EUROPEAN JOURNAL OF PURE AND APPLIED MATHEMATICS
2025, Vol. 18, Issue 3, Article Number 6470
ISSN 1307-5543 – ejpam.com
Published by New York Business Global

Multiple RGB Images Security based on Substitution–Permutation Network over the Residue Classes of Eisenstein Integer $\mathbb{Z}[\Omega]_\pi$

Maha Alammari[1], Muhammad Sajjad[2,*], Mushtaq K. Abdalrahem[3], Robinson-Julian Serna[4]

[1] *Department of Mathematics, College of Science, King Saud University, P.O. Box 22452 Riyadh 11495, Saudi Arabia*
[2] *NUTECH School of Applied Science and Humanities, National University of Technology, Islamabad, 44000, Pakistan*
[3] *College of Pharmacy, University of Al-Ameed*
[4] *Escuela de Matemáticas y Estadística, Universidad Pedagógica y Tecnológica de Colombia, Tunja, Colombia*

Abstract. This paper presents a multiple RGB image encryption scheme that utilizes a pair of 8×8 S-boxes constructed over the residue classes of Eisenstein integers $\mathbb{Z}[\Omega]_\pi$, implemented within a three-stage Substitution–Permutation Network (SPN) architecture. The S-boxes are generated using Eisenstein integer algebra through affine transformations and their corresponding inverse functions, ensuring strong nonlinearity. The first S-box serves as a substitution function, while the second contributes to both permutation and diffusion. Enhanced cryptographic strength is achieved through modular arithmetic in $\mathbb{Z}[\Omega]_\pi$, which supports essential encryption properties such as confusion and diffusion. Further complexity is introduced by combining the two S-boxes via an XOR operation to construct a third S-box, promoting greater inter-channel diffusion among the RGB components. The proposed SPN framework is designed to resist differential and linear cryptanalysis through its layered substitution, permutation, and XOR-based mixing operations. Separate yet interlinked processing pathways for each image channel ensure secure and efficient encryption. Experimental evaluations validate the proposed method, demonstrating high entropy, low inter-channel correlation, and robust resistance to various attacks, making it a strong candidate for secure multimedia communication applications.

2020 Mathematics Subject Classifications: 11T71, 14G50, 94A60, 81P94, 16S38, 97G70

Key Words and Phrases: Eisenstein integers, Multiple Image Encryption, Substitution Permutation Network, Security Analysis

*Corresponding author.
DOI: https://doi.org/10.29020/nybg.ejpam.v18i3.6470

Email addresses: malammari@ksu.edu.sa (M. Alammari), muhammad.sajjad@nutech.edu.pk (M. Sajjad), mushtaq.k@alameed.edu.iq (M. K. Abdalrahem), robinson.serna@uptc.edu.co (R-J. Serna)

1. Introduction

Cryptography is the practice of transforming information into a format that is unreadable to unauthorized users, ensuring confidentiality and security. Historically, cryptographic techniques have evolved from simple substitution ciphers to complex mechanical and digital systems. With the rise of digital communication, modern cryptography has become essential for protecting privacy, ensuring data integrity, and enabling secure authentication. Contemporary encryption systems incorporate advanced mathematical foundations and sophisticated algorithms that far surpass traditional approaches. Cryptographic schemes are broadly categorized into symmetric and asymmetric systems. Symmetric cryptography uses a single key for both encryption and decryption, while asymmetric cryptography employs a public-private key pair. Both types play a crucial role in securing data through hash functions and digital signatures, which verify authenticity and prevent tampering. As digital environments continue to expand, cryptography evolves to include quantum-resistant methods and stronger encryption strategies [1, 2].

Substitution–permutation networks (SPNs) are a fundamental cryptographic framework employed in modern block ciphers. Within SPNs, substitution boxes (S-boxes) serve as nonlinear components that significantly enhance security by introducing confusion—scrambling input so that even small changes produce vastly different outputs. Strong S-boxes are designed to ensure balanced output distribution, high nonlinearity, and avalanche effects. Algebraic structures, random mappings, and optimization techniques are used to construct secure S-boxes, and current research explores novel designs over alternative mathematical domains to improve both robustness and efficiency [3].

RGB image encryption is a critical subfield of cryptography concerned with securing digital image content against unauthorized access or tampering. An RGB image comprises three color channels—red, green, and blue—each with its own pixel intensity matrix. Unlike text encryption, image encryption must handle large data volumes, spatial redundancy, and high inter-pixel correlation. To address these challenges, encryption schemes employ pixel-level substitution, permutation, and diffusion techniques. When encrypting multiple RGB images, added complexity is required to prevent inter-image correlation. XOR-based transformations, key-dependent operations, and multi-channel mixing enhance security by neutralizing differential attacks and preserving uniqueness across encrypted datasets. This demand is especially high in domains such as cloud storage, secure image sharing, and medical imaging [4, 5].

Beyond conventional number systems, Eisenstein integers—complex numbers of the form $a + b\omega$, where ω is a primitive cube root of unity—offer a rich algebraic structure with notable symmetry and well-defined modular arithmetic. These properties make Eisenstein integers suitable for secure cryptographic system design, particularly for nonlinear transformations within SPNs. Their inherent mathematical features provide natural resistance against common cryptographic attacks, and they continue to attract attention for applications in coding theory, encryption, and signal processing [6–10].

With the growing demands for secure storage and transmission of visual data, substitution–permutation structures remain central to modern cryptographic design. The role

of chaotic maps, conservative hyperchaotic systems, Knuth–Durstenfeld algorithms, and Hopfield neural networks in image encryption has also been widely studied [11–16]. Recent works have integrated one-time keys, spatial permutations, DNA-based operations, and Boolean networks for enhancing encryption resilience. Optical asymmetric key cryptosystems, pixel exchange schemes, and spectral transformations are also employed to address efficiency and attack resistance [17–20]. The Eisenstein integer domain has increasingly been explored for cryptographic component design, extending from its roots in error-correcting code construction to advanced image encryption systems [6, 7, 9].

Furthermore, recent contributions have shown the feasibility of RGB image encryption using Gaussian integers within SPN frameworks [21–24]. The use of quaternion integers and BCH-code constructions over finite fields has strengthened digital communication security by reducing vulnerability to analytical attacks [25]. Integration of chaotic maps with elliptic curve cryptography, quantum-walk-based pseudo-random number generators, and multimedia steganography has enabled encrypted image concealment within diverse content [26–28]. Parallel computing techniques have also accelerated encryption algorithms, enabling real-time applications [29]. Other breakthroughs include compressive ghost imaging and 3D permutation models for multi-image protection [30, 31].

The increasing reliance on multiple-image encryption in military communication, medical diagnostics, and secure cloud systems reveals the limitations of early cryptographic methods. Despite the robustness of classical approaches such as RSA and protocols in the Handbook of Applied Cryptography, they can fall short when processing high-volume multimedia data [1, 2]. While chaotic maps [4], DNA coding [15, 32], and neural networks [13] have addressed image security to some extent, they often suffer from limited key sensitivity or high computational costs. Recent developments involving quaternion and Gaussian integers offer promising alternatives [22–25], and Eisenstein integers present a fresh avenue for developing secure block ciphers [7, 9].

In this paper, we propose a novel encryption framework based on Eisenstein integers, implemented within a three-stage SPN architecture for the encryption of multiple RGB images. Unlike conventional designs, our scheme employs a pair of 8×8 S-boxes over the residue classes of Eisenstein integers $\mathbb{Z}[\Omega]_\pi$, ensuring high nonlinearity and strong confusion properties. Affine transformations and their inverses enhance resistance to cryptanalytic attacks. Additionally, an XOR-derived third S-box is used to increase inter-channel diffusion across RGB components. The system is designed for high entropy, minimal correlation, and effective defence against differential and linear cryptanalysis.

The remainder of this paper is structured as follows. Section 2 introduces the mathematical background, including Eisenstein integers and relevant residue class theorems. Section 3 describes the construction of cryptographically secure S-boxes over Eisenstein primes. Section 4 details the encryption process for multiple RGB images using the proposed SPN model. Section 5 presents a comprehensive security and performance evaluation. Finally, Section 6 concludes the paper and outlines future research directions. Our results demonstrate that modular arithmetic over Eisenstein residue classes can offer robust multimedia encryption with strong empirical validation and high resistance to known attacks.

2. Eisenstein Integers and Their Properties

Following the discussions in [6–10], Eisenstein integers (EIs) form a distinguished subset of the complex numbers, denoted by $\mathbb{Z}[\Omega] = \{a + b\Omega \mid a, b \in \mathbb{Z}\}$, where $\Omega = (-1 + \sqrt{3}i)/2$ is a primitive cube root of unity. This set forms a commutative ring with identity under addition and multiplication.

Let $z = a + b\Omega$ be an Eisenstein integer. Its complex conjugate is defined as:

$$\bar{z} = a + b\bar{\Omega} = a + b\Omega^2,$$

where Ω^2 is the complex conjugate of Ω. The *norm* of z is then given by:

$$N(z) = z\bar{z} = (a + b\Omega)(a + b\Omega^2) = a^2 - ab + b^2.$$

Theorem 1 ([7, 8, 10])**.** *Let p be a rational prime. Then there exists an Eisenstein prime $c \in \mathbb{Z}[\Omega]$ such that $N(c) = c\bar{c} = p$ if and only if p is not a prime in $\mathbb{Z}[\Omega]$.*

Theorem 2 ([7, 8, 10])**.** *If the norm $N(c)$ of an Eisenstein integer c is a rational prime, then c is a prime in $\mathbb{Z}[\Omega]$.*

2.1. Residue Class of Eisenstein Integers [7, 8]

Given $c = a + b\Omega \in \mathbb{Z}[\Omega]$, the residue class modulo c is denoted as $\mathbb{Z}[\Omega]_c$. The modulo operation $f : \mathbb{Z}[\Omega] \to \mathbb{Z}[\Omega]_c$ is defined by:

$$f(x) = y \bmod c = x - \left\lfloor \frac{x\bar{c}}{c\bar{c}} \right\rfloor c,$$

where the floor operation is applied separately to the real and imaginary parts to ensure that $y \in \mathbb{Z}[\Omega]_c$ remains an Eisenstein integer.

2.2. Eisenstein Mannheim Weight and Distance [7, 8]

Let $\beta, \gamma \in \mathbb{Z}[\Omega]_c$ and define $\alpha = \gamma - \beta = c + d\Omega$ as an Eisenstein integer. The *Eisenstein Mannheim weight* $W_{\mathrm{EM}}(\alpha)$ is defined by:

$$W_{\mathrm{EM}}(\alpha) = |c| + |d|.$$

The *Eisenstein Mannheim distance* between β and γ is:

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

Proposition 1 ([7, 8])**.** *Let $\delta_k = c_k + d_k\Omega$ be distinct primes in $\mathbb{Z}[\Omega]_c$ such that $p^k = c_k^2 - c_k d_k + d_k^2$ are distinct rational primes. If $\mathbb{Z}[\Omega]^*_{(\delta^k)}$ is generated by α, then:*

$$\alpha^{\phi(p^k)/2} \equiv -1 \pmod{\delta^k}.$$

Proposition 2 ([7, 8]). *Let $\delta_1 = c_1 + d_1\Omega$ and $\delta_2 = c_2 + d_2\Omega$ be two prime Eisenstein integers with corresponding rational primes $p = c_1^2 - c_1d_1 + d_1^2$ and $q = c_2^2 - c_2d_2 + d_2^2$. Then, there exist elements $e, f \in \mathbb{Z}[\Omega]^*_{(\delta_1\delta_2)}$ such that:*

$$f^{\phi(p)} \equiv 1 \pmod{\delta_1\delta_2}, \quad e^{\phi(q)} \equiv 1 \pmod{\delta_1\delta_2}.$$

Proposition 3 ([7]). *Let $\delta_k = c_k + d_k\Omega$ be distinct Eisenstein primes and $p^k = c_k^2 - c_kd_k + d_k^2$ distinct rational primes. Then there exists an element $\tau_k \in \mathbb{Z}[\Omega]^*_{(\delta_1\delta_2\cdots\delta_k)}$ such that:*

$$\tau_k^{\phi(p^k)} \equiv 1 \pmod{\delta_1\delta_2\cdots\delta_k}, \quad \text{for } k = 1, 2, \ldots, m.$$

Theorem 3 ([7]). *Let c be an Eisenstein prime with norm $N(c)$, and let $\alpha \neq 0$ be a nonzero Eisenstein integer. Then:*

$$\alpha^{N(c)} \equiv \alpha \pmod{c}.$$

Theorem 4 ([7, 8]). *If $\langle\alpha\rangle = \langle a + b\Omega\rangle$ is a principal ideal in $\mathbb{Z}[\Omega]$ with $\gcd(a, b) = 1$, then:*

$$\mathbb{Z}[\Omega]/\langle a + b\Omega\rangle \cong \mathbb{Z}_{a^2-ab+b^2}.$$

3. Redesigning of $n \times n$ S-boxes over the Eisenstein Integers

Ensuring strong security remains a fundamental requirement in modern cryptographic systems. Among the core techniques that enhance cryptographic resilience, the introduction of confusion plays a central role. Substitution boxes (S-boxes) are widely employed nonlinear components in symmetric ciphers and contribute significantly to the overall security by disrupting statistical patterns and increasing unpredictability. The strength of an S-box improves significantly when constructed using robust algebraic structures, such as the Eisenstein integers (EIs). The rich mathematical properties of EIs support the development of cryptographically strong S-boxes with enhanced nonlinearity, optimal differential uniformity, and high avalanche effect. This section presents a step-by-step algorithm for constructing $n \times n$ S-boxes over the Eisenstein integer residue class ring.

3.1. Step-by-Step Construction Methodology

(i) **Group Formation:** Use the definitions and theorems outlined in Section 2 to form a cyclic group $G \subset \mathbb{Z}[\Omega]^*$ of order $p - 1$, where $p = N(E)$ is a rational prime derived from the norm of an Eisenstein prime E.

(ii) **Mapping Function:** Define a nonlinear mapping over the cyclic group $G = \{x_1, x_2, \ldots, x_{p-1}\}$ by:

$$g(x_i) = \frac{1}{ax_i^{-1} + b},$$

where x_i^{-1} is the multiplicative inverse of $x_i \in G$, and $a, b \in \mathbb{Z}[\Omega]\setminus\{0\}$ are parameters chosen to ensure bijectivity and cryptographic complexity.

(iii) **Component Separation:** Decompose each $g(x_i)$ into its non-Ω (real) and Ω-part (imaginary) components:

$$g(x_i) = u_i + v_i\Omega.$$

(iv) **Modulo Operation:** Apply modular reduction over 2^n to both components independently to generate two sets:

$$g_1 = \{u_i \bmod 2^n\}, \quad g_2 = \{v_i \bmod 2^n\}.$$

(v) **Affine Transformation:** Define affine transformations over the sets g_1 and g_2 as:

$$h(x_i) = (cx_i + d) \bmod 2^n,$$

where $c, d \in \mathbb{Z}$ are carefully selected constants that maximize nonlinearity and cryptographic resistance [24].

(vi) **Final S-box Pair:** Construct the final S-boxes S_1 and S_2 by applying the affine transformation to the elements of g_1 and g_2, respectively:

$$S_1(i) = h(u_i), \quad S_2(i) = h(v_i), \quad \text{for } i = 0, 1, \ldots, 2^n - 1.$$

3.2. Significance of Eisenstein Integer-Based S-boxes

The proposed method yields S-boxes with strong cryptographic characteristics, including:

- Enhanced arithmetic capabilities through Eisenstein modular operations,
- Improved resistance to differential and linear attacks via optimized algebraic structure,
- Increased statistical randomness and nonlinearity due to the combined mapping and transformation stages.

These properties make Eisenstein integer-based S-boxes highly suitable for use in substitution–permutation networks (SPNs), block ciphers, and multimedia security systems.

3.3. Construction of 8×8 S-boxes over Eisenstein Integers

To demonstrate the practicality of the proposed algorithm, we construct a pair of 8×8 S-boxes over the Eisenstein residue class ring using an Eisenstein prime:

$$E = 73 + 31\Omega.$$

The norm of this Eisenstein integer is:

$$N(E) = 73^2 - 73 \cdot 31 + 31^2 = 4027,$$

which is a prime number in $\mathbb{Z}$. Therefore, the residue class ring $\mathbb{Z}[\Omega]_E$ forms a finite field, and the generator $\delta \in \mathbb{Z}[\Omega]_E^*$ is selected accordingly.

By applying the aforementioned construction steps and selecting appropriate transformation constants a, b, c, d, we generate the final S-box pair S_1 and S_2. These are presented in Tables 1 and 2, respectively.

Table 1: S_1 over the non-Omega Part of EI

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

3.4. Nonlinearity Analysis of Eisenstein Integer-Based S-boxes

S-boxes derived from Eisenstein integers demonstrate strong nonlinearity properties, which critically enhance their resistance against linear and differential cryptanalysis. Due to their inherent hexagonal lattice structure, Eisenstein integers provide a unique mathematical foundation for S-box construction that supports advanced security features. Nonlinearity in an S-box is quantitatively defined as the smallest Hamming distance between the output Boolean functions of the S-box and the set of all affine functions. Higher nonlinearity values directly correlate with stronger resistance against linear approximation attacks. The symmetric and multiplicative properties of Eisenstein integers, when applied to S-box construction, yield nonlinearity metrics that match or surpass those observed in classical S-boxes defined over finite fields of characteristic two. Through Eisenstein integer-based transformations, the input differentials are dispersed more uniformly, enabling the S-box to achieve both high nonlinearity and low differential uniformity. These characteristics are essential for thwarting differential attacks by reducing the probability of predictable output differences. Simulation-based experiments and theoretical evaluations confirm that symmetric-key cryptographic schemes employing Eisenstein-integer-based S-boxes offer elevated levels of security. The comparative analysis with standard S-box constructions is presented in Tables 3 and 4, highlighting the robustness of the proposed S-box architecture against known cryptanalytic techniques [24, 27, 31].

3.5. Bit Independence Criterion (BIC)

The Bit Independence Criterion (BIC) is a vital statistical measure for evaluating the resistance of S-boxes against linear and differential cryptanalysis. It assesses how inde-

Table 2: S_2 over the Omega Part of EI

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

Table 3: Nonlinearity of Proposed S-boxes Functions

S-boxes	g_1	g_2	g_3	g_4	g_5	g_6	g_7	g_8
S_1	106.00	106.00	108.00	108.00	106.00	108.00	106.00	108.00
S_2	106.00	106.00	108.00	108.00	106.00	108.00	106.00	108.00

pendently output bits respond when a single input bit is flipped, revealing the presence or absence of linear correlations or predictable dependencies among output bits. Eisenstein-integer-based S-boxes utilize their rich algebraic and symmetric structures to disrupt these correlations effectively. Their hexagonal lattice foundation and modular arithmetic contribute to a highly nonlinear and unpredictable mapping between inputs and outputs. These mathematical features lead to enhanced propagation of bit differences across the output, minimizing potential vulnerabilities exploitable by attackers. The BIC evaluation for the constructed S-boxes S_1 and S_2 demonstrates their strong statistical independence among output bits. Computational simulations and empirical analyses validate that both S-boxes meet high BIC standards, indicating robust protection against both linear and

Table 4: Average Nonlinearity Comparisons

S-boxes	Schemes	Nonlinearity
S_1	Proposed (EI)	107.00
S_2	Proposed (EI)	107.00
[27]	Elliptic Curve	104.00
[24]	Gaussian Integers	106.50
[31]	Chaotic Map	104.70

differential attack strategies [25, 27]. The BIC matrices for S_1 and S_2 are presented in Tables 5 and 6, respectively, followed by a comparative summary with existing literature in Table 7.

Table 5: BIC Analysis Matrix for S-box S_1

0.000	0.506	0.516	0.514	0.516	0.486	0.512	0.490
0.506	0.000	0.490	0.486	0.510	0.504	0.498	0.473
0.516	0.490	0.000	0.502	0.529	0.479	0.516	0.471
0.514	0.486	0.502	0.000	0.510	0.500	0.512	0.484
0.516	0.510	0.529	0.510	0.000	0.527	0.518	0.518
0.486	0.504	0.479	0.500	0.527	0.000	0.502	0.506
0.512	0.498	0.516	0.512	0.518	0.502	0.000	0.492
0.490	0.473	0.471	0.484	0.518	0.506	0.492	0.000

Table 6: BIC Analysis Matrix for S-box S_2

0.000	0.506	0.516	0.514	0.516	0.486	0.512	0.490
0.506	0.000	0.490	0.486	0.510	0.504	0.498	0.473
0.516	0.490	0.000	0.502	0.529	0.479	0.516	0.471
0.514	0.486	0.502	0.000	0.510	0.500	0.512	0.484
0.516	0.510	0.529	0.510	0.000	0.527	0.518	0.518
0.486	0.504	0.479	0.500	0.527	0.000	0.502	0.506
0.512	0.498	0.516	0.512	0.518	0.502	0.000	0.492
0.490	0.473	0.471	0.484	0.518	0.506	0.492	0.000

Table 7: Comparison of BIC Scores with Existing Literature

S-boxes	Maximum	Minimum	Average
S_1 (Proposed)	0.594	0.391	0.502
S_2 (Proposed)	0.594	0.391	0.502
[27]	0.543	0.473	0.503
[25]	0.609	0.375	0.505

3.6. Strict Avalanche Criterion (SAC)

A secure cryptographic evaluation of S-box remaining strength depends on the SAC, which guarantees input bit alterations result in output bit changes with a 50% probability for each bit. The algebraic features of Eisenstein integers create a special foundation for building S-boxes which demonstrate exceptional diffusion properties. Complex transformations in this structure distribute non-linearly the input variations throughout the output bits, thus improving avalanche results. A SAC-compliant S-box requires that each output bit position shows complete independence to input changes and maintains equal

probability of change, which makes it impossible for adversaries to predict bit transitions. Arithmetic operations inside this Eisenstein lattice domain establish complex bit interrelationships which make the system secure. Results from computational assessments show that Eisenstein-integer-based S-boxes achieve an almost perfect SAC because their output bits display uniform change distribution after any input bit modification. SAC resistance against differential cryptanalysis depends on this property, which makes symmetric cryptographic systems incorporating the mentioned S-box design methods more secure [25, 27]. SAC reports a comparison of proposed results against existing literature through Tables 8, 9, and 10.

Table 8: SAC Analysis of S_1

0.484	0.500	0.516	0.531	0.531	0.484	0.500	0.547
0.531	0.500	0.438	0.563	0.484	0.500	0.547	0.500
0.578	0.422	0.563	0.500	0.500	0.563	0.531	0.422
0.516	0.500	0.500	0.500	0.531	0.422	0.516	0.500
0.406	0.500	0.563	0.547	0.500	0.500	0.438	0.500
0.516	0.500	0.547	0.516	0.578	0.484	0.531	0.500
0.469	0.469	0.516	0.516	0.531	0.563	0.531	0.375
0.531	0.453	0.531	0.547	0.516	0.484	0.594	0.531

Table 9: SAC Analysis of S_2

0.484	0.500	0.516	0.531	0.531	0.484	0.500	0.547
0.531	0.500	0.438	0.563	0.484	0.500	0.547	0.500
0.578	0.422	0.563	0.500	0.500	0.563	0.531	0.422
0.516	0.500	0.500	0.500	0.531	0.422	0.516	0.500
0.406	0.500	0.563	0.547	0.500	0.500	0.438	0.500
0.516	0.500	0.547	0.516	0.578	0.484	0.531	0.500
0.469	0.469	0.516	0.516	0.531	0.563	0.531	0.375
0.531	0.453	0.531	0.547	0.516	0.484	0.594	0.531

Table 10: Comparison of SAC with Existing Literature

S-boxes	Maximum	Minimum	Average
S_1	0.594	0.375	0.508
S_2	0.594	0.375	0.508
[27]	0.610	0.422	0.516
[25]	0.594	0.406	0.504

3.7. Linear Approximation Probability

The Linear Approximation Probability (LAP) serves as a key cryptographic property of S-boxes made from Eisenstein integers because it measures the highest possible correlation differences between linear input-output expressions, thereby determining the resistance against linear cryptanalysis. Eisenstein integers provide complex algebraic properties which increase the mapping complexities of S-boxes to protect them from linear approximation attacks. A Low Probability of Approximation (LAP) in an S-box functions to protect security because it prevents the determination of output-input relationships with probabilities greater than 0.5 through linear equations. S-boxes built from Eisenstein field arithmetic show highly non-linear behavior because they spread input variations through nonlinear modular arithmetic operations. The selection and optimization process for Eisenstein integer mappings enables these S-boxes to demonstrate minimal bias in linear approximation, which results in low maximal LAP metrics. Eisenstein-integer-based S-boxes demonstrate strong resistance against linear attacks through empirical testing and theoretical evaluation because they function well in secure encryption algorithms [25, 27]. A comparison between the proposed work and existing literature regarding the LAP can be seen in Table 11.

Table 11: Comparison of LAP with Existing Literature

S-boxes	LAP
S_1	0.125
S_2	0.125
[27]	0.148
[25]	0.133

3.8. Differential Approximation Probability

The Differential Approximation Probability (DAP) represents a fundamental criterion for evaluating the resistance of S-boxes generated by Eisenstein integers because it determines the maximum probability of detecting output differentials from particular input differentials. Eisenstein integers establish an original mathematical framework which leads to better distribution of data while minimizing the ability to predict differential characteristics. A low DAP value stops attackers from detecting any specific differential output relation based on input variations since it generates unknown output differences based on every input combination. The nonlinear outcome of complex multiplication with Eisenstein integers within the domain uses modular arithmetic to distribute input differences randomly throughout the output dimensions. The precise construction of Eisenstein integer mapping functions leads these S-boxes to possess minimal differential uniformity which ensures that any differential pair remains unlikely to happen. The strong resistance to differential cryptanalysis demonstrated by Eisenstein-integer-based S-boxes qualifies them as ideal components for secure encryption algorithms that need powerful nonlinearity and

diffusion characteristics [25, 27]. The proposed results undergo DAP with literature comparison through Tables 12, 13, and 14.

Table 12: DAP Analysis of S_1

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 13: DAP Analysis of S_2

0.02344	0.03906	0.02344	0.03125	0.02344	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	0.02344	0.02344	0.02344	0.03125	0.03125	0.02344	0.02344	0.03125	0.02344	0.02344	0.03906	0.02344	0.03906	0.02344
0.02344	0.03125	0.03125	0.02344	0.02344	0.03125	0.02344	0.02344	0.02344	0.02344	0.02344	0.03125	0.03125	0.02344	0.03125	0.03125
0.03125	0.02344	0.03125	0.02344	0.03125	0.03125	0.02344	0.02344	0.03125	0.02344	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	0.03125	0.02344	0.02344	0.03125	0.02344	0.03125	0.02344	0.01562	0.02344
0.02344	0.02344	0.02344	0.02344	0.03125	0.02344	0.03125	0.02344	0.02344	0.03125	0.02344	0.03125	0.03125	0.02344	0.03906	0.02344
0.02344	0.02344	0.02344	0.02344	0.02344	0.03125	0.03125	0.03125	0.03125	0.02344	0.02344	0.02344	0.02344	0.02344	0.02344	0.02344
0.02344	0.02344	0.03125	0.03125	0.03125	0.02344	0.03125	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	0.03125	0.03125	0.03125	0.03125	0.03125	0.02344	0.02344	0.02344	0.02344	0.02344	0.02344	0.02344
0.02344	0.02344	0.03125	0.03125	0.03125	0.03125	0.02344	0.02344	0.02344	0.03125	0.02344	0.03125	0.02344	0.02344	0.02344	0.03125
0.04688	0.03125	0.02344	0.02344	0.02344	0.02344	0.02344	0.02344	0.01562	0.03125	0.03125	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	0.02344	0.03125	0.03125	0.02344	0.03125	0.03125	0.03125
0.01562	0.03125	0.02344	0.02344	0.02344	0.03125	0.03906	0.03125	0.03125	0.02344	0.03125	0.02344	0.03125	0.02344	0.02344	0.02344
0.02344	0.02344	0.03125	0.02344	0.02344	0.02344	0.02344	0.03906	0.02344	0.02344	0.02344	0.02344	0.02344	0.03906	0.02344	0.02344
0.03125	0.03125	0.02344	0.02344	0.03906	0.03125	0.03125	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	0.03125	0.03125	0.03125	0.02344	0.02344	0.02344	0.02344	0.02344	0.02344	0.03125	0.03125	0.00000

Table 14: Comparison of DAP with Existing Literature

S-boxes	DAP
S_1	0.039
S_2	0.047
[27]	0.047
[25]	0.039

3.9. Fixed Point, DBN, LBN, and Linear Structure

A fixed point in an S-box is defined as a value $S(x) = x$. The presence of fixed points can weaken the cryptographic strength of an S-box, as they provide predictable mappings that may be exploited by adversaries. Secure S-box designs aim to avoid or minimize fixed points. However, in certain cryptographic systems, the inclusion of fixed points is intentional to satisfy specific design objectives [22, 33]. Table 15 presents a comparative analysis of fixed points.

The Differential Branch Number (DBN) is a key cryptographic metric used to evaluate an S-box's resistance to differential cryptanalysis. It is defined as the minimum sum of active input and output bits for all nonzero input differences. An S-box with a high DBN ensures strong diffusion, making it more difficult for an attacker to exploit differential patterns since a minor change in the input causes widespread changes in the output. Thus, optimizing DBN improves the diffusion characteristics of S-boxes and enhances security against differential attacks [22, 33]. The linear approximation is used to evaluate resistance against linear cryptanalysis through the Linear Branch Number (LBN). It is defined as the minimum sum of active input and output bits over all nonzero linear masks. A high LBN indicates strong resistance to linear approximations, meaning that linear relationships between input and output bits are minimized. This significantly reduces the probability of successful linear attacks, thereby enhancing the security of symmetric key cryptosystems [22, 33]. Table 15 compares the DBN and LBN values of different S-boxes.

An S-box is said to exhibit a Linear Structure (LS) if there exists an input difference a and an output difference b such that for all x, $S(x \oplus a) \oplus S(x) = b$. The existence of such structures indicates predictability in transformations, making the S-box vulnerable to linear cryptanalysis. Hence, a secure S-box should have no or very few linear structures to ensure high nonlinearity and resistance to such attacks [22, 33]. A comparison of the LS property is also presented in Table 15.

Table 15: Comparison of FP, DBN, LBN, and LS with Existing Literature

S-boxes	DBN	LBN	FP	LS
S_1	1	1	1	0
S_2	3	1	1	0
[33]	1	2	2	0
[22]	2	2	2	0

4. Multiple RGB Image Algorithm over Eisenstein Integer

The encryption process of multiple RGB images using Eisenstein integers $\mathbb{Z}[\omega]$ consists of the following sequential steps:

(i) **Input Preparation**
The encryption process begins with importing the RGB images requiring protection. Each image is composed of Red, Green, and Blue components. The pixel values are transformed by mapping the color channels to elements of the Eisenstein integer ring $\mathbb{Z}[\omega]$, preparing the data for secure encoding.

(ii) **S-box Construction**
As detailed in Section 3, two 8×8 S-boxes, denoted as S_1 and S_2, are constructed over the residue classes of Eisenstein integers $\mathbb{Z}[\omega]$. These structures are integral to increasing the cryptographic strength of the encryption scheme.

(iii) **SPN Framework**
The proposed Substitution-Permutation Network (SPN) framework applies the constructed S-boxes to enhance the security of multiple RGB images using three primary stages:

(a) **Substitution Phase**
The substitution phase begins with applying S-box S_1 to introduce non-linearity (confusion). All pixel values from the Red, Green, and Blue channels are substituted such that the output values exhibit a non-linear dependency on the input. The usage of $\mathbb{Z}[\omega]$ increases security due to its rich algebraic structure, making cryptanalysis (especially linear and differential attacks) significantly harder.

(b) **Permutation Phase**
The next stage applies S-box S_2 to perform permutations that enhance diffusion. Pixel values from each channel are spatially rearranged so that patterns are removed, and substitution effects are spread across the entire image. A distinct permutation is applied to each color channel to avoid predictable transformations.

(c) **Final XOR Operation**
A third S-box S_3 is dynamically generated by XORing S_1 and S_2. This S-box is then used to XOR the pixel values of the image. This introduces further randomness and enhances complexity. The XOR operation ensures that without the proper key (which generates S_3), the transformation cannot be reversed.

(iv) **Final Transformation**
The SPN process thoroughly transforms each channel, optimizing both confusion and diffusion, and thereby safeguarding the image from a broad range of cryptanalytic attacks.

(v) **Output the Encrypted Image**
After applying the transformations, the modified Red, Green, and Blue channels are combined to form the final encrypted image. This encryption process is applied across all images in the dataset.

(vi) **Final Output**
The resulting encrypted images exhibit significantly increased entropy, lower correlation between adjacent pixels, and enhanced resistance against differential and linear attacks, ensuring the robustness of multimedia data transmission.

Significance of the SPN Framework:
The proposed three-stage SPN achieves an optimal balance between confusion and diffusion, critical for effective cryptographic systems. The dynamic switching and shuffling operations eliminate sequential predictability and ensure that visual transformations are distributed uniformly throughout the image. The incorporation of the XOR operation via S_3 introduces high unpredictability, minimizing susceptibility to cryptanalytic techniques.

Leveraging Eisenstein integer residue classes $\mathbb{Z}[\omega]$ constructs encryption layers that are far more complex than traditional RSA, thus substantially enhancing security.
Sections 3 and 4 S-box construction joins the production process with multiple RGB image encryption methods as described in Section 5 according to Figure 1.

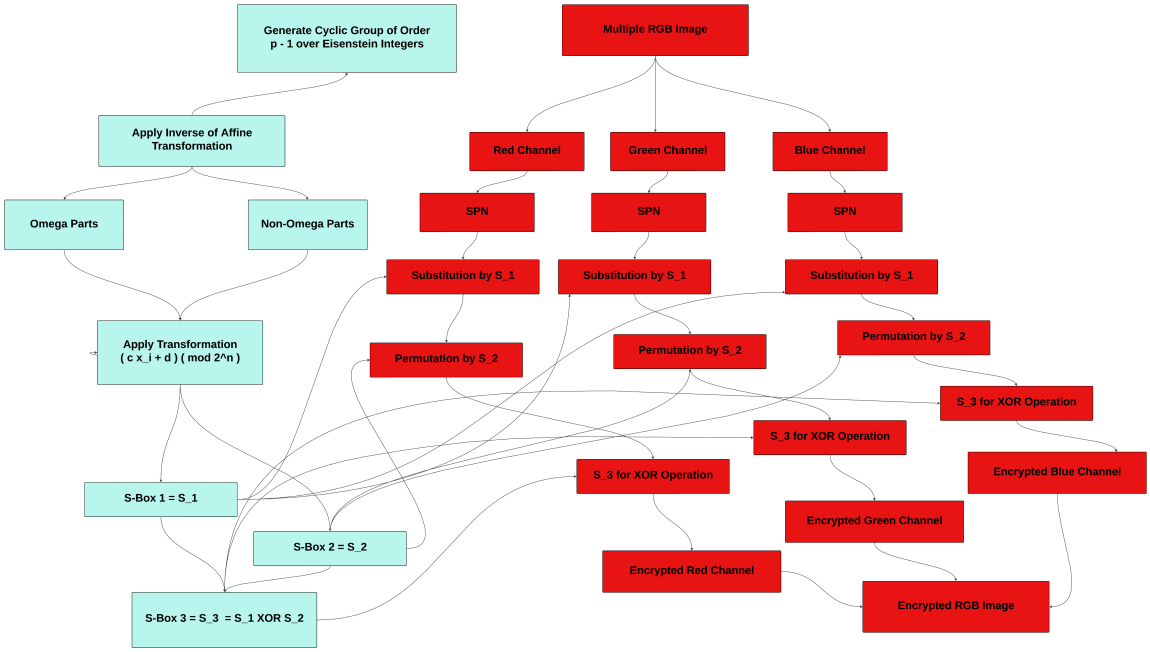


Figure 1: Flowchart of the Proposed Study

5. Multiple RGB Image Encryption Implementation and Analysis over Eisenstein Integers

This innovative form of encryption protects digital images using the mathematical structure of Eisenstein integers for multiple RGB image files. The encryption method processes the color channels—Red, Green, and Blue—through a higher-dimensional algebraic space, providing powerful diffusion and confusion security capabilities. The process employs several transformations, including substitution-permutation networks (SPNs) and chaotic mappings, and performs modular arithmetic over Eisenstein integers to build highly sensitive systems resistant to known cryptographic attacks such as differential and statistical threats. By leveraging the non-trivial number-theoretic properties of Eisenstein integers, the encryption scheme introduces complexity that makes keyless decryption of protected images highly impractical for adversaries. This technique offers superior security features compared to traditional cryptographic methods due to increased randomness and entropy. Furthermore, the method demonstrates optimal performance in concurrent image processing, enabling the encryption of multiple images in parallel by exploiting the inherent algebraic structure for efficient key management. This contributes significantly to

secure image transmission, multimedia security, and cloud storage applications by ensuring both confidentiality and integrity of visual data. Figure 2 displays two original RGB images labeled A and B, alongside their corresponding encrypted versions, illustrating the effectiveness of the proposed encryption scheme.

(a) Original Image A (b) Original Image B

(c) Encrypted Image A (d) Encrypted Image B

Figure 2: Original RGB images (a) and (b), and their encrypted versions (c) and (d) using the proposed Eisenstein-integer-based encryption.

5.1. Histogram Analysis

Histogram analysis serves as a key statistical tool in evaluating the security of multiple RGB image encryption schemes based on Eisenstein integers. Specifically, it assesses the

distribution of pixel intensities across the red, green, and blue channels in the encrypted images. An effective encryption method produces histograms with uniform distributions for all channels, indicating the elimination of original image patterns and correlations. In the proposed method, complex arithmetic operations over Eisenstein integers ensure high randomness in the distribution of pixel values. This randomness disrupts statistical regularities, thereby thwarting adversaries from exploiting histogram-based cryptanalytic techniques. The visual comparison of the histograms of original and encrypted images offers a direct measure of encryption strength. A robust encryption approach is validated when the histogram of the encrypted image diverges significantly from the original, resembling a noise-like uniform distribution. Such transformation demonstrates the success of the diffusion and confusion mechanisms embedded in the encryption algorithm. The histogram analysis, therefore, confirms the encryption system's resilience against statistical attacks and its ability to preserve data confidentiality during storage or transmission [24, 25]. The histogram results for Image B are illustrated in Figure 3.

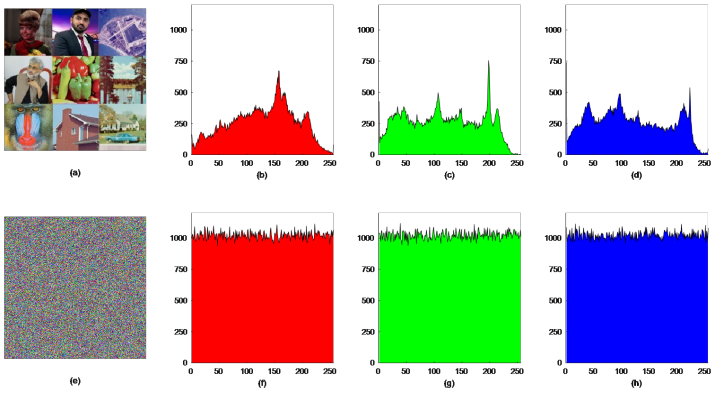


Figure 3: Histogram comparison of original and encrypted Image B across RGB channels

5.2. NPCR and UACI

The Number of Pixel Change Rate (NPCR) is a fundamental metric for evaluating the security of multiple RGB image encryption schemes, especially those based on Eisenstein integers. It quantifies the degree of pixel modification resulting from slight changes in the input image. A robust encryption system should yield NPCR values close to 99%, indicating that even minimal changes in the plaintext image cause widespread alterations in the encrypted image. This characteristic enhances resistance against differential attacks, since it becomes nearly impossible for an attacker to infer how small changes in the input propagate through the encryption process. The arithmetic operations over Eisenstein integers contribute to this unpredictability by spreading changes across all three RGB channels.

The Unified Average Changing Intensity (UACI) quantifies the average intensity variation between original and encrypted images. A high UACI value (ideally around 33% for

8-bit images) signifies that the encryption process successfully disrupts pixel intensities, preventing any correlation or leakage of statistical patterns from the original image. The use of Eisenstein integer arithmetic further reinforces encryption strength by applying modular transformations that obscure relationships between the input and output data.

Table 16 provides a comparative analysis of NPCR and UACI values for two encrypted images (Image A and Image B), alongside results from previously published methods [5, 22, 24, 26, 34]. These results confirm the effectiveness of the proposed encryption method in achieving high security through high NPCR and UACI values.

Table 16: NPCR and UACI analysis

	NPCR			UACI		
Images	Red	Green	Blue	Red	Green	Blue
Image A	0.9961	0.9962	0.9961	0.2990	0.3151	0.3178
Image B	0.9963	0.9961	0.9962	0.2964	0.3091	0.3115
[26]	0.9960	0.9961	0.9961	0.3347	0.3347	0.3346
[5]	0.9969	0.9969	0.9966	0.3367	0.3332	0.3367
[22]	0.9961	0.9961	0.9961	0.3544	0.3177	0.3419
[24]	0.9959	0.9964	0.9962	0.3269	0.3037	0.2762
[34]	0.9960	0.9961	0.9963	0.2956	0.3094	0.3112

5.3. Maximum Deviation and Irregular Deviation

Maximum deviation serves as a fundamental metric to assess multiple RGB image encryption over Eisenstein integers because it determines the biggest possible difference between pixel distributions of plaintext and ciphertext images. An encryption process achieves effective pixel value randomization when maximum deviation numbers are elevated, which reduces the correlation between plaintext and ciphertext visuals. The encryption process needs this randomness to stop attacks based on statistical analysis because adversaries could spot patterns between pixels to discover keys or rebuild parts of the original content. Eisenstein integer-based encryption employs algebraic structure for pixel changes that enhance pixel intensity differences between color channels of images. Strong diffusion properties of an encryption algorithm across multiple images are verified through continuing maximum deviation assessments of the encryption process. The security assessment of the encryption scheme benefits from this metric, and it pairs effectively with NPCR and UACI to show the system's effectiveness in producing secure image encryption results [22, 24, 34]. The deviations from MD testing are provided within Table 17.

The assessment of encryption effectiveness relies on irregular deviation, as it measures the irregular pixel intensity variations between original and encrypted images. The encryption algorithm's ability to interrupt adjacent pixel value connections becomes visible through Eisenstein integer-based multiple RGB image encryption since irregular deviation measures pixel variation discrepancies. A high irregular deviation results from encryption schemes that create complicated color channel transformations to disrupt all substantial or

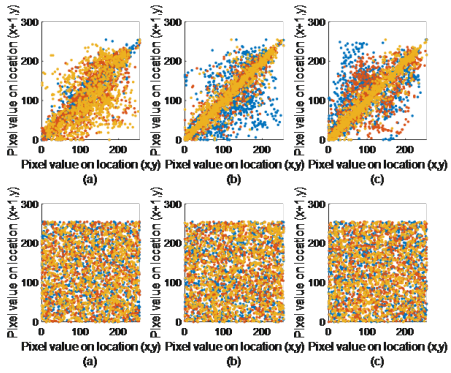
linear relationships between neighbouring image pixels. Eisenstein integers augment the encryption security through their non-commutative, non-associative mathematical properties, which fragment pixel intensity distribution and impede attacks on encrypted data. The security of the encryption process strengthens as multiple image encryptions produce high irregular deviation values throughout all channels, which creates randomized ciphertext appearance similar to noise patterns [22, 24, 34]. Table 17 presents the results regarding ID.

Table 17: Maximum Deviation and Irregular Deviation Comparative Analysis

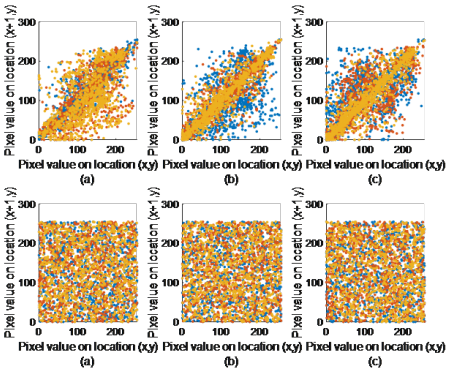
	MD			ID		
Images	Red	Green	Blue	Red	Green	Blue
Encrypted Image A	58211	49079	54201	27373	27770	27072
Encrypted Image B	60779	58417	57547	38072	38030	38125
[22]	53397	48329	53529	29231	25127	28374
[24]	60210	47069	62218	26266	19443	27027
[34]	52021	61841	61742	38097	37989	37924

5.4. Correlation Analysis

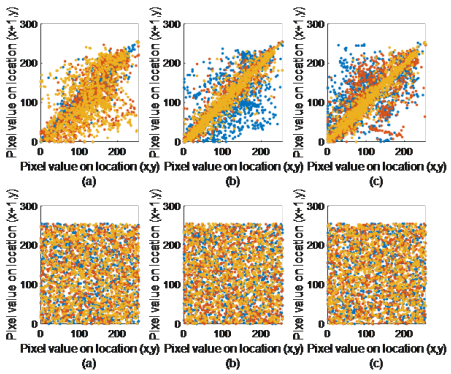
A critical security evaluation of multiple RGB image encryption over Eisenstein integers depends on correlation analysis which analyzes horizontal, vertical, and diagonal directions. The research analyzes the connection patterns between image pixel values across multiple image orientations. A reliable encryption solution should produce no substantial relationships between pixels of an encrypted image because this implies pixels should not affect neighboring pixels. The encrypted pixel relationships in Eisenstein integer systems become harder to break because the system's algebraic functionality combines complex mathematics with modular arithmetic. The encrypted image shows complete pixel independence in all directions, as its horizontal, vertical, and diagonal correlation values tend toward zero. The absence of pattern definitions between any pair of horizontal, vertical, or diagonal pixels enhances security by resisting multiple statistical attacks. Without these image correlations, attackers struggle to predict pixel values based on positions and surrounding pixels. This robustness improves further when the encryption method simultaneously processes multiple RGB images, as the lack of correlation affects every color channel and direction. After encryption, the images transform into random noise patterns, ensuring higher security and protection against standard attacks. This mechanism safeguards image integrity in practical scenarios like secure transmission and encrypted storage [5, 22, 24, 26, 34]. The analysis is supported by the correlation values and images presented in Figure 5 and Table 18.



(a) Horizontal Correlation



(b) Diagonal Correlation

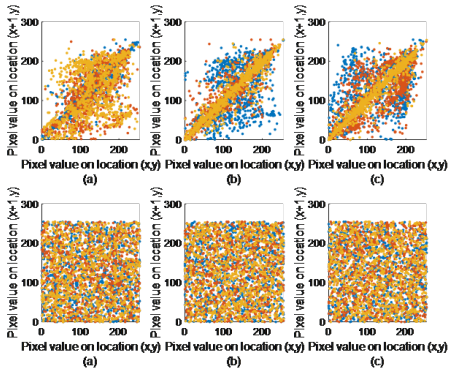


(c) Vertical Correlation

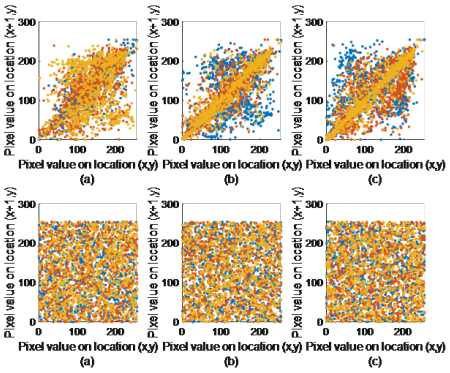
Figure 4: Correlation analysis of Image A in horizontal, diagonal, and vertical directions

5.5. Information Entropy

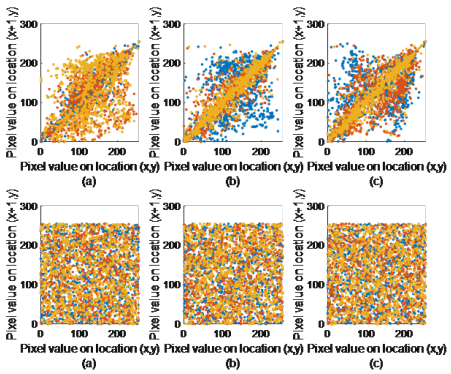
The assessment of encrypted image unpredictability and randomness depends upon information entropy, which shows how successfully encryption methods remove discernible patterns from original images. The multiple RGB image encryption over Eisenstein integers uses entropy to determine the uncertainty and disorder of encrypted image pixel intensity distributions. A perfect entropy rating near the maximum value indicates a uniform pixel intensity distribution, which represents maximal disorder and randomness in the image. The protection of encrypted images depends heavily on high entropy because increased randomness makes statistical analysis insufficient to reveal important information about original images. By implementing Eisenstein integers in the encryption process, the scheme achieves randomness through complex arithmetic operations that destroy image structure and produce encrypted content with distributed pixel values. The encryption method preserves security when applied to RGB image collections because it generates equally high entropy values across all red, green, and blue channels, demonstrating complete masking of predictable data. Encryption methods with this feature provide strong protection by making images resistant to cryptanalysis and unauthorized statistical anal-



(a) Horizontal Correlation



(b) Diagonal Correlation



(c) Vertical Correlation

Figure 5: Correlation analysis of Image B in horizontal, vertical, and diagonal directions

ysis [5, 24, 26, 34]. The entropy evaluation of the proposed work is in agreement with existing research, as shown in Table 19.

5.6. MSE and PSNR

The evaluation of encryption effectiveness depends heavily on the Mean Squared Error (MSE), as this metric quantifies the average pixel intensity deviations between the original and encrypted images through squared differences. The proposed encryption method demonstrates significant modification to pixel intensities; a high MSE value indicates that the encrypted image exhibits considerable differences from its original form. In the case of multiple RGB image encryption over Eisenstein integers, such alterations enhance security by ensuring that all discernible patterns and structural similarities vanish. The complex non-linear transformations using Eisenstein integers induce maximum diffusion, transforming the original image into an encrypted form with substantial variations. The high MSE values across red, green, and blue channels confirm the robustness of the encryption against statistical attacks [22, 34]. Furthermore, consistently high MSE values across different images signify the reliability of the method in preserving security across

Table 18: Comparative Analysis of Horizontal, Diagonal, and Vertical Correlation

		Horizontal			Diagonal			Vertical		
Images	Red	Green	Blue	Red	Green	Blue	Red	Green	Blue	
Image A Original	Red	0.5620	0.9271	0.9426	0.5351	0.9108	0.9153	0.5420	0.9474	0.9431
	Green	0.5420	0.9474	0.9431	0.5494	0.9068	0.9054	0.5506	0.9410	0.9388
	Blue	0.5089	0.7093	0.9524	0.5234	0.7250	0.8961	0.5423	0.7284	0.9462
Image A Encrypted	Red	-0.0098	0.0084	0.0187	-0.0572	0.0584	-0.0036	-0.0238	0.0209	-0.0200
	Green	0.0365	0.0077	0.0653	-0.0037	0.0120	0.0005	-0.0037	-0.0565	-0.0145
	Blue	-0.0269	0.0285	0.0286	-0.0044	-0.0220	-0.0877	-0.0194	0.0168	0.0103
Image B Original	Red	0.9169	0.5977	0.3950	0.8780	0.6129	0.3067	0.9302	0.5772	0.4273
	Green	0.3930	0.9145	0.9449	0.3178	0.8745	0.8974	0.3839	0.9018	0.9323
	Blue	0.4005	0.7157	0.9434	0.3418	0.6757	0.9139	0.3793	0.7213	0.9276
Image B Encrypted	Red	-0.0117	-0.0382	0.0538	0.0122	0.0282	0.0625	0.0297	-0.0072	-0.0500
	Green	0.0503	0.0148	-0.0193	-0.0327	0.0185	0.0353	-0.0236	0.0494	-0.0306
	Blue	-0.0539	0.0508	-0.0197	0.0015	0.0488	0.0018	0.0063	0.0147	0.0331

Table 19: Information Entropy comparison

	Information Entropy			
Images	Red	Green	Blue	Average
Image A	7.9993	7.9993	7.9993	7.9993
Image B	7.9993	7.9993	7.9994	7.9994
[26]	7.9913	7.9914	7.9916	7.9916
[5]	7.9995	7.9995	7.9994	7.9995
[24]	7.9976	7.9967	7.9976	7.9987
[34]	7.9992	7.9994	7.9993	7.9993

varied inputs. The MSE evaluation of the proposed work is in agreement with existing research, as shown in Table 20.

Peak Signal-to-Noise Ratio (PSNR) serves as a complementary metric to MSE, measuring the ratio of maximum possible pixel intensity to the MSE on a logarithmic scale. In secure image encryption, low PSNR values are preferred, as they signify large deviations between original and encrypted images. The use of Eisenstein integers ensures non-linear and unpredictable pixel alterations, resulting in minimal resemblance between the two. The inverse relationship between MSE and PSNR validates the effectiveness of the encryption; higher MSE corresponds to lower PSNR, reflecting greater data obfuscation. All RGB channels show uniformly low PSNR values, indicating strong diffusion and confusion properties. The encryption process becomes more secure when such consistency is observed across multiple images, ensuring that no visual or statistical reconstruction of the original image is feasible. This confirms the capability of the proposed encryption scheme in safeguarding RGB image confidentiality [22, 34]. The PSNR evaluation of the proposed work is in agreement with existing research, as shown in Table 20.

5.7. Contrast and Energy

The assessment of multiple RGB image encryption over Eisenstein integers relies significantly on contrast measurements, as this metric reflects the pixel intensity variations

Table 20: MSE and PSNR Comparative Analysis

	MSE			PSNR		
Images	Red	Green	Blue	Red	Green	Blue
Original Image A	44.1849	44.4965	44.1297	2.50	2.33	2.53
Encrypted Image A	44.2659	44.3553	44.2291	2.45	2.40	2.47
Original Image B	44.1320	43.9747	44.2144	2.53	2.62	2.48
Encrypted Image B	44.3440	44.3418	44.2445	2.41	2.41	2.47
Original [22]	44.6746	44.2313	44.9505	2.23	2.47	2.10
Encrypted [22]	44.3020	44.3185	44.4057	2.43	2.42	2.38
Original [34]	44.1849	44.4965	44.1297	2.50	2.33	2.53
Encrypted [34]	44.1080	44.2180	44.3952	2.54	2.48	2.38

between adjacent pixels in an image. An effective encryption process should drastically alter the contrast levels of the original image, aiming to minimize any perceptible patterns in the ciphered output. The proposed encryption method, which employs Eisenstein integers, applies complex mathematical transformations that introduce widespread changes in the image, effectively removing all original intensity gradients—even those arising from subtle pixel value differences. This encryption technique produces images where pixel intensities are uniformly randomized, leading to noise-like patterns that obscure any identifiable structures or features. Consequently, contrast analysis of several RGB images processed by this method shows no meaningful intensity correlation, validating the cryptographic strength of the proposed approach. By suppressing contrast-based patterns, the encryption ensures protection against attacks that exploit visual characteristics or perceptual cues, thereby safeguarding image privacy during storage and transmission [5, 22, 34]. The contrast evaluation results are presented in Table 21.

In addition, the encryption of multiple RGB images over Eisenstein integers is evaluated using energy as a complementary statistical measure. Energy quantifies the uniformity and intensity distribution within an image by computing the sum of squared pixel values. After encryption, the resulting image exhibits lower energy due to the uniform distribution of pixel values, induced by the complex algebraic operations involved in the Eisenstein integer framework. This reduction in energy confirms the randomness of the ciphered image, eliminating recognizable intensity concentrations. The encryption process consistently maintains this low-energy distribution across all RGB components, thus providing a uniform ciphertext with minimal structural cues. Such randomness resists cryptanalysis attempts based on statistical inference, ensuring high data confidentiality in practical applications such as secure transmission and storage of digital images [5, 22, 34]. The energy evaluation results are presented in Table 21.

5.8. Homogeneity and Standard Deviation

The security evaluation of RGB image encryption based on Eisenstein integers depends on analyzing image pixel uniformity through homogeneity. Homogeneity measures the closeness of similar intensity values in an image; encrypted images should ideally ex-

Table 21: Contrast and Energy Analysis of Different Images

Images	Contrast			Energy		
	Red	Green	Blue	Red	Green	Blue
Original Image A	0.5693	0.6411	0.6196	0.0752	0.0735	0.0713
Encrypted Image A	10.5229	10.5093	10.5358	0.0156	0.0156	0.0156
Original Image B	0.6062	0.7930	0.6063	0.0828	0.0748	0.0906
Encrypted Image B	10.5357	10.4913	10.4710	0.0156	0.0156	0.0156
Original [5]	0.5439	0.5000	0.4726	0.0779	0.0821	0.1708
Encrypted [5]	10.5114	10.4770	10.4894	0.1051	0.1048	0.1049
Original [22]	0.4717	0.4879	0.4261	0.0838	0.0834	0.1242
Encrypted [22]	10.4878	10.4861	10.5034	0.0156	0.0156	0.0156
Original [34]	0.5693	0.6411	0.6196	0.0752	0.0735	0.0713
Encrypted [34]	10.5357	10.4913	10.4710	0.0156	0.0156	0.0156

hibit low homogeneity to demonstrate that uniform patterns are thoroughly disrupted. A robust encryption algorithm using Eisenstein integers randomizes pixel intensity values across the full range, causing neighboring pixels to become decorrelated and visually noisy. This outcome confirms effective confusion and diffusion in all three RGB channels. Consistently low homogeneity values across images indicate that the encryption technique masks structured image content and defends against unauthorized statistical analysis [22, 34]. The homogeneity evaluation results are presented in Table 22.

In parallel, standard deviation (SD) serves as a statistical measure to evaluate the dispersion of pixel intensities. A high SD in encrypted images implies that pixel values are spread over the entire possible range, supporting the presence of randomness and information diffusion. Eisenstein-based transformations induce such statistical unpredictability via their nonlinear arithmetic properties. A secure image encryption process should exhibit high SD across all RGB channels, aligning the encrypted image statistics with white noise and minimizing the risk of pattern leakage [22, 34]. The standard deviation evaluation results are presented in Table 22.

Table 22: Homogeneity and Standard Deviation Analysis of Different Images

Images	Homogeneity			Standard Deviation		
	Red	Green	Blue	Red	Green	Blue
Original A	0.8335	0.8324	0.8293	57.4332	64.5652	65.8041
Encrypted A	0.3890	0.3891	0.3880	73.9658	73.9845	73.9391
Original B	0.8384	0.8198	0.8499	54.7733	63.0304	63.5231
Encrypted B	0.3891	0.3892	0.3899	73.9073	73.9022	73.9116
Original [22]	0.8855	0.8726	0.8855	9.5315×10^3	8.5820×10^3	1.0732×10^4
Encrypted [22]	0.3892	0.3897	0.3889	72.3821	67.0023	61.9652
Original [34]	0.8835	0.8324	0.8293	57.4332	64.5652	65.8041
Encrypted [34]	0.3891	0.3892	0.3899	73.8951	73.9193	73.9622

5.9. NIST Test

The NIST test suite serves as a comprehensive benchmark to evaluate the statistical strength of encryption algorithms, especially for RGB image encryption using Eisenstein integers. This suite encompasses various randomness tests to ensure that encrypted images exhibit properties similar to truly random sequences, thereby making them resilient to cryptographic attacks. The frequency and block frequency tests assess whether pixel values are evenly distributed. The rank test evaluates linear independence of pixel groups, while the runs test (with $M = 10,000$) checks the occurrence of consecutive identical bits. The long runs of ones test identifies long uninterrupted sequences, ensuring that no patterns survive encryption. Template-based tests like overlapping and non-overlapping templates detect fixed patterns within encrypted data. The Discrete Fourier Transform (DFT) test checks for periodic features in pixel distributions. The approximate entropy test measures data complexity, while the universal test and serial test examine compression potential and sequence structure, respectively. Both forward and reverse cumulative sum tests identify systematic biases. The random excursions and random excursions variants assess the behavior of cumulative sums across specific states. Successful performance across these tests indicates effective diffusion and confusion. Eisenstein integer-based encryption demonstrates uniformly high security performance across RGB channels, as shown in Table 23. The algebraic complexity and chaotic properties of Eisenstein operations significantly improve encryption robustness, leading to highly unpredictable output that resists statistical and differential cryptanalysis [5, 22, 24, 26, 34].

Table 23: NIST Analysis of RGB Image A

Tests		P-values			Remarks
		Red	Green	Blue	
Frequency		0.41097	0.19479	0.80028	✓
Block frequency		0.96476	0.74492	0.02102	✓
Rank		0.29191	0.29191	0.29191	✓
Runs (M=10,000)		0.74369	0.70048	0.61359	✓
Long runs of ones		0.71270	0.71270	0.71270	✓
Overlapping templates		0.85988	0.85988	0.85988	✓
No overlapping templates		0.92285	0.99561	0.96777	✓
Spectral DFT		0.46816	0.11048	0.24574	✓
Approximate entropy		0.00610	0.68249	0.50842	✓
Universal		0.98125	0.98914	0.98654	✓
Serial	p values 1	0	0.26606	0.22531	✓
Serial	p values 2	0	0.47179	0.06546	✓
Cumulative sums forward		0.23783	0.36684	0.18702	✓
Cumulative sums reverse		1.06720	1.62490	0.88700	✓
Random excursions	X = -4	0.87792	0	0.91256	✓
	X = -3	0.36782	0.22540	0.83339	✓
	X = -2	0.62224	0.79201	0.35516	✓
	X = -1	0.48909	0.87691	0.85346	✓
	X = 1	0.76990	0.87691	0.71270	✓
	X = 2	0.47291	0.82820	0.86295	✓
	X = 3	0.73730	0.98202	0.86069	✓
	X = 4	0.85692	0.98894	0.59778	✓
Random excursions variants	X = -5	0.91388	1.00000	0.59588	✓
	X = -4	0.80626	0.89369	0.59298	✓
	X = -3	0.77167	0.52709	0.69263	✓
	X = -2	0.92538	0.10247	0.75946	✓
	X = -1	0.62650	0.07710	0.85968	✓
	X = 1	0.33039	0.47950	0.72367	✓
	X = 2	0.22339	0.54029	1.00000	✓
	X = 3	0.16808	0.52709	0.75183	✓
	X = 4	0.24403	0.59298	0.89369	✓
	X = 5	0.30423	0.63735	0.76828	✓

6. Conclusion and Future Directions

The proposed encryption method based on a Substitution-Permutation Network (SPN) operating over Eisenstein integers $\mathbb{Z}[\omega]_\pi$ establishes a robust framework for securing multiple RGB images. The cryptographic strength of the system is enhanced by its novel S-box architecture, which leverages the algebraic properties of Eisenstein integers to achieve high

nonlinearity and effective modular arithmetic. By integrating substitution operations with permutations and XOR mechanisms in an SPN structure, the scheme achieves substantial diffusion and confusion properties, improving its resistance to linear and differential cryptanalysis. The encryption system ensures data integrity and processing efficiency by independently securing each color channel, making it a viable solution for encrypted multimedia transmission. The method demonstrates practical potential for image security through high entropy, low correlation, and strong resistance against statistical and structural attacks.

Although promising, the algorithm could benefit from further development, particularly for real-time implementation and hardware acceleration to enhance performance in large-scale applications. Additionally, future research may explore the application of Eisenstein integers in cryptographic primitives such as key exchange protocols and digital signature schemes. A comprehensive security analysis against contemporary and emerging attack techniques would further establish its applicability in secure communication systems.

Acknowledgements

This research is supported by Universidad Pedagógica y Tecnológica de Colombia (SGI 3725) and Minciencias (Conv. 934).

Data availability

The images used in this study were obtained from 'The USC-SIPI Image Database' (https://sipi.usc.edu/database). The images were combined and processed to meet the specific pixel requirements of the experiment. The researcher can contact to the Muhammad Sajjad for getting the images.

Tribute

We wish to express our heartfelt gratitude to our beloved supervisor, Professor Dr. Tariq Shah (late), whose exceptional guidance, profound knowledge, and unwavering support profoundly shaped our journey as researchers in algebra, number theory, coding theory, and cryptography. His mentorship was a cornerstone of our academic and personal growth, and his presence continues to inspire our scholarly endeavours. May his soul rest in eternal peace.

Figure 6: Prof. Dr. Tariq Shah

References

[1] Alfred J Menezes, Paul C Van Oorschot, and Scott A Vanstone. *Handbook of applied cryptography*. CRC press, 2018.

[2] Ronald L Rivest. *Cryptography*. Elsevier, 1990.

[3] Claude Carlet and Cunsheng Ding. Nonlinearities of s-boxes. *Finite fields and their applications*, 13(1):121–135, 2007.

[4] Gang Cheng, Chuan Wang, and Hao Chen. A novel color image encryption algorithm based on hyperchaotic system and permutation-diffusion architecture. *International Journal of Bifurcation and Chaos*, 29(09):1950115, 2019.

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

[6] V. Buçaj. Finding factors of factor rings over the eisenstein integers. In *Int. Math. Forum*, volume 9, pages 1521–1537, 2014.

[7] M. M. Hazzazi, M. Sajjad, Z. Bassfar, T. Shah, and A. Albakri. Nonlinear components of a block cipher over eisenstein integers. *CMC-Computers Materials & Continua*, 77(3):3659–3675, 2023.

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

[9] M. Sajjad, T. Shah, Q. Xin, and B. Almutairi. Eisenstein field bch codes construction and decoding. *AIMS Mathematics*, 8(12):29453–29473, 2023.

[10] Muhammad Sajjad, Tariq Shah, Muhammad Abbas, Mohammad Alammari, and Raul J Serna. The impact of alternant codes over eisenstein integers on modern technology. *Computational and Applied Mathematics*, 44(1):95, 2025.

[11] C. L. Li, H. M. Li, F. D. Li, D. Q. Wei, X. B. Yang, and J. Zhang. Multiple-image encryption by using robust chaotic map in wavelet transform domain. *Optik*, 171:277–286, 2018.

[12] Shengli Wang, Chuan Wang, and Cheng Xu. An image encryption algorithm based on a hidden attractor chaos system and the knuth–durstenfeld algorithm. *Optics and Lasers in Engineering*, 128:105995, 2020.

[13] X. Y. Wang and Z. M. Li. A color image encryption algorithm based on hopfield chaotic neural network. *Optics and Lasers in Engineering*, 115:107–118, 2019.

[14] Qi Yin and Chuan Wang. A new chaotic image encryption scheme using breadth-first search and dynamic diffusion. *International Journal of Bifurcation and Chaos*, 28(04):1850047, 2018.

[15] X. Zhang and X. Wang. Multiple-image encryption algorithm based on dna encoding and chaotic system. *Multimedia Tools and Applications*, 78(6):7841–7869, 2019.

[16] Min Zhou and Chuan Wang. A novel image encryption scheme based on conservative hyperchaotic system and closed-loop diffusion between blocks. *Signal Processing*, 171:107484, 2020.

[17] P. Deng, M. Diao, M. Shan, Z. Zhong, and Y. Zhang. Multiple-image encryption using spectral cropping and spatial multiplexing. *Optics Communications*, 359:234–239, 2016.

[18] W. Liu, Z. Xie, Z. Liu, Y. Zhang, and S. Liu. Multiple-image encryption based on optical asymmetric key cryptosystem. *Optics Communications*, 335:205–211, 2015.

[19] X. Wang and S. Gao. Image encryption algorithm for synchronously updating boolean networks based on matrix semi-tensor product theory. *Information Sciences*, 507:16–36, 2020.

[20] Y. Xiong, C. Quan, and C. J. Tay. Multiple image encryption scheme based on pixel exchange operation and vector decomposition. *Optics and Lasers in Engineering*, 101:113–121, 2018.

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

[22] 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 z[i]_h. *Scientific Reports*, 15(1):1–21, 2025.

[23] M. Sajjad, T. Shah, and R. J. Serna. Designing pair of nonlinear components of a block cipher over gaussian integers. *Computers, Materials & Continua*, 75(3), 2023.

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

[25] 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.

[26] 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.

[27] S. Ibrahim and A. Alharbi. Efficient image encryption scheme using henon map, dynamic s-boxes and elliptic curve cryptography. *IEEE Access*, 8:194289–194302, 2020.

[28] Z. Shamsi, A. K. Saha, R. Patgiri, K. M. Singh, and L. D. Singh. Steganalysis on dual-layer security of messages using steganography and cryptography. In *2023 15th International Conference on Information Technology and Electrical Engineering (ICITEE)*, pages 264–269. IEEE, 2023.

[29] X. Wang, L. Feng, and H. Zhao. Fast image encryption algorithm based on parallel computing system. *Information Sciences*, 486:340–358, 2019.

[30] X. Li, X. Meng, X. Yang, Y. Wang, Y. Yin, X. Peng, and H. Chen. Multiple-image encryption via lifting wavelet transform and xor operation based on compressive ghost imaging scheme. *Optics and Lasers in Engineering*, 102:106–111, 2018.

[31] X. Zhang and X. Wang. Multiple-image encryption algorithm based on the 3d permutation model and chaotic system. *Symmetry*, 10(11):660, 2018.

[32] X. Y. Wang, Y. Q. Zhang, and X. M. Bao. A novel chaotic image encryption scheme using dna sequence operations. *Optics and Lasers in Engineering*, 73:53–61, 2015.

[33] F. Artuğer and F. Özkaynak. An effective method to improve nonlinearity value of substitution boxes based on random selection. *Information Sciences*, 576:577–588, 2021.

[34] Muhammad Sajjad and Nawaf A. Alqwaifly. A novel spn based multiple rgb images security over the residue classes of quaternion integers h[k]_. *European Journal of Pure and Applied Mathematics*, 18(2):6228, 2025.