EUROPEAN JOURNAL OF PURE AND APPLIED MATHEMATICS
2025, Vol. 18, Issue 2, Article Number 6228
ISSN 1307-5543 – ejpam.com
Published by New York Business Global

A Novel SPN based Multiple RGB Images Security over the Residue Classes of Quaternion Integers $H[K]_\delta$

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. In this paper, we propose a Substitution and Permutation Network (SPN)-based encryption scheme for secure multiple RGB images over the residue classes of quaternion integers $H[K]_\delta$. In this context, the new construction of $n \times n$ substitution boxes (S-boxes) using quaternion integers is proposed in order to enhance cryptographic strength. The traditional approaches for S-boxes are mostly based on Gaussian, Eisenstein, and elliptic curves, but quaternion integers are a four-dimensional algebra that is somewhat different mathematically, and these provide additional resistance in terms of cryptographic attacks. The strong security attributes of the designed S-boxes. As for multiple RGB image encryption, in order to achieve both confusion and diffusion, the proposed method employs the SPN framework and quaternion integer-based S-boxes. Structured SPN framework based on substitution, permutation, and XOR operations used by the encryption algorithm. It is shown that the encryption method proposed greatly increases the resistance against statistical, differential, and cryptanalytic attacks. The quaternion integer-based encryption framework is used to convey the confidentiality and integrity of multiple RGB images, which promises to be a good solution for secure multimedia applications. The results confirm that quaternion integer algebra can constitute a useful basis for constructing resilient cryptographic primitives for the modern digital security challenges.

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

Key Words and Phrases: Quaternion integers, Multiple RGB Image Encryption, SPN, Confusion, Diffusion, Security Analysis

1. Introduction

To safeguard multimedia content from unauthorized access, tampering, and cyber threats, advanced cryptographic techniques have emerged in response to the evolving landscape of digital communication and data sharing. Traditionally these include AES

*Corresponding author.
*Corresponding author.
DOI: https://doi.org/10.29020/nybg.ejpam.v18i2.6228

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

and RSA-type schemes but have been rendered less viable due to challenges like the quantum computing threat and so on; thus, we now have more resilient approaches like post-quantum cryptography (PQC), homomorphic encryption and lattice-based cryptosystems. Although encryption in multimedia security is not sufficient, further mechanisms such as digital watermarking, steganography, and perceptual hashing are incorporated for authenticity and copyright protection while allowing for secure content distribution. In addition, chaos-based encryption methods and cryptographic models built using deep learning have established a place for them, as they allow for improvement over randomness and adaptability, thus making them ideally suitable to face off against statistical and differential attacks. Since the development of blockchain technology, secure multimedia transactions have also been explored on the basis of security frameworks that are decentralized the need, on the one hand, to depend on centralized authorities and, on the other hand, to guarantee traceability and integrity in these transactions. Cryptography also becomes more optimized for reducing stronger security mechanisms through artificial intelligence and machine learning by increasing synergy with cryptography [1]. This means that adaptive security can be done that focuses on real-time threats in multimedia communications.

The primary component of non-linearity in block ciphers is substitution boxes (S-boxes), which are very important components to strengthen the crypto security because they provide confusion and are immune to cryptanalytic attacks. This design of an optimal S-box balances various cryptographic properties such as high nonlinearity, low differential uniformity, and minimum probability of linear approximation to make the S-box robust against linear and differential cryptanalysis. Current S-box construction approaches are based on algebraic structures, specifically in the form of finite fields; however, there have been a number of developments in constructing S-boxes from a more sophisticated algebraic domain, i.e., Gaussian and Eisenstein integers, quaternion algebras, and Galois fields, to increase their cryptographic strength. Furthermore, S-boxes are generated dynamically by evolutionary algorithms, artificial intelligence techniques and deep learning models according to the needs of an evolving security challenge. Currently, modern encryption protocols start introducing dynamic and key-dependent S-boxes in order to introduce additional complexity and make the cryptographic systems less vulnerable with respect to the adaptive attacks. However, their application is not limited to the conventional ciphers but also extends to the transparent braiding ciphers, where they are found important in the areas of lightweight cryptography, chaotic encryption schemes, and secure image processing, where the nonlinearity in them is a very effective means of providing security of data and unpredictability of data [2, 3].

The single and multiple image RGB encryption is a very complex task which must be done to ensure confidentiality, integrity, and resistance to tax attacks while retaining the visual data quality. In contrast to grayscale images whose pixel intensity values lie in only one channel, RGB images contain three interdependent color channels, and consequently there exist specialized encryption techniques to deal with the multi-dimensional structure of the RGB images. Pixel-level permutation and diffusion mechanisms are conventional;

modern approaches involve the use of chaos theory, fractal geometry or DNA encryption with strength of security and efficiency. Furthermore, the encryption over quaternion and Eisenstein integer domains is also more robust by bringing in structurally higher dimensions into the algebraic structures, thereby enhancing randomness and intrinsic security. For multiple image encryption applications, joint encryption schemes, compressive sensing, etc., are used for simultaneous encryption and, at the same time, keeping complexity low. Moreover, real-time image encryption using a hybrid model that improves adaptability and efficiency was also explored by combining deep learning and cryptographic techniques. Moreover, robust encryption mechanisms for RGB multimedia data are desired due to the increasing demand for secure image transmission in medical imaging, surveillance, etc [4, 5].

Quaternion integers allow us to move past complex numbers and take an extension of algebra into a four-dimensional algebraic system with some unique properties that have been used in cryptography, coding theory and secure communications. Quaternion algebras are defined as the non-commutative extension of the Gaussian and Eisenstein integers and yield a rich mathematical framework in which one can define cryptographic primitives with enhanced security characteristics. Such inherent structure allows the development of SPNs with improved confusion and diffusion properties and secure realization of encryption schemes. Quaternion-based constructions in error-correcting codes help in robust channel coding techniques, which enhance the data reliability in a noisy communication environment. Moreover, quaternion integer-based cryptosystems have also been used for public key encryption, digital signatures and secure key exchange protocols using their algebraic complexity that makes them resistant to conventional cryptanalytic attacks. Indeed, recent research also explores their usage in image and signal processing, specifically in extracting new and secure features in image and signal representation. Also, with the growing evolution in the security threats, the integration of quaternion-based mathematical structures in the modern cryptographic systems can open a way to develop enhanced configurable cryptographic information spread algorithms with high performance and enhanced resistance towards the modern attack vectors [6–8].

To begin with, the encryption system is based on algebraic structures and multimedia security, which is now a key component in the encryption schemes. On the other hand, Menezes et al. [1] report in detail traditional cryptographic methods which offer strong and secure communications. These challenges, however, call for the adoption of the advanced mathematical structures with quaternion integers, which allow more algebraic properties in the encryption and error correction [6]. Ozen and Guzeltepe [9, 10], which bring the use of quaternion integers into cyclic codes, and hence into robust encryption schemes. Shah and Rasool [8] also develop this research by demonstrating how quaternion-based coding can be advantageous in secure data transmission. More recently, Sajjad and Shah [7] suggest a version of the Berlekamp–Massey algorithm for decoding cyclic codes over quaternion integers, which further confirms their cryptographic power. Additionally, Sajjad et al. [11] give higher-length cyclic codes based on quaternion integers as well as new

decoding algorithms for better error resilience. S-boxes are fundamental nonlinear components in symmetric cryptography to make it secure by introducing confusion. Khan et al. [3] provide more motivation for the construction of strong S-boxes by noting that this remains a focal area of research, and we use chaotic Lorenz systems to construct robust substitution boxes. Carlet and Ding [2] give a comprehensive consideration on how to analyze S-box nonlinearities from a cryptographic point of view. These concepts are then utilized to design S-boxes over Gaussian and Eisenstein integers by Sajjad et al. [12, 13] and shown to be useful in block cipher security. Moreover, in [4] the substitution box generator is introduced that is purpose-built for image encryption together with its extension of quaternion intensity in [14] to achieve enhanced nonlinearity and security. These results have been further optimized in recent research of Artuğer and Özkaynak [15], who applied randomized selection methodologies to S-box nonlinearity.

In recent years, the increase in multimedia communication has created the need for image encryption, especially with RGB images. An SPN-based RGB image encryption scheme over Gaussian numbers is proposed by Sajjad et al. [5], and it is shown to be more resistant to statistical attacks compared to its counterpart over a finite field. Abd EL-Latif et al. [16] use quantum walk-based pseudorandom number generators for quantum color image encryption, and Ibrahim and Alharbi [17] integrate Henon maps and elliptic curve cryptography to provide efficient image security. Shamsi and Laiphrakpam [18] in a similar fashion widen the scope of multimedia data embedding to the case of audio-based image encryption. Consequently, Wang et al. [19] propose fast encryption based on parallel computing, while Cheng et al. [20] use hyperchaotic systems and permutation diffusion architecture to enhance the security. Malik and Shah [21] also design a scheme for multiple image encryption using 3D chaotic maps which utilize the power of chaos theory in multimedia security. With the development of many advanced transformations and chaotic systems, the multiple image encryption techniques have become much more complex. Both Yin and Wang [22] use breadth-first search and dynamic diffusion for better randomness, while Wang et al. [23] use DNA sequence operations for chaotic image encryption. Wang et al. [24, 25] recently created hidden attractor chaos systems and conservative hyperchaotic architectures, which strengthen cryptographic strength even more. Wang and Li [26] also combine Hopfield chaotic neural networks into color image encryption, and Wang and Gao [27] also use Boolean network synchronization. An additional dimension of security is also provided by optical cryptosystems such as asymmetric key cryptosystems for multiple image encryption described by Liu et al. [28]. Xiong et al. [29] is one other well-known contribution based on pixel exchange operations and vector decomposition, and Deng et al. [30] is yet another contribution based on spectral cropping and spatial multiplexing. Li et al. [31] also investigatedwang2020imagea wzhou2020novelform-based techniques, which, however, use robust chaotic maps for secure image encryption. Zhang and Wang [32, 33] also extend DNA encoding and 3D permutation models, and Li et al. [31] further improve security using compressive ghost imaging.

In response to the fast growth of digital communication and multimedia applications,

strong security features are required for secure access to sensitive image data from cyber or unauthorized access. Traditional methods of encryption using Gaussian integers and Eisenstein integers have been shown to be useful for protecting the content in a digital domain, but the cryptanalysis of such traditional methods has sometimes been too easy [5, 12–14]. It is further evident from the advances in attacks due to increasing sophistication, including, among others, differential cryptanalysis, linear cryptanalysis, and statistical attacks, that the need for a more resilient cryptographic framework is all the more important [2–4]. Quaternion integers form a non-commutative extension of complex numbers and, as such, furnish more algebraic structure and more security for encryption systems in a higher dimension. Relevant recent research [7, 9–11] has also pointed out quaternion algebra's possibility to be employed in building cryptographic primitives, in particular, designing S-boxes and encrypting frameworks. Indeed, the employment of quaternion integers in cryptographic applications offers some unique advantages, such as increased diffusion and confusion properties, less algebraic complexity, and a larger key space that aids in combating different attacks [5, 13, 14]. As a result, encryption schemes based on Substitution Permutation Network (SPN) are found to be very effective for secure image encryption. SPN frameworks based on S-boxes over finite fields like GF(2^n), elliptic curves or Gaussian integers, remain vulnerable to cryptanalysis for the reason that they have algebraic properties [12, 13]. This is a novel cryptographic primitive based on quaternion integer-based S-boxes which augment the nonlinearity and differential uniformity of the encryption process by introducing quaternion integer-based S-boxes into the utilization of the SPN structure [5, 14]. The rationale behind this study is that a very secure multiple RGB image encryption system based on the mathematical strength of quaternion integers is to be developed. The proposed approach is to use quaternion-integer-based S-boxes to integrate the security of digital images against multiple attacks with good efficiency of computation [5, 13, 14]. In terms of multimedia security, this research adds an innovative cryptographic model in the form of combining algebraic developments and pragmatic encryption mechanisms to address the fast-emerging difficulties that digital data protection in modern communication systems faces.

The goal of this research is to propose a new cryptographic framework, among whose building blocks are quaternion integers, which improve the security of conferences where several RGB images are being displayed at once. Another one of the key contributions is the formation of an original way to create $n \times n$ S-boxes based on quaternion integers. In contrast to other S-box designs based on Gaussian or Eisenstein integers, elliptic curves or chaotic functions, the proposed method is algebraically distinct in that it uses the exceptional four-dimensional algebraic structure of quaternion integers. As for the generated S-boxes, the non-commutative nature of quaternion multiplication allows for much more nonlinear, differential uniform, and strict avalanche characteristics than can be obtained using finite field techniques, which makes it highly resistant to linear and differential cryptanalysis. Finally, the proposed framework uses these S-boxes as substitution and permutation elements of an SPN, with the aim of guaranteeing a high degree of confusion and diffusion properties to achieve secure multimedia encryption. The work makes

another considerable contribution by introducing a fast multi-image encryption scheme which allows processing multiple RGB images simultaneously. The encryption scheme has been designed with strong security features and efficient computation, ideal for application in real time, such as secure cloud storage, medical imaging, video surveillance, etc. Statistical tests, entropy measurement, correlation analysis and differential attack resistance are rigorously performed on the proposed method, and it is shown to achieve superior performance in terms of security when compared with the existing techniques. In addition, this research points out the ability of quaternion integers to be used in the analogical cryptographic applications and lays a foundation for future studies of more high-dimensional algebraic structures, which can be used for encryption. The results lead us to conclude that the proposed system is practical and efficient, which helps to advance secure multimedia communication.

2. Quaternion Integers

By following [7–11], let $\mathbb{H}(\mathbb{R})$ be the Hamilton quaternion algebra over the real numbers $\mathbb{R}$. It is a non-commutative but associative unital algebra if it satisfies the following conditions.

- $\mathbb{H}(\mathbb{R}) = \{a_0+a_1i+a_2j+a_3k : \forall a_i \in \mathbb{R}\}$ is a free $\mathbb{R}$-module with basis $\{\pm 1, \pm i, \pm j, \pm k\}$.
- Element 1 is the multiplicative identity.
- Operations on the basis elements $\pm 1, \pm i, \pm j, \pm k$ are given in Figure. 1.

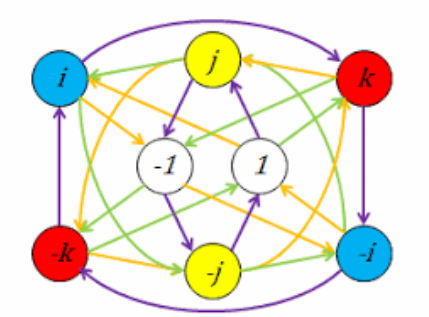

Figure 1: Multiplication of basis elements

The ring of quaternion $H(\mathbb{Z}) = \{b_0+b_1i+b_2j+b_3k : \text{ for all } b_0, b_1, b_2, b_3 \in \mathbb{Z}\}$ contained in $H(\mathbb{R})$, where $\mathbb{Z}$ is the ring of integers. If $q = b_0 + b_1i + b_2j + b_3k$ is a quaternion integer, then $\bar{q} = b_0-b_1i-b_2j-b_3k$ is the quaternion conjugate of q. Let $N(q) = q\bar{q} = b_0^2+b_1^2+b_2^2+b_3^2$ be the norm of q. A quaternion integer q has only two parts: one is the scalar part (S.P.) b_0 and the other is the vector part (V.P.) $b_1i+b_2j+b_3k$. In a quaternion, the commutative property of multiplication does not hold. It is possible only in the case of two vector parts of quaternion integers being parallel.

2.1. Subring of the Quaternion Integer Ring [7, 11]

Define $H(K)$ as:

$$H(K) = \{a + bU \mid a, b \in \mathbb{Z}\},$$

where $U = i + j + k$. Hence, $H(K)$ is a subring of the quaternion integer ring $H(\mathbb{Z})$, and also the commutative property of multiplication holds $H(K)$.

2.2. Sum and Product of Two Quaternions [6]

Let $q_1 = c_0 + c_1 i + c_2 j + c_3 k$ and $q_2 = d_0 + d_1 i + d_2 j + d_3 k$ be two quaternion integers. Then, their sum $q_1 + q_2$ and product $q_1 q_2$ will also be quaternion integers as:

$$q_1 + q_2 = (c_0 + c_1 i + c_2 j + c_3 k) + (d_0 + d_1 i + d_2 j + d_3 k)$$

$$= (c_0 + d_0) + (c_1 + d_1)i + (c_2 + d_2)j + (c_3 + d_3)k = e_0 + e_1 i + e_2 j + e_3 k = q_3.$$

$$\begin{aligned} q_1 q_2 &= (c_0 + c_1 i + c_2 j + c_3 k)(d_0 + d_1 i + d_2 j + d_3 k) \\ &= c_0 d_0 + c_0 d_1 i + c_0 d_2 j + c_0 d_3 k + c_1 d_0 i - c_1 d_1 + c_1 d_2 k - c_1 d_3 j + c_2 d_0 j - c_2 d_1 k - c_2 d_2 + c_2 d_3 i \\ &\quad + c_3 d_0 k + c_3 d_1 j - c_3 d_2 i - c_3 d_3 \\ &= (c_0 d_0 - c_1 d_1 - c_2 d_2 - c_3 d_3) + (c_0 d_1 + c_1 d_0 + c_2 d_3 - c_3 d_2) i \\ &\quad + (c_0 d_2 + c_2 d_0 + c_3 d_1 - c_1 d_3) j + (c_0 d_3 + c_3 d_0 + c_1 d_2 - c_2 d_1) k \\ &= g_0 + g_1 i + g_2 j + g_3 k = q_4. \end{aligned}$$

Theorem 1. *[3, 11], the set of natural numbers for each odd rational prime p, there exists a prime $\delta \in \mathbb{H}(\mathbb{Z})$ such that,*

$$N(\delta) = p = \delta\bar{\delta},$$

in particular, p is not prime in $\mathbb{H}(\mathbb{Z})$.

Theorem 2. *[3, 11], let $\delta \in \mathbb{H}(\mathbb{Z})$ be prime in $\mathbb{H}(\mathbb{Z})$ if and only if $N(\delta)$ is prime in $\mathbb{Z}$.*

Definition 1. *[3, 11], let $\mathbb{H}(K)_\delta$ be the residue class of $\mathbb{H}(K)$ modulo δ, where $\delta = a + bU$. Then the modulo function is defined as:*

$$\phi : \mathbb{H}(K) = \{a + bU : a, b \in \mathbb{Z}\} \to \mathbb{H}(K)_\delta,$$

$$\phi(q) = z \mod \delta = q - \left[\frac{q\bar{\delta}}{p}\right]\delta,$$

where $z \in \mathbb{H}(K)_\delta$, and the brackets $[\cdot]$ denote rounding to the nearest integer. To perform quaternion integer (QI) rounding, the scalar part (S.P.) and the coefficient of the vector part (C.V.P.) must be independently rounded to the nearest integers.

Definition 2. *[3, 11], let $\beta, \rho \in \mathbb{H}(K)_\delta$ and define $\alpha = \beta - \rho = (b_0 + b_1 i + b_2 j + b_3 k) \mod \delta$. The quaternion Mannheim weight $W_{QM}(\alpha)$ is defined as:*

$$W_{QM}(\alpha) = |b_0| + |b_1| + |b_2| + |b_3|.$$

The quaternion Mannheim distance $d_{QM}(\rho, \beta)$ between β and ρ is then given by:

$$d_{QM}(\rho, \beta) = W_{QM}(\alpha).$$

Remark 1. *[11], indeed, quaternion Mannheim weight W_{QM} is metric.*

Theorem 3. *[7], if $\gcd(a, b) = 1$, then*

$$\mathbb{H}(K)/\langle a + b(i + j + k)\rangle \cong \mathbb{Z}_{a^2+3b^2}.$$

Proposition 1. *[7], let $\delta_k = a_k + b_k(i + j + k)$ be distinct primes in $\mathbb{H}(K)$, and let $p_k = \mathbb{Z}_{a_k^2+3b_k^2}$ be distinct primes in $\mathbb{Z}$, for $k = 1, 2, 3, \ldots, m$. If g is a generator of $\mathbb{H}(K)_{\delta^k}$, then*

$$g^{\frac{\varphi(p^k)}{2}} \equiv -1 \mod \delta^k.$$

Proposition 2. *[7], let $\delta_1 = a_1 + b_1(i + j + k)$ be a prime in $\mathbb{H}(K)$, and let $p \in \mathbb{Z}_{a_1^2+3b_1^2}$ be a prime in $\mathbb{Z}$. If $\mathbb{H}(K)_\delta$ is generated by g, then*

$$\alpha^{\frac{\varphi(p)}{2}} \equiv -1 \mod \delta.$$

Corollary 1. *[7], let $\delta = a + b(i + j + k)$ be a quaternion prime in $\mathbb{H}(K)$, such that the norm $N(\delta) = p = a^2 + 3b^2$ is a prime in $\mathbb{Z}$. If $\mathbb{H}(K)_\delta$ is generated by α, then*

$$\alpha^{\varphi(p)} \equiv 1 \mod \delta.$$

Remark 2. *The group generated by $\langle\alpha\rangle$ in the above Corollary is denoted by $\mathcal{Q}_R$.*

3. Quaternion Integers based $n \times n$ S-boxes

Substitution boxes (S-boxes) are essential components used in modern cryptography, introducing confusion in encryption algorithms to enhance their security. Traditionally, S-boxes are constructed using finite fields. However, recent studies reveal the potential of quaternion integers to design highly nonlinear and cryptographically resilient S-boxes. Quaternions, which generalize complex numbers into a four-dimensional non-commutative algebra, provide unique mathematical properties that offer increased resistance to cryptanalytic attacks. In the proposed method, the S-box is defined as a $k \times k$ matrix of quaternion integers. The quaternion algebraic structure is then employed to construct $n \times n$ ($n \leq k$) S-boxes with desirable cryptographic properties such as high nonlinearity and low differential uniformity. Quaternion integer elements are systematically selected and integrated into a secure substitution layer with strong security and sound efficiency. The construction utilizes an optimization algorithm to enhance cryptographic strength.

S-Box Construction Steps:

(i) Based on definitions and theorems in Section II, a quaternion integer-based cyclic group, denoted as Q_R, is defined. This group is structured to have an order of $p-1$.

(ii) The group Q_R is subjected to the following transformation and mapped to another quaternion group using a transformation function:

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

where x_i^{-1} is the multiplicative inverse of x_i in Q_R, and a and b are quaternion integers. The expression $ax_i^{-1} + b$ must be a non-zero part of the quaternion residue class.

(iii) The scalar and vector parts of the resulting quaternion elements are separated to form the output of the mapping function. These components are processed independently in the following steps.

(iv) Apply modular reduction modulo 2^n to each component (scalar and vector), producing two separate sets of order 2^n, denoted as Q_{R_1} and Q_{R_2}.

(v) Another transformation is applied to both sets Q_{R_1} and Q_{R_2} using the function:

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

where c and d are constants carefully selected to ensure the cryptographic properties such as high nonlinearity and low differential uniformity are met.

(vi) A secure encryption process is then performed to generate a pair of S-boxes, denoted S_s and S_v, using quaternion operations. These S-boxes serve as the core nonlinear components in cryptographic systems to resist various attacks.

Significance of Quaternion-Based S-Boxes: The use of quaternion integers in the construction of S-boxes provides several advantages that can enhance both the security and efficiency of the substitution layers in block ciphers. Unlike traditional finite field-based S-boxes, quaternion-based S-boxes leverage the non-commutative algebraic structure of quaternions to introduce increased complexity and resilience to attacks. Due to their four-dimensional nature, quaternions offer a richer mathematical framework, improving nonlinearity — a critical attribute against differential and linear cryptanalysis. Quaternion integer-based S-boxes exhibit a strong avalanche effect, whereby small changes in input cause substantial changes in output, thereby enhancing security. Furthermore, such S-boxes demonstrate low differential uniformity, making differential attacks ineffective, and maintain bijectivity (one-to-one mapping), which is essential for secure substitution. Moreover, these S-boxes are efficient and scalable, making them ideal for modern cryptographic applications, including lightweight encryption schemes for resource-constrained environments such as IoT devices and embedded systems. Consequently, quaternion integer-based S-boxes emerge as robust and promising alternatives to traditional designs, offering enhanced protection against emerging cryptographic threats.

4. 8×8 S-boxes over Quaternion Integers and Analysis

From quaternion algebra transformations, it is possible to construct 8×8 S-boxes with scalar and vector parts independently processed. Suppose the quaternion prime

$$\delta = 80 + 31i + 31j + 31k,$$

with norm

$$N(\delta) = 9283,$$

being prime in $\mathbb{Z}$, and the generator

$$\alpha = 2 + 19i + 19j + 19k.$$

Two S-boxes are constructed distinctively as follows:

(i) **Scalar Parts S-box S_s:** This S-box S_s is designed by running all the steps as described above on the real (scalar) part of quaternions. It is mapped using the 'inverse affine' transformation, modular arithmetic, and the transformation function $h(x_i)$ applied to the input values.

(ii) **Vector Parts S-box S_v:** This is an S-box created for the vector (pure quaternion) part, based on the transformation of the i, j, k parts of quaternion elements to make it resistant to differential attacks.

By independently designing S_s and S_v, the resulting S-boxes, the vulnerability to cryptanalysis is reduced in both cryptographic applications, secure image encryption, and block ciphers. This is achieved by utilizing the multidimensional algebraic properties of quaternions. Tables 1 and 2 contain the completed S-box values.

4.1. Nonlinearity

S-box nonlinearity (NL) represents a fundamental element of cryptographic strength because S-boxes use quaternion integer parts to generate separate nonlinearity functions between scalar and vector components. The S-boxes benefit from quaternion algebra to achieve their increased complexity since this mathematical framework exploits the multidimensional nature of the structure. The scalar S-box performs computations on quaternion element real parts through modular transformations and permutation mappings along with affine operations, thereby establishing high levels of nonlinearity that counter linear approximations. The vector S-box uses modular exponentiation and rotation-based diffusion together with non-affine substitutions as individual transformations for the pure quaternion components to achieve strong resistance to differential cryptanalysis. The evaluation of S-box nonlinearity depends on calculating their Hamming distances from affine functions to ensure maximum unpredictability in output variations from small input variations. The quaternion structure protects system security through the distribution of mathematical operations among multiple parts, which reduces statistical correlations, making it practically

Table 1: S_s over the scalar part of QI

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

impossible to perform linear approximations. These S-boxes achieve strong confusion and diffusion capabilities through independent scalar and vector part processing, which protects against attacks including linear cryptanalysis, differential cryptanalysis and algebraic attacks. The complex encryption system's strength increases through the combination of quaternion integer algebraic characteristics in substitution processes. The distinct nonlinearity features of quaternion-based S-boxes provide an enhanced cryptographic approach for developing block ciphers along with implementing secure image encryption systems and future cryptographic protocol designs [3, 5, 12, 17]. The research for nonlinearity characteristics and relevant literature review appears in the proposed results in Table 3 as well as Table 4.

4.2. Bit Independent Criteria

It is crucial for enhancing resistance against differential and linear cryptanalysis that the S-boxes over quaternion integers are separately constructed according to the Bit Independent Criteria (BIC) nonlinearity of the scalar and vector parts. The more independent the change of each output bit with respect to changes in input is, the more this criterion is satisfied, and there should be no predictable pattern of any bit. By applying modular transformation and affine mappings to the real part of quaternion elements, the scalar S-box is designed such that each output bit is statistically independent. On the other hand, the vector S box processes the pure quaternion components separately using different modular exponentiation and rotation-based transformations to increase the unpredictability of the output bits. We compute the correlation between pairs of output bits and find that changes in one bit do not affect the others in a way that is predictable. In cryptographic applications this bit independence property is critical, since the presence of such

Table 2: S_v over the scalar part of QI

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

Table 3: NL of the S-box functions

S-boxes	g_1	g_2	g_3	g_4	g_5	g_6	g_7	g_8
S_s	108.00	108.00	106.00	108.00	108.00	104.00	106.00	108.00
S_v	108.00	108.00	106.00	108.00	108.00	104.00	106.00	108.00

an S-box renders the linear correlations or differential trails attacked useless. Quaternion-based S-boxes, due to independent scalar and vector processes of the scalar and vector parts, spread bit changes over several dimensions, and their complexity and security are further increased. Because quaternions are inherently multidimensional, the BIC of the patterns remains very dispersed among bits, rendering algebraic and statistical attacks ineffective. The properties are such that quaternion-based S-boxes are indeed highly suited for cryptographic applications like secure encryption, block cipher design, and advanced data protection mechanisms [12, 13, 17]. Part of the proposed research of BIC is shown in Tables 5, 6, and 7, which present the results and comparative analysis of the results

Table 4: NL of the S-box functions

S-boxes	Schemes	Nonlinearity
S_s	Proposed (QI)	107.00
S_v	Proposed (QI)	107.00
[12]	Eisenstein Integers	106.75
[17]	Elliptic Curve	104.00
[3]	Chaotic Map	104.70
[5]	Gaussian Integers	106.50

found in existing literature.

Table 5: BIC of S_s

0.0	0.5371	0.4785	0.4980	0.5020	0.4922	0.5000	0.5137
0.5371	0.0	0.4844	0.5332	0.5020	0.5156	0.4902	0.5000
0.4785	0.4844	0.0	0.4824	0.4883	0.4922	0.5137	0.4902
0.4980	0.5332	0.4824	0.0	0.4805	0.4863	0.5117	0.4980
0.5020	0.5020	0.4883	0.4805	0.0	0.5039	0.5020	0.5059
0.4922	0.5156	0.4922	0.4863	0.5039	0.0	0.4824	0.4980
0.5000	0.4902	0.5137	0.5117	0.5020	0.4824	0.0	0.5000
0.5137	0.5000	0.4902	0.4980	0.5059	0.4980	0.5000	0.0

Table 6: BIC of S_v

0.0	0.5371	0.4785	0.4980	0.5020	0.4922	0.5000	0.5137
0.5371	0.0	0.4844	0.5332	0.5020	0.5156	0.4902	0.5000
0.4785	0.4844	0.0	0.4824	0.4883	0.4922	0.5137	0.4902
0.4980	0.5332	0.4824	0.0	0.4805	0.4863	0.5117	0.4980
0.5020	0.5020	0.4883	0.4805	0.0	0.5039	0.5020	0.5059
0.4922	0.5156	0.4922	0.4863	0.5039	0.0	0.4824	0.4980
0.5000	0.4902	0.5137	0.5117	0.5020	0.4824	0.0	0.5000
0.5137	0.5000	0.4902	0.4980	0.5059	0.4980	0.5000	0.0

Table 7: BIC of S_v

S-boxes	Maximum	Minimum	Average
S_s	0.609	0.391	0.499
S_v	0.609	0.391	0.499
[12]	0.625	0.391	0.502
[17]	0.543	0.473	0.503
[13]	0.609	0.375	0.505

4.3. Strict Avalanche Criterion

The strict avalanche criterion of S-boxes over quaternion integers is a key property for high diffusion and cryptographic attack resistance. For the S-box to be used in SAC, the change from the input, as tiny as flipping a single bit, should lead to about a 50% change of the output bits; i.e., it should be highly unpredictable. The real part of quaternion elements is applied to the scalar S-box in quaternion-based scale S-box design by using modular transformations and affine mapping, so that the scalar S-box retains strong avalanche property in the scalar domain. On the contrary, the vector S-box works on the

independent imagination component separately, and doing so independently of its transformations, such as modular exponentiation, rotation-based diffusion, and non-affine permutations, in order to maximize the number of bit transitions induced from input changes. The quaternion structure, however, develops an inherent way of enhancing SAC compliance due to multidimensional transformations encasing the effects of each single bit flip over both scalar and vector components, resulting in a much greater global flow of outputs. This property greatly contributes to security since it makes it impossible for attackers to establish predictable relationships between input and output values. Quaternion-based cryptographic systems are said to meet SAC requirements, so that they ensure the scalar and vector S-boxes are resistant to differential and linear cryptanalysis and therefore are appropriate cryptographic systems for use in encryption, block ciphers, and other types of advanced cryptographic systems [12, 13, 17]. Tables 8, 9 and 10 compare the proposed results to existing literature via SAC.

Table 8: SAC of S_s

0.53125	0.546875	0.5	0.5625	0.484375	0.546875	0.46875	0.515625
0.46875	0.4375	0.515625	0.515625	0.484375	0.53125	0.46875	0.546875
0.546875	0.4375	0.515625	0.46875	0.59375	0.484375	0.4375	0.5
0.53125	0.484375	0.515625	0.53125	0.5	0.546875	0.46875	0.5
0.515625	0.421875	0.5	0.5625	0.46875	0.515625	0.46875	0.5
0.515625	0.546875	0.5	0.5	0.546875	0.40625	0.484375	0.5
0.5625	0.515625	0.5625	0.5	0.484375	0.453125	0.5	0.53125
0.484375	0.53125	0.546875	0.421875	0.53125	0.53125	0.453125	0.46875

Table 9: SAC of S_v

0.53125	0.546875	0.5	0.5625	0.484375	0.546875	0.46875	0.515625
0.46875	0.4375	0.515625	0.515625	0.484375	0.53125	0.46875	0.546875
0.546875	0.4375	0.515625	0.46875	0.59375	0.484375	0.4375	0.5
0.53125	0.484375	0.515625	0.53125	0.5	0.546875	0.46875	0.5
0.515625	0.421875	0.5	0.5625	0.46875	0.515625	0.46875	0.5
0.515625	0.546875	0.5	0.5	0.546875	0.40625	0.484375	0.5
0.5625	0.515625	0.5625	0.5	0.484375	0.453125	0.5	0.53125
0.484375	0.53125	0.546875	0.421875	0.53125	0.53125	0.453125	0.46875

4.4. Linear Approximation Probability

Linear Approximation Probability (LAP) of S-boxes over quaternion integers over scalar and vector domains separately is an important measure to resist linear cryptanalysis such that the linear relation between input and output bits is not easily exploitable. Another thing is the efficiency of the attacks — the lower the LAP value, the higher the probability that no linear equation will fit the S-box accurately; therefore, the attacks

Table 10: SAC Comparison

S-boxes	Maximum	Minimum	Average
S_s	0.594	0.406	0.503
S_v	0.594	0.406	0.503
[12]	0.578	0.375	0.502
[17]	0.610	0.422	0.516
[13]	0.594	0.406	0.504

remain ineffectual. In quaternion-based S-box construction, the scalar S-box is designed by doing modular arithmetic and doing affine transformation on the real part of the quaternion so that the correlations between input and output are still nonlinear. To further reduce the linear dependencies, the imaginary components are transformed through independent transformations like modular exponentiation and rotation-based diffusion, as well as non-affine mappings using vector S- boxes. The nonlinearity of S-boxes is naturally improved using a quaternion structure, where the sweeping transformations over multiple dimensions increase the degree of randomness in the linearity of the approximation. An overall cryptographic system is ensured of stronger security through the low LAP of the scalar and vector S-boxes, which helps resist the linear cryptanalysis. That being said, S-boxes based on quaternions have a high suitability in encryption schemes, block ciphers, and other cryptographic applications that utilize those characteristics to keep the data safe [12, 13, 17]. Table 11 is the comparison between the proposed work and existing literature regarding the LAP.

Table 11: LAP Comparison

S-boxes	LAP
S_s	0.141
S_v	0.141
[12]	0.133
[17]	0.148
[13]	0.133

4.5. Differential Approximation Probability

Differential Approximation Probability (DAP) of S-boxes over quaternion integers is a key security parameter that characterizes their resistance against differential cryptanalysis by measuring the probability of occurring predictable output differences for which one determines some specific input differences. The strong diffusion required of the S-box is guaranteed by a lower DAP value, so that the transformation process could be relatively hard to trace for the attackers. In quaternion-based S-box design, the scalar S-box is built by modular arithmetic and affine mappings on the real component so as the input changes by a small bit, the output turns out to be very unpredictable. Just

as the vector S box processes the imaginary components, it uses independent transformations like modular exponentiation, rotation-based diffusion, and non-affine permutations and applies those extremely unpredictable differential transitions. The quaternion algebra naturally improves the diffusion properties of S-boxes by distributing transformation in multi-dimensional space in such a way that differences in the input tokens propagate through a very complex and highly nonlinear process. Quaternion-based cryptographic systems independently optimize the scalar as well as vector parts to incorporate minimal DAP values and hence provide superior resistance against differential attacks, making them ideal for use in the encryption algorithms, block ciphers, and secure communication algorithms that need strong confusion and diffusion to guarantee data security [12, 14, 17]. Literature comparison through Tables 12, 13, and 14 is done with the proposed results.

Table 12: DAP of S_s

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

Table 13: DAP of S_v

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

Table 14: DAP Comparison

S-boxes	DAP
S_s	0.047
S_v	0.047
[12]	0.039
[17]	0.047
[14]	0.039

4.6. Fixed Points

A fixed point of a function f is an element x in the domain such that $f(x) = x$. This may provide an exploitable foundation for cryptographic systems, allowing attackers to exploit predictable mappings. In quaternion-based S-Box implementation, where scalar and vector parts are separately processed, certain careful choices of modular transformation and affine mapping result in minimal numbers of fixed-point occurrences. A nonlinear transformation of the scalar S box derived from the real part of quaternion integers is performed to vastly diversify the outputs. Just like the vector S-box dealing with the imaginary components, it applies independent modular exponentiation and rotation-based transformations to break the direct input-to-output relationships that may exist. Eliminating or reducing fixed points by introducing quaternion-based S-boxes, security can be improved in the sense that they are more resistant to algebraic attacks and can be applied elsewhere in encryption schemes and secure communication systems [4, 15]. The fixed point's comparison is given in Table 15.

4.7. Differential and Linear Branch Number

As was stated above, the branch number of an S-box plays a crucial factor in measuring its effectiveness in spreading input differences over the output and thus its efficiency against differential and linear cryptanalysis. Increasing differential branch number (DBN) guarantees a small input difference produces large output differences; thus, differential attacks impose less damage. Likewise, a high linear branch number (LBN) prevents linear approximation attacks by making it difficult for attackers to have a good statistical correlation between input and output values. In quaternion-based S-box design, scalar S-box maximizes these branch numbers in modulo arithmetic and affine transformations, and vector S-box improves it in the same component mapping. Being inherently multidimensional, quaternion integers provide superior confusion and diffusion as compared to usual transformations that would result in even more complex complexity of these transformations inherently, which further enhances the cryptographic security [4, 15]. LBN and DBN comparison is given in Table 15.

4.8. Linear Structure

It is the idea that when linear relations exist between input and output bits, they can be used for the application of linear cryptanalysis against the encryption system. In a well-designed S-box, the substitution process should be highly nonlinear and unpredictable, and there should be a minimum linear structure. Non-affine transformations, modular exponentiation and quaternion rotations on the multidimensional quaternion space are applied to obtain quaternion-based S-boxes where scalar and vector parts are generated separately under quaternion linear transformations without linear dependencies. The scalar S-box is there to ensure the real number transformations make inimitable patterns, and the vector S-box, which concerns the imaginary parts, uses independent transformations to further boost the non-linearity. Quaternions-based S-boxes minimize computational cost

and minimize linear structure, resulting in high resistance to linear cryptanalysis, and are thus ideal for secure encryption protocols, block ciphers and other cryptographic applications needing strong nonlinearity [4, 15]. The linear structure comparison is given in Table 15.

Table 15: Comparative analysis of DBN, LBN, FP, and LS

S-boxes	DBN	LBN	FP	LS
S_s	1	1	1	0
S_v	1	1	1	0
[15]	2	2	2	0
[4]	1	2	2	0

5. Multiple RGB Image Algorithm over Quaternion Integers

(i) **Input Preparation:** First, the RGB images which need to be protected are imported, and the encryption process starts. Images stored in the RGB color model have each pixel consisting of a combination of red, green and blue values. In order to achieve encryption, the pixel values of the image channels are mapped to elements of the quaternion integer set $H(K)_\delta$. Specifically, this mapping ensures that the encryption scheme is conducted in the quaternion domain with the dip advantage of the quaternion algebraic structure to provide enhanced security.

(ii) **S-Box Construction:** Using quaternion integer residue classes $H(K)_\delta$, two 8×8 S-boxes are constructed S_s and S_v. The introduction of nonlinearity and complexity with these structures is important, as they enormously strengthen the encryption. The use of quaternion arithmetic has a unique set of properties that are more resistant to cryptographic breaking attacks than what is provided using integer-based approaches.

(iii) **SPN Framework:** The encryption scheme is developed in the SPN framework, and the security of multiple RGB images is improved by the following three steps: **Substitution Step:** Of the stages, the first is the Substitution Step, where the confusion is introduced using S-box S_s. Then substitute every one of the Red, Green, and Blue channel pixels accordingly by a substitution operation which replaces the input values with the corresponding outputs from S_s. Thus, quaternion-integer-based S-boxes allow high nonlinearity, rendering it much more difficult to carry out a study, particularly on linear and differential attacks. **Permutation Step:** The S-box S_v is used in the second stage to perform a permutation step, which improves the diffusion properties by redistributing transformed pixel values. The reordering of each RGB channel is independent of each other, eliminating substitution-induced correlations for a reduced chance for pattern detection from attackers. This process is enhanced by adding the quaternion integer domain, which increases the number

structure to a more complex number and disrupts statistical relations further. **Final XOR Operation:** The generation of S'-box depends on performing an XOR operation between S_s and S_v which marks the final transformation. Security reaches its highest mark in the last step, which introduces additional randomization. The pixel values in digital images experience an XOR operation using rendering; it is impractical for hackers to perform keyless reconstruction of transformations. The decryption process remains possible only through the precise encryption key that was originally used in the process.

(iv) **Final Transformation:** Every RGB channel receives a transformation through the SPN process which optimizes confusion and diffusion across the complete image. The purpose of this security-enhancing step is to protect against both differential and statistical attacks, thus creating an encrypted image with strong resistance against unauthorized decryption attempts.

(v) **Output the Encrypted Image:**: The implementation of all encryption methods produces an encrypted RGB image which results from merging the modified red, green and blue color channels. The encryption algorithm runs for all RGB images contained in the dataset to deliver complete information security.

(vi) **Security Enhancement and Final Output:** A cryptographic process results in encrypted images that present high levels of randomness through increased entropy along with low pixel correlation alongside intense resilience to cryptographic analysis. Through quaternion integer-based encryption the framework delivers secure multimedia transmission since encrypted images become significantly unpredictable to both modern cryptanalysis methods and traditional cryptanalytic attacks.

Significance of RGB Multiple Color Image Encryption: Secure multimedia data transmission benefits substantially from the use of quaternion integers to encrypt multiple RGB images. Modern cryptographic attacks frequently break traditional encryption methods based on real and complex numbers because these methods lack enough algebraic complexity. The security benefits from quaternion integer use stem from their elevated dimensional structure along with their non-commutative properties, which cause brute-force attacks, linear approximations and differential cryptanalysis to become increasingly difficult to perform. The main benefit of using quaternion encryption is its channel independence processing capability, which ensures secure image integrity by maintaining dependencies across color channels and providing strong diffusion and confusion capabilities. Quaternion residue classes integrated with substitution-permutation networks (SPN) adopt mathematical methods for distributing pixel data that make them resilient against statistical attacks. Nonlinearities strengthen due to the construction of secure S-boxes based on quaternion integer residue classes because these results help protect against cryptographic weaknesses. Quaternions enable efficient implementation of secure transformations that produce encrypted images with high entropy values and reduced correlation along with strong dependency to keys. The encryption technique delivers exceptional benefits for secure image transfer and cloud backup alongside defence needs because

it maintains highly confidential data while resisting attacks effectively. This encryption framework takes advantage of quaternion integers' distinct algebraic properties to develop a superior encryption system when compared to classic approaches, thus delivering better security and computation speed to actual multimedia encryption operations.
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 2.

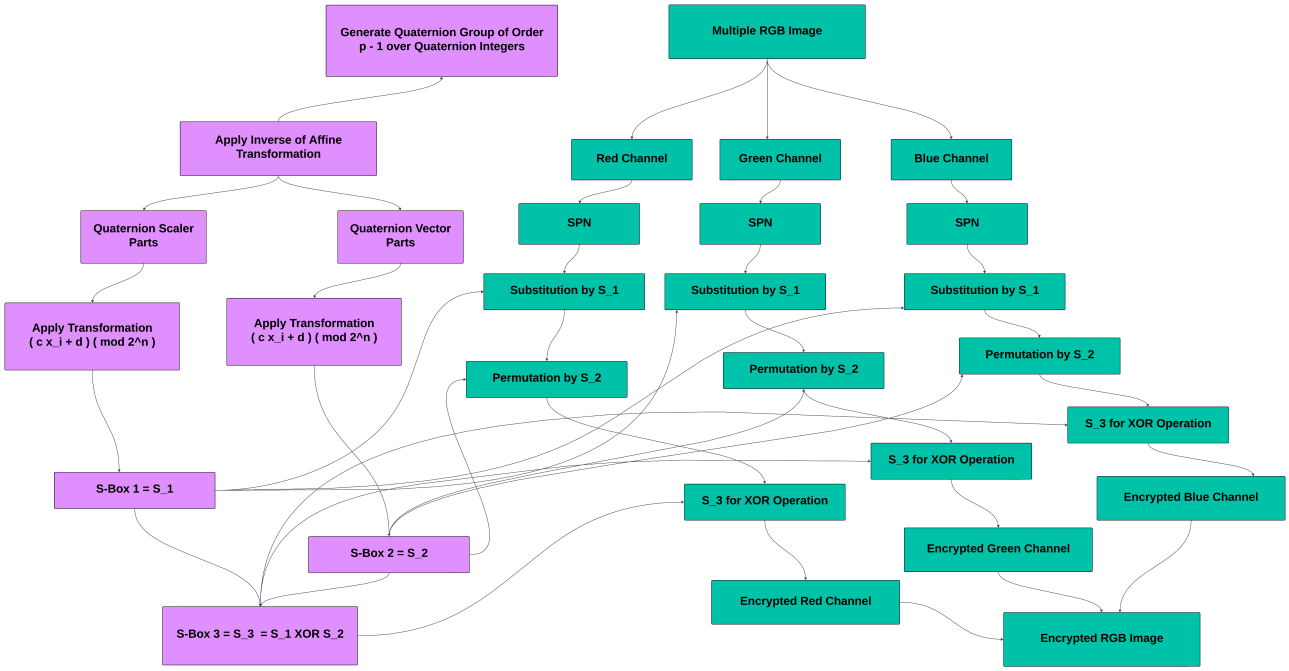

Figure 2: Flowchart of proposed study

6. Applications of Multiple RGB Image Encryption over Quaternion Integers

Multiple RGB image encryption over quaternion integers is a very powerful technique for encrypting the digital images in a secure way by utilizing the multidimensional properties of the quaternions. Quaternions are four-dimensional, and quaternion-based encryption operates over the quaternion system, which means scalar and three imaginary components. The increase in complexity and unpredictability of the encryption process is achieved by means of this higher-dimensional representation which is capable of complex transformation. Using this methodology, each of the RGB images is separated into their color channels, where they are then converted into quaternion space and processed with encryption using substitution-permutation networks (SPN), modular arithmetic and affine transformations, respectively, on the scalar and vector components. This involves strong diffusion and confusion, meaning that even a very modest change of the original image leads to a very different output in the encrypted version. Quaternion multiplication and

rotation functions allow for much more sensitivity of the system to keys, and the system is thus very resistant to brute force and statistical attacks. With this technique, the secure encryption and transmission of multiple RGB images while resisting cryptography attacks can be easily achieved; hence, this is a good technique for secure image communication, cloud saving, and multimedia security applications [5, 16, 21, 34]. Figure 3 shows two original multiple RGB images I_1, and I_2 alongside their encrypted versions.

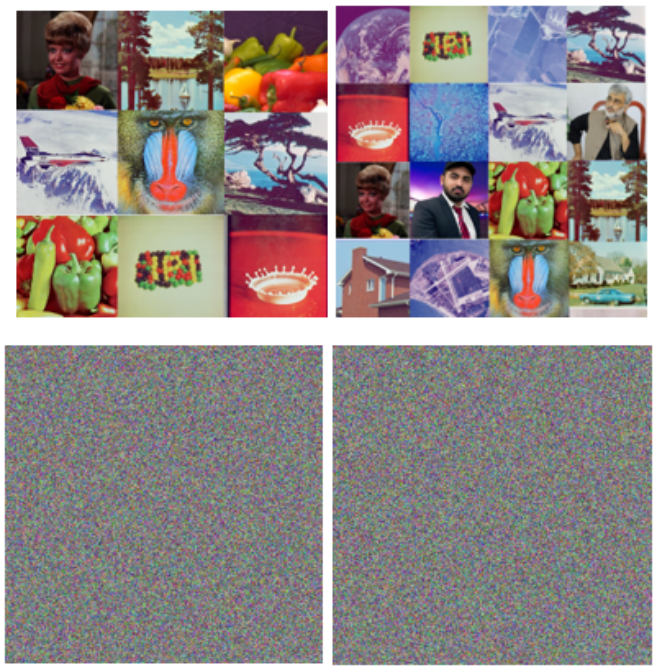

Figure 3: Quaternion integers-based multiple original and encrypted RGB images

6.1. Histogram Analysis (HA)

Histogram analysis is a vital method of checking the security and performance of more than one RBG image encryption utilizing quaternion integers. This analyzes the distribution of pixel intensity values in encrypted images to determine whether the encryption process indeed covers up all the statistical properties of the original images. In a well-encrypted image both the histogram and the power spectrum should look uniform (homogeneously distributed across the entire intensity/density range); this blocks any detectable patterns for attackers to exploit. If we encrypt the RGB images that are in the form of quaternion integers using such an encryption algorithm, the encryption algorithm transforms the scalar and vector components separately based on nonlinear operations such as substitution, permutation, and quaternion multiplication. By placing constraints on individual components of a color plane of an image, this further strengthens the security of the encrypted image such that each color channel undergoes independent transformations that are still correlated. The histograms of the original and encrypted images analyzed show

that the proposed quaternion-based encryption breaks the pixel correlations, hence producing histograms largely similar to signatures of randomness. This randomness greatly limited the likelihood of a statistical attack based on the encrypted image since the attackers cannot learn any meaningful information from the encrypted image. This encryption scheme is proven effective in that the histogram of the encrypted image is entirely devoid of any resemblance to that of the original image and is strong against frequency-based cryptanalysis; hence, the images are kept confidential [5, 16, 21]. Figure 4 is the multiple original and encrypted RGB image histogram analysis.

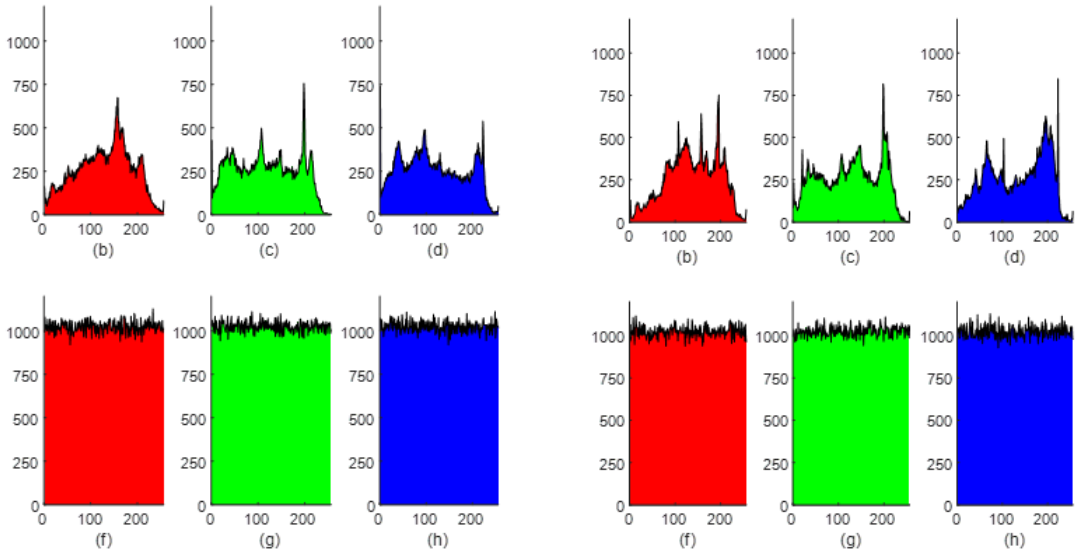

Figure 4: Histogram analysis of original and encrypted images $I_1 \& I_2$

6.2. NPCR

In regards to multiple RGB image encryption over quaternion integers, we have a metric of key interest: the Number of Pixels Change Rate (NPCR), which measures how sensitive an encryption algorithm is to small changes in the plaintext image. The NPCR measures the percentage of pixels that are moved (changed) in the encrypted image to only one changed pixel in the original image. A higher value of NPCR indicates that the encryption process spreads minor changes over the whole encrypted image, so the changes are resistant to attacks and cannot be used to extract details from encrypted images. In quaternion-based encryption, where an RGB image is mapped to quaternion space and processed independently on scalar and vector parts, a small modification to the input causes a large alteration in the encrypted output. Quaternion multiplication, rotation-based transformations, and substitution permutation networks (SPN) are used to guarantee even a very small change in any one pixel will propagate unintelligibly into all three color channels. Therefore, an ideal quaternion-based encryption scheme achieves NPCR near to 99%, indicating that the encryption method gives a high degree of random-

ness and unpredictability, making it very hard to extract meaningful info from encrypted pictures for the assailants [5, 16, 21, 34]. The NPCