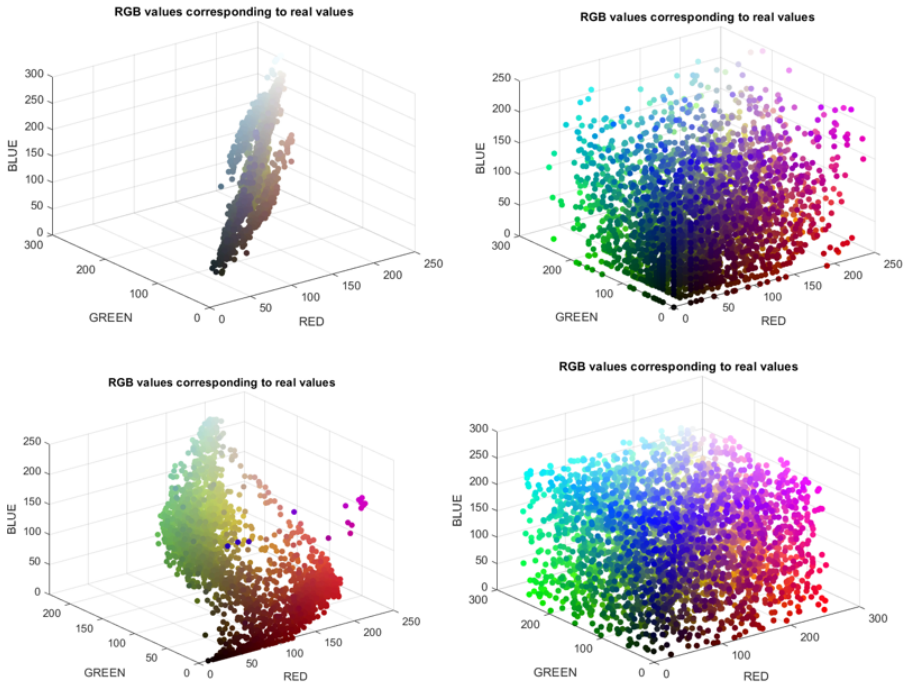

Figure 5: Original and Encrypted 3D Histogram of Sailboat and Pepper Images

for attackers to find meaningful patterns. By achieving a high NPCR value, the proposed encryption method guarantees that small perturbations in the input image do not produce predictable variations in the output, thereby strengthening resistance against statistical and differential cryptanalysis.

UACI (Unified Average Changing Intensity) is another vital statistical measure used to assess the effectiveness of an image encryption algorithm. It quantifies the average intensity difference between two encrypted images that are generated from original images differing by only a single pixel. UACI evaluates how drastically pixel intensities change after encryption, ensuring that the encrypted image maintains a noise-like appearance with no recognizable structures. A higher UACI value suggests that the encryption method introduces significant variations in pixel intensity, making it harder for attackers to identify relationships between encrypted and original images. The use of Eisenstein integers in RGB image encryption contributes to an increased UACI value by applying complex modular arithmetic operations that transform pixel values in a highly unpredictable manner. The algebraic properties of Eisenstein integers, combined with affine transformations and substitution-permutation operations, disrupt the pixel correlations, ensuring that even minor input changes lead to substantial intensity differences across the encrypted image. This randomness in intensity variation enhances security by making the encrypted image resistant to differential cryptanalysis, where attackers attempt to exploit slight differences in encryption results to retrieve the original image. A high UACI score validates the ro-

bustness of the proposed encryption technique, confirming its ability to generate encrypted images with strong diffusion and confusion properties, essential for secure digital image transmission and storage. Table 12 shows the results of NPCR and UACI [3, 12, 26, 30].

Table 12: NPCR and UACI Results of Encrypted Images

	NPCR			UACI		
Images	Red	Green	Blue	Red	Green	Blue
Earth (Proposed)	0.9961	0.9952	0.9963	0.3347	0.3371	0.3336
House (Proposed)	0.9960	0.9960	0.9960	0.3014	0.3099	0.3108
Sailboat (Proposed)	0.9962	0.9964	0.9963	0.2799	0.3388	0.3413
Pepper (Proposed)	0.9961	0.9967	0.9959	0.3373	0.3330	0.3356
[3]	0.9960	0.9960	0.9960	0.3348	0.3348	0.3348
[26]	0.9960	0.9961	0.9961	0.3347	0.3347	0.3346
[12]	0.9959	0.9964	0.9962	0.3269	0.3037	0.2762
[30]	0.9957	0.9957	0.9957	0.3328	0.3328	0.3328

6.4. Maximum Deviation and Irregular Deviation

Maximum Deviation is a key statistical measure used to evaluate the randomness and unpredictability of an encrypted image. It quantifies the highest difference in pixel intensity values between the original and encrypted images, providing insight into the strength of the encryption algorithm in terms of diffusion. In an effective image encryption scheme, the maximum deviation should be large, ensuring that the encrypted image significantly differs from the original, making it nearly impossible for attackers to retrieve meaningful information. When RGB image encryption is performed over the residue classes of Eisenstein integers, the encryption process applies modular arithmetic, affine transformations, and complex algebraic structures, causing drastic alterations in pixel values. The Eisenstein integer-based operations introduce non-linearity and unpredictability in the encryption process, further amplifying the maximum deviation. A high maximum deviation value indicates that pixel intensities are widely dispersed, making the encrypted image highly resistant to statistical attacks. This ensures that even if an attacker gains access to partial image data, they cannot reconstruct the original image due to the substantial deviations between encrypted and unencrypted pixel values.

Irregular Deviation measures the inconsistency and randomness in pixel intensity changes after encryption. Unlike maximum deviation, which considers the highest difference, irregular deviation evaluates how unpredictably pixel values change across the entire encrypted image. In a robust encryption system, pixel variations should follow a random and non-uniform pattern, ensuring that no discernible relationships exist between the original and encrypted images. Eisenstein integer-based encryption plays a significant role in increasing irregular deviation by introducing complex mathematical transformations that disrupt pixel distributions in a non-linear manner. The inherent properties of Eisenstein integers, such as their unique residue classes and modular operations, contribute

to the irregularity of pixel variations, ensuring that encryption results are highly unpredictable. A high irregular deviation value signifies that encrypted pixel intensities do not follow a structured pattern, making it extremely difficult for attackers to apply statistical methods to extract useful information. The combination of high maximum deviation and irregular deviation ensures that the encryption method effectively conceals image data, providing strong security against various cryptographic attacks, including statistical, differential, and frequency-based attacks. The results of MD and ID comparison [10, 12, 13] are provided in Table 13.

Table 13: MD and ID values for RGB Encrypted Images

	MD			ID		
Images	Red	Green	Blue	Red	Green	Blue
Earth (Proposed)	53792	41283	58639	27562	31903	21041
House (Proposed)	41261	61774	28852	25962	29651	26282
Sailboat (Proposed)	44732	45270	60591	21922	29600	24742
Pepper (Proposed)	59853	41613	47019	26431	25591	29258
[13]	52021	61841	61742	38097	37989	37924
[10]	59397	48329	53529	29231	25127	28374
[12]	60210	47069	62218	26266	19443	27027

6.5. PSNR and MSE Analysis

Peak Signal-to-Noise Ratio (PSNR) is another important metric used to evaluate the level of distortion in an encrypted image compared to its original counterpart. It is expressed in decibels (dB) and is inversely related to MSE, meaning that a higher MSE results in a lower PSNR value. In RGB image encryption over the residue classes of Eisenstein integers, a low PSNR value is desirable as it indicates that the encrypted image has been significantly altered, appearing as noise-like and revealing no visual resemblance to the original image. The encryption process utilizes the unique arithmetic properties of Eisenstein integers to introduce non-linear transformations and modular operations, ensuring that pixel intensities are well-distributed and unrecognizable. A lower PSNR value signifies that the encryption algorithm has effectively concealed all identifiable features of the original image, preventing statistical and visual attacks. Since PSNR is commonly used to measure image quality in compression and watermarking, its role in encryption is different, where a lower value validates the strength of the encryption. Thus, achieving a low PSNR in encrypted images confirms the robustness of Eisenstein integer-based encryption, ensuring secure image transmission and storage.

Mean Squared Error (MSE) is a fundamental metric used to measure the average squared difference between the original and encrypted image pixels in RGB image encryption over the residue classes of Eisenstein integers. A high MSE value signifies a greater deviation from the original image, confirming that the encryption algorithm has effectively randomized pixel values, making the encrypted image unrecognizable. In the proposed en-

cryption approach, Eisenstein integers introduce complex algebraic transformations and modular arithmetic operations that significantly alter the pixel intensities, ensuring that the MSE value remains high. This high deviation is crucial for security, as it prevents attackers from extracting meaningful information from the encrypted image. Additionally, the transformation of RGB pixel values into the residue classes of Eisenstein integers ensures that even a minor change in the original image results in a significant increase in MSE, further strengthening the encryption scheme. A high MSE value guarantees that the encryption process has effectively disrupted the correlation between the original and encrypted images, making it nearly impossible to reconstruct the original without the correct decryption key. The collected PSNR and MSE data [10, 13] are contained in Table 14.

Table 14: Comparative Analysis of PSNR and MSE for Encrypted RGB Images

	PSNR			MSE		
Images	Red	Green	Blue	Red	Green	Blue
Earth original	46.0926	46.0051	45.8002	1.61	1.64	1.72
Earth encrypted	44.0424	44.3559	44.2269	2.58	2.40	2.48
House original	44.0952	44.3637	44.0282	2.55	2.40	2.59
House encrypted	44.3986	44.0835	44.3352	2.38	2.56	2.42
Sailboat original	43.9840	43.8726	44.2964	2.62	2.69	2.44
Sailboat encrypted	44.4964	44.5677	44.3576	2.33	2.29	2.40
Pepper original	44.2777	44.5794	44.3140	2.45	2.28	2.43
Pepper encrypted	43.9548	44.6592	44.4470	2.64	2.24	2.35
[13] original	44.1849	44.4965	44.1297	2.50	2.33	2.53
[13] encrypted	44.1080	44.2180	44.3952	2.54	2.48	2.38
[10] original	44.6746	44.2313	44.9505	2.23	2.47	2.10
[10] encrypted	44.3020	44.3185	44.4057	2.43	2.42	2.38

6.6. Correlation Analysis

Correlation analysis is a fundamental statistical tool used to assess the security strength of an image encryption algorithm by measuring the degree of similarity between adjacent pixel values in an image. In an unencrypted image, adjacent pixels exhibit a high correlation, meaning their values are closely related, leading to smooth transitions and recognizable patterns. However, an effective encryption algorithm should break this correlation, ensuring that adjacent pixels in the encrypted image appear completely uncorrelated and noise-like. In RGB image encryption over the residue classes of Eisenstein integers, correlation analysis is performed in three directions—horizontal, vertical, and diagonal—to evaluate how well the encryption disrupts pixel dependencies. Horizontal correlation analysis examines the relationship between adjacent pixels along the same row. In an unencrypted image, horizontally adjacent pixels tend to have similar intensity values, contributing to smooth image structures. However, after applying Eisenstein integer-based encryption,

modular arithmetic, and affine transformations, these pixel dependencies are eliminated, resulting in an encrypted image where horizontally adjacent pixels have near-zero correlation. Vertical correlation analysis measures the similarity between pixels in the same column. Since natural images exhibit high vertical correlation due to the continuity of objects and textures, an effective encryption algorithm must ensure that vertically adjacent pixels in the encrypted image become statistically independent. The Eisenstein integer-based encryption scheme disrupts this correlation by applying non-linear transformations, substitutions, and permutations, ensuring that encrypted pixel values in the vertical direction are randomized. Diagonal correlation analysis assesses the dependency between pixels positioned diagonally in an image. In unencrypted images, diagonal pixel relationships are often less pronounced than horizontal and vertical ones but still maintain some level of correlation. The encryption process using Eisenstein integers ensures that diagonal correlations are also significantly reduced, making it difficult for attackers to exploit any structural information. The introduction of complex arithmetic operations and Eisenstein integer residue classes effectively scatters pixel values in a non-deterministic manner, thereby achieving near-zero diagonal correlation in the encrypted image. By performing correlation analysis in these three directions, the robustness of the encryption algorithm is validated. A well-encrypted image should exhibit correlation values close to zero in all directions, indicating that the encryption method successfully obscures structural patterns and resists statistical attacks. The use of Eisenstein integers enhances this randomness, ensuring a high level of security against cryptographic threats. Table 15 data is used to give correlation analysis in Figures 6, and 7.

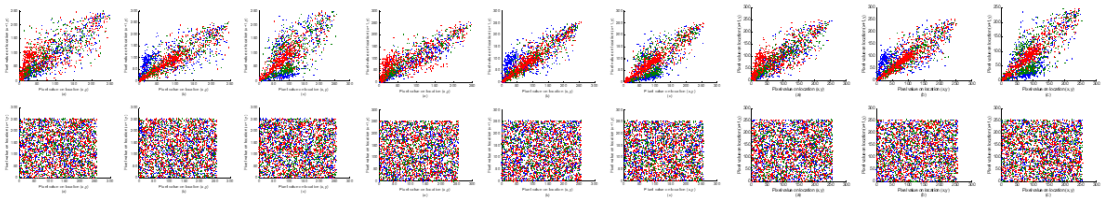

Figure 6: Diagonal, Horizontal & Vertical Correlation of Earth Image before and after Encryption

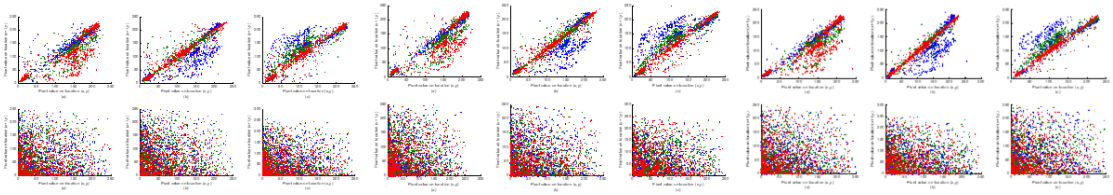

Figure 7: Diagonal, Horizontal & Vertical Correlation of Sailboat Image before and after Encryption

6.7. Information Entropy

Information entropy is a fundamental measure used to assess the randomness and security of encrypted images. In RGB image encryption over the residue classes of Eisenstein

Table 15: Correlation Coefficient for Original and Encrypted RGB Images

		Diagonal			Horizontal			Vertical		
Images	Red	Green	Blue	Red	Green	Blue	Red	Green	Blue	
Earth Original	Red	0.9211	0.8955	0.8190	0.9552	0.9419	0.8518	0.9400	0.9308	0.8303
	Green	0.7969	0.9215	0.9303	0.8279	0.9564	0.9596	0.8211	0.9411	0.9390
	Blue	0.7903	0.8407	0.9230	0.8078	0.8778	0.9530	0.8099	0.8414	0.9563
Earth Encrypted	Red	-0.0319	0.0031	0.0732	0.0397	0.0133	-0.0162	0.0369	0.0255	0.0440
	Green	-0.0049	-0.0373	0.0159	0.0355	-0.0180	0.0253	0.0419	-0.0096	0.0263
	Blue	-0.0817	-0.0265	0.0340	-0.0147	-0.0464	-0.0026	0.0394	-0.0115	-0.0221
House Original	Red	0.9697	0.9367	0.8717	0.9843	0.9391	0.8774	0.9934	0.9468	0.8858
	Green	0.8719	0.9737	0.9677	0.8782	0.9798	0.9839	0.8840	0.9931	0.9900
	Blue	0.8794	0.9553	0.9739	0.8632	0.9668	0.9750	0.8873	0.9733	0.9873
House Encrypted	Red	0.0170	-0.0206	0.0094	0.0528	0.0330	-0.0003	-0.0371	0.0029	-0.0118
	Green	0.0134	-0.0309	-0.0286	-0.0031	-0.0611	-0.0418	-0.0469	0.0013	0.0282
	Blue	0.0270	-0.0581	0.0511	-0.0064	0.0267	-0.0374	-0.0304	0.0157	0.0025
Sailboat Original	Red	0.9326	0.9097	0.8357	0.9728	0.9323	0.8535	0.9677	0.9412	0.8478
	Green	0.8288	0.9445	0.9520	0.8496	0.9638	0.9726	0.8432	0.9657	0.9681
	Blue	0.8215	0.8725	0.9569	0.8487	0.8939	0.9709	0.8490	0.9003	0.9749
Sailboat Encrypted	Red	0.0273	0.0018	0.0162	-0.0053	-0.0040	0.0145	0.0110	0.0094	0.0247
	Green	0.0338	0.0532	0.0425	-0.0160	0.0611	0.0244	0.0326	-0.0104	0.0468
	Blue	-0.0013	-0.0022	0.0060	0.0115	-0.0040	0.0367	0.0126	0.0008	0.0144
Pepper Original	Red	0.9077	0.2314	0.3188	0.9481	0.2542	0.3743	0.9392	0.2803	0.4023
	Green	0.3364	0.9395	0.8807	0.3595	0.9388	0.9308	0.4124	0.9611	0.9464
	Blue	0.3214	0.7788	0.8758	0.3374	0.7993	0.9289	0.3763	0.8324	0.9255
Pepper Encrypted	Red	-0.0462	-0.0125	0.0335	0.0185	0.0208	-0.0229	-0.0059	-0.0214	0.0236
	Green	-0.0262	-0.0539	0.0111	0.0117	-0.0046	-0.0176	0.0194	0.0165	-0.0075
	Blue	-0.0028	0.0336	0.0387	-0.0434	-0.0268	-0.0034	0.0138	0.0269	0.0353

integers, high entropy ensures that the encrypted image exhibits a noise-like structure with no discernible patterns, making it resistant to statistical attacks. A secure encryption scheme should produce an entropy value close to 8 bits per pixel for an 8-bit image, indicating a uniform distribution of pixel intensities. The encryption process involving Eisenstein integers enhances entropy by introducing complex algebraic transformations, modular arithmetic, and affine mappings, which obscure the correlation between the original and encrypted pixel values. These operations disrupt predictable structures in the image, ensuring that even a slight modification in the original image results in significant changes in the encrypted output, further increasing entropy. Since RGB images consist of three separate channels—red, green, and blue—entropy analysis is performed independently for each channel to verify that all components of the image maintain high randomness. The use of Eisenstein integers ensures that pixel values are widely dispersed across different residue classes, making it nearly impossible for attackers to exploit statistical patterns or frequency distributions. High information entropy confirms that the encryption method effectively eliminates redundancy, making the encrypted image highly unpredictable and secure. By leveraging the unique mathematical properties of Eisenstein integers, this encryption approach enhances the resistance of image data against cryptographic threats, including entropy-based attacks and frequency analysis. Therefore, achieving high entropy in encrypted RGB images is crucial for ensuring the confidentiality and robustness of the encryption scheme, particularly for applications requiring strong data security, such as medical imaging, secure communications, and military-grade en-

cryption systems. The current work was compared to the existing research noted in Table 16 in the sense of the comparison of entropy evaluation proposed [12, 14, 26, 28, 29].

Table 16: Information Entropy comparison

Images	Red	Green	Blue	Encrypted Images
Earth	7.9970	7.9974	7.9973	7.9972
Pepper	7.9975	7.9974	7.9974	7.9974
House	7.9969	7.9969	7.9973	7.9971
Sailboat	7.9968	7.9971	7.9972	7.9970
[28]	7.9974	7.9962	7.9972	7.9969
[26]	7.9896	7.9893	7.9907	7.9899
[14]	7.9913	7.9914	7.9916	7.9916
[12]	7.9976	7.9967	7.9976	7.9973
[29]	7.9899	7.9873	7.9870	7.9897

6.8. Contrast

Contrast is a crucial metric in image encryption that evaluates the variation in intensity between neighboring pixels. In RGB image encryption over the residue classes of Eisenstein integers, contrast analysis ensures that the encrypted image exhibits a highly randomized pixel distribution, making it resistant to visual and statistical attacks. A well-encrypted image should have a high contrast value, indicating that pixel intensities are significantly different from their neighbors, thereby eliminating identifiable patterns. The encryption process based on Eisenstein integers introduces complex modular arithmetic and algebraic transformations, which significantly alter pixel values, resulting in a uniform distribution across the encrypted image. This ensures that any correlation between adjacent pixels in the original image is completely destroyed. The randomness introduced by Eisenstein integer-based transformations increases the overall contrast of the encrypted image, making it appear noise-like and unintelligible. A high contrast value confirms that the encryption algorithm effectively disrupts the structural consistency of the original image, reinforcing its security against attacks that rely on statistical analysis. Table 17 shows the presented contrast data [10, 13, 27].

6.9. Energy

Energy is another significant texture-based measure used to analyze the distribution of pixel values in an encrypted image. It represents the sum of squared pixel values in a given region, reflecting the uniformity or randomness of intensity variations. In the context of RGB image encryption over the residue classes of Eisenstein integers, energy analysis helps determine the effectiveness of the encryption scheme in dispersing pixel values across the encrypted image. A well-encrypted image should exhibit a balanced energy distribution, ensuring that no specific areas retain structured patterns from the original image. The use

Table 17: Contrast Comparative Analysis of Original and Encrypted RGB Images

Images	Red	Green	Blue
Earth Original	0.4040	0.4063	0.3995
Earth Encrypted	10.4327	10.4897	10.4779
House Original	0.4812	0.4917	0.4682
House Encrypted	10.5833	10.5614	10.4730
Sailboat Original	0.4246	0.5591	0.5195
Sailboat Encrypted	10.4083	10.5128	10.5170
Pepper Original	0.3535	0.5562	0.3360
Pepper Encrypted	10.5151	10.4779	10.4237
[27] Original	0.5439	0.5000	0.4726
[27] Encrypted	10.5114	10.4770	10.4894
[13] Original	0.5693	0.6411	0.6196
[13] Encrypted	10.5357	10.4913	10.4710
[10] Original	0.4717	0.4879	0.4261
[10] Encrypted	10.4878	10.4861	10.5034

of Eisenstein integers in encryption introduces non-linear transformations that distribute pixel intensities evenly, ensuring that the energy levels remain stable across different image regions. This contributes to the overall security of the encrypted image, as it prevents attackers from identifying patterns that could aid in breaking the encryption. A high and uniform energy value in the encrypted image suggests strong diffusion and confusion properties, confirming that Eisenstein integer-based encryption effectively conceals the original image details while maintaining a secure and unpredictable pixel distribution. Table 18 shows the presented energy data [10, 13, 27].

6.10. Homogeneity

Homogeneity is a texture-based measure that evaluates the uniformity of intensity variations in an image. In the context of RGB image encryption over the residue classes of Eisenstein integers, homogeneity analysis determines how well the encryption algorithm disrupts the smooth regions of the original image. A lower homogeneity value in the encrypted image indicates a higher level of randomness, meaning that pixel values are well-distributed without retaining any structured patterns from the original image. The encryption process using Eisenstein integers introduces non-linear transformations and modular arithmetic operations, ensuring that pixel intensities are scattered in a way that eliminates any noticeable similarity between adjacent pixels. By reducing homogeneity, the encryption algorithm enhances security by making it nearly impossible for an attacker to detect or reconstruct image features using statistical analysis. The use of Eisenstein integers further ensures that any minor change in the original image results in a substantial alteration in the encrypted image, reinforcing the unpredictability and robustness of the encryption scheme. Table 19 shows the presented homogeneity data [10, 13].

Table 18: Energy Comparative Analysis of Original and Encrypted RGB Images

Images	Red	Green	Blue
Earth Original	0.3292	0.2594	0.2135
Earth Encrypted	0.0156	0.0156	0.0156
House Original	0.1275	0.1544	0.1303
House Encrypted	0.0156	0.0156	0.0156
Sailboat Original	0.1114	0.0879	0.1303
Sailboat Encrypted	0.0156	0.0156	0.0156
Pepper Original	0.1326	0.1122	0.1682
Pepper Encrypted	0.0156	0.0156	0.0156
[27] Original	0.0779	0.0821	0.1708
[27] Encrypted	0.1051	0.1048	0.1049
[13] Original	0.0752	0.0735	0.0713
[13] Encrypted	0.0156	0.0156	0.0156
[10] Original	0.0838	0.0834	0.1242
[10] Encrypted	0.0156	0.0156	0.0156

6.11. Time Analysis

The time analysis of a novel RGB image encryption scheme using operations on residue classes of eisenstein integers $\mathbb{Z}[\omega]_\pi$ evaluates the computational efficiency of the proposed algorithm in terms of encryption and decryption speed. The scheme is implemented and tested on a system equipped with an Intel(R) Core(TM) i5-1135G7 @ 2.40 GHz processor and 8 GB of RAM, offering a balanced environment for performance benchmarking. The encryption process relies on operations defined over the residue classes of Eisenstein integers, incorporating substitution-permutation techniques, modular arithmetic, and algebraic transformations tailored for RGB image data. To assess the algorithm's performance, multiple RGB images of varying resolutions and content complexities were encrypted and decrypted, and the execution times were recorded. The results indicate that the algorithm maintains efficient processing speeds while preserving high levels of security, even for large images. The lightweight nature of arithmetic over $\mathbb{Z}[\omega]_\pi$ contributes to reduced computational overhead, and the structure of the algorithm allows it to benefit from moderate parallelism available in the processor architecture. Although the i5 processor and 8 GB memory impose practical limits, the scheme remains effective for real-time applications. Speed metrics across various test cases demonstrate that the proposed encryption technique is both scalable and suitable for secure multimedia communications. A comparative analysis of encryption and decryption times with existing state-of-the-art methods is presented in Table 20, confirming the algorithm's superior performance and practical feasibility [30, 35].

Table 19: Homogeneity Comparative Analysis of Original and Encrypted RGB Images

Images	Red	Green	Blue
Earth Original	0.8753	0.8719	0.8718
Earth Encrypted	0.3907	0.3915	0.3900
House Original	0.8620	0.8608	0.8642
House Encrypted	0.3890	0.3889	0.3906
Sailboat Original	0.8521	0.8348	0.8473
Sailboat Encrypted	0.3911	0.3887	0.3887
Pepper Original	0.8808	0.8731	0.8844
Pepper Encrypted	0.3908	0.3889	0.3894
[13] Original	0.8335	0.8324	0.8293
[13] Encrypted	0.3891	0.3892	0.3899
[10] Original	0.8855	0.8726	0.8855
[10] Encrypted	0.3892	0.3897	0.3889

Table 20: Encryption and Decryption Speed Analysis in Seconds

Schemes	**Computer Configuration**	**Encryption Time (s)**	**Decryption Time (s)**	**Total Time (s)**
Earth	Intel i5-1135G7 @ 2.40 GHz, 8 GB RAM	0.2433	0.2710	0.5143
House	Intel i5-1135G7 @ 2.40 GHz, 8 GB RAM	0.2589	0.2511	0.5100
Sailboat	Intel i5-1135G7 @ 2.40 GHz, 8 GB RAM	0.2521	0.2509	0.5030
Pepper	Intel i5-1135G7 @ 2.40 GHz, 8 GB RAM	0.2603	0.2622	0.5225
[35]	Intel i7-8550U @ 1.80 GHz, 8 GB RAM	0.4180	0.6910	1.1090
[30]	Intel i5-1135G7 @ 2.40 GHz, 16 GB RAM	0.2648	0.2619	0.5267

6.12. NIST Test

The NIST test suite is a comprehensive set of statistical tests designed to evaluate the randomness and security of cryptographic algorithms, making it a crucial tool for assessing the strength of RGB image encryption over the residue classes of Eisenstein integers. The frequency test examines whether the proportion of zeros and ones in the encrypted image is balanced, ensuring that no bias exists in pixel transformations. The block frequency test extends this analysis by dividing the encrypted image into smaller blocks and checking for uniform distribution, ensuring that randomness is maintained across all sections. The rank test evaluates the linear dependency of pixel values by analyzing the rank of overlapping matrices derived from the encrypted image, confirming that no predictable patterns persist. The runs test (M=10,000) and long runs of Ones test check for sequences of repeating pixel values, ensuring that the encryption disrupts any structured patterns present in the original image. The overlapping and non-overlapping template matching tests assess whether any specific bit patterns appear more frequently than expected, indicating potential vulnerabilities if certain sequences remain recognizable. The spectral DFT test detects periodicities in the encrypted data by analyzing frequency components, ensuring that encryption effectively disperses image features. The approximate entropy test measures the complexity of pixel variations, validating that encrypted images exhibit high randomness. The universal test assesses the compressibility of the encrypted image,

where a high level of incompressibility signifies strong encryption. The serial tests analyze the occurrence of various pixel patterns to confirm that all sequences appear with equal probability. The cumulative sums tests (forward and reverse) check for statistical deviations that might reveal predictable changes in pixel intensity. Lastly, the random excursions and random excursions variant tests evaluate how encrypted pixel sequences behave in relation to predefined thresholds, ensuring that pixel distributions remain unpredictable. The successful passing of these NIST tests demonstrates the robustness of RGB image encryption over the residue classes of Eisenstein integers, verifying that the encrypted images exhibit ideal cryptographic properties such as randomness, uniformity, and resistance to statistical attacks. Table 21 evaluate the NIST analysis of Earth results.

7. Conclusion, and Future Work

The novel cryptographic algorithm for encrypting RGB images based on the two S-boxes that act over the Eisenstein integers is described in this work. This new strategy leverages the strengths of Eisenstein integers to build feasible replacement boxes and the latter is then used for each channel of the image. The experimental outcome proves that the suggested technique provides a high level of security and does not compromise the decrypted image's quality. As for the strengths of this approach, it is important to list that it is effectively protected from the well-known methods of differential and linear cryptanalysis. This is due to the fact that complex integers are employed which bring non-linearity hence complexity into the encryption aspects. Furthermore, there is also superior security, which can be obtained with relatively small keys, evidencing the efficiency of the proposed technique compared to the existing ones. That it has also proved more robust compared with other encryption systems using the replacement boxes which in the past have been considered more difficult to crack. Also, it is more diffused with small changes in the plaintext which are dissipated all over the cipher text making it harder for the attackers to identify a pattern. However, the aspect of how simple it is to implement makes it widely applicable across population. Experimental analysis shows that the time complexity of the suggested technique is low regarding computation time and memory usage which IS important for real time systems.

This technique has prospects for further research in other multimedia types, such as videos, MP3 files and further incorporation of mathematical structures, including quaternions. Additionally, comparisons with the traditional encryption algorithms will also be carried out to test the security of the document encryption.

Acknowledgements

The Researchers would like to thank the Deanship of Graduate Studies and Scientific Research at Qassim University for financial support (QU-APC-2025).

Table 21: NIST Analysis Results for Earth Encrypted RGB Images

Tests		P-values			Remarks
		Red	Green	Blue	
Frequency		0.52709	0.32694	0.37592	✓
Block Frequency		0.98143	0.93533	0.92237	✓
Rank		0.29191	0.29191	0.29191	✓
Runs	M = 10,000	0.34596	0.66982	0.83978	✓
Long Runs of Ones		0.71270	0.71270	0.71270	✓
Overlapping Templates		0.85988	0.85988	0.85988	✓
Non-overlapping Templates		0.16439	0.97809	1.00000	✓
Spectral DFT		0.66336	0.30979	1.00000	✓
Approximate Entropy		0.62891	0.22728	0.26326	✓
Universal		0.99946	0.99608	0.98707	✓
Serial	p-value 1	0.70248	0.73018	0.23497	✓
	p-value 2	0.90613	0.87130	0.13369	✓
Cumulative Sums Forward		0.24299	0.33000	0.28130	✓
Cumulative Sums Reverse		1.08320	1.36450	0.67591	✓
Random Excursions	X = -4	0.14727	0.99019	0.55706	✓
	X = -3	0.13156	0.98815	0.83905	✓
	X = -2	0.37541	0.22052	0.73959	✓
	X = -1	0.09461	0.89148	0.65503	✓
	X = 1	0.00046	0.12573	0.93677	✓
	X = 2	0.01925	0.98276	0.68690	✓
	X = 3	0.05576	0.85373	0.81666	✓
	X = 4	0.09399	0.00031	0.98730	✓
Random Excursions Variants	X = -5	0.57315	0.58621	0.52243	✓
	X = -4	0.32205	0.16491	0.42034	✓
	X = -3	0.15093	0.36131	0.70292	✓
	X = -2	0.07898	1.00000	0.62246	✓
	X = -1	0.01796	0.68309	0.52243	✓
	X = 1	0.02799	0.41422	0.39377	✓
	X = 2	0.05704	0.34578	0.53825	✓
	X = 3	0.08210	0.71500	0.77485	✓
	X = 4	0.02145	0.75762	0.62875	✓
	X = 5	0.01317	0.68309	0.52243	✓

Data availability

The images used in this study were obtained from 'The USC-SIPI Image Database' (https://sipi.usc.edu/database/). The researcher can contact to the Muhammad Sajjad for getting the images.

References

[1] Bruce Schneier. *Applied cryptography: protocols, algorithms, and source code in C*. John Wiley & Sons, 2007.

[2] T. Shah and A. Qureshi. S-box on subgroup of galois field. *Cryptography*, 13(3):1–9, 2019.

[3] G. Chen, Y. Chen, and X. Liao. An extended method for obtaining s-boxes based on three-dimensional chaotic baker maps. *Chaos, Solitons & Fractals*, 31(3):571–579, 2007.

[4] H. Iqtadar, S. Tariq, A. G. Muhammad, A. K. Waqar, and M. Hasan. A group theoretic approach to construct cryptographically strong substitution boxes. *Neural Computing and Applications*, 23:97–104, 2013.

[5] M. Khan, T. Shah, H. Mahmood, M. A. Gondal, and I. Hussain. A novel technique for the construction of strong s-boxes based on chaotic lorenz systems. *Nonlinear Dynamics*, 70:2303–2311, 2012.

[6] M. Zhao, Y. Luo, Z. Yuan, and L. Li. A fast color image encryption scheme based on the new chaotic structure and dynamic strong s-boxes. *Nonlinear Dynamics*, 113(6):5837–5863, 2025.

[7] U. Çavuşoğlu, A. Zengin, I. Pehlivan, and S. Kaçar. A novel approach for strong s-box generation algorithm design based on chaotic scaled zhongtang system. *Nonlinear Dynamics*, 87:1081–1094, 2017.

[8] E. Özpolat, V. Çelik, and A. Gülten. Hyperchaotic system-based prng and s-box design for a novel secure image encryption. *Entropy*, 27(3):299, 2025.

[9] M. Sajjad, T. Shah, M. Alammari, and H. Alsaud. Construction and decoding of bch-codes over the gaussian field. *IEEE Access*, 2023.

[10] M. Sajjad, T. Shah, R. Hamza, B. Almutairi, and R. J. Serna. Multiple color images security by spn over the residue classes of gaussian integer. *Scientific Reports*, 15(1):6425, 2025.

[11] M. Sajjad, T. Shah, and R. J. Serna. Designing pair of nonlinear components of a block cipher over gaussian integers. *Computers, Materials & Continua*, 75:5287–5305, 2023.

[12] M. Sajjad, T. Shah, T. ul Haq, B. Almutairi, and Q. Xin. Spn based rgb image encryption over gaussian integers. *Heliyon*, 10(9):1–17, 2024.

[13] M. Sajjad and N. A. Alqwaifly. A novel spn-based multiple rgb images security over the residue classes of quaternion integers $\mathbb{H}[k]_\delta$. *European Journal of Pure and Applied Mathematics*, 18(2):6228–6228, 2025.

[14] M. Sajjad, T. Shah, H. Alsaud, and M. Alammari. Designing pair of nonlinear components of a block cipher over quaternion integers. *AIMS Mathematics*, 8(9):21089–21105, 2023.

[15] M. Sajjad, T. Shah, M. Abbas, M. Alammari, and R. J. Serna. The impact of alternant codes over eisenstein integers on modern technology. *Computational and Applied Mathematics*, 44(1):95, 2025.

[16] M. Sajjad, T. Shah, Q. Xin, and B. Almutairi. Eisenstein field bch codes construction

and decoding. *AIMS Mathematics*, 8(12):29453–29473, 2023.

[17] K. Huber. Codes over eisenstein-jacobi integers. *Contemporary Mathematics*, 168:165–165, 1994.

[18] B. Valmir. Finding factors of factor rings over the eisenstein integers. *International Mathematical Forum*, 9:1521–1537, 2014.

[19] J. Zhang, B. Yin, and X. Deng. A novel color image encryption method based on an evolved dynamic parameter-control chaotic system. *Multimedia Tools and Applications*, 80(18):27155–27170, 2021.

[20] L. Huang, S. Cai, X. Xiong, and M. Xiao. On symmetric color image encryption system with permutation-diffusion simultaneous operation. *Optics and Lasers in Engineering*, 115:7–20, 2019.

[21] L. Teng, X. Wang, and Y. Xian. Image encryption algorithm based on a 2d-clss hyperchaotic map using simultaneous permutation and diffusion. *Information Sciences*, 605:71–85, 2022.

[22] X. Liu, X. Tong, Z. Wang, and M. Zhang. A novel hyperchaotic encryption algorithm for color image utilizing dna dynamic encoding and self-adapting permutation. *Multimedia Tools and Applications*, 81:21779–21810, 2022.

[23] X. Chen, M. Gong, Z. Gan, Y. Lu, X. Chai, and X. He. Cie-lscp: color image encryption scheme based on the lifting scheme and cross-component permutation. *Complex & Intelligent Systems*, 9(1):927–950, 2023.

[24] D. El-Damak, W. Alexan, E. Mamdouh, M. El-Aasser, A. Fathy, and M. Gabr. Fibonacci q-matrix, hyperchaos, and galois field GF(2^8) for augmented medical image encryption. *IEEE Access*, 2024.

[25] E. Z. Zefreh. Psdcls: Parallel simultaneous diffusion–confusion image cryptosystem based on latin square. *Journal of Information Security and Applications*, 83:103785, 2024.

[26] R. Enayatifar, A. H. Abdullah, and I. F. Isnin. Chaos-based image encryption using a hybrid genetic algorithm and a dna sequence. *Optics and Lasers in Engineering*, 56:83–93, 2014.

[27] D. S. Malik and T. Shah. Color multiple image encryption scheme based on 3d-chaotic maps. *Mathematics and Computers in Simulation*, 178:646–666, 2020.

[28] A. A. Abd EL-Latif, B. Abd-El-Atty, and S. E. Venegas-Andraca. Controlled alternate quantum walk-based pseudo-random number generator and its application to quantum color image encryption. *Physica A: Statistical Mechanics and its Applications*, 547:123869, 2020.

[29] L. Yao, C. Yuan, J. Qiang, S. Feng, and S. Nie. An asymmetric color image encryption method by using deduced gyrator transform. *Optics and Lasers in Engineering*, 89:72–79, 2017.

[30] N. Rani. Image ciphering algorithm based on novel icmm and modified differential encoding. *Physica Scripta*, 100(4):045211, 2025.

[31] W. Alexan, K. Hosny, and M. Gabr. A new fast multiple color image encryption algorithm. *Cluster Computing*, 28(5):1–34, 2025.

[32] J. H. Yakubu, M. Ashiru, and E. P. Musa. Chaos-based image encryption algorithm

for rgb images using rucklidge chaotic system. *Physica Scripta*, 2025.

[33] P. C. Pandian. Bounds for covering radius in specific classes of codes over finite rings r. *TWMS Journal of Applied and Engineering Mathematics*, 2025.

[34] P. C. Pandian. On the covering radius of some classes of dna code over finite ring. *TWMS Journal of Applied and Engineering Mathematics*, 2025.

[35] S. Deb and P. K. Behera. Design of key-dependent bijective s-boxes for color image cryptosystem. *Optik*, 253:168548, 2022.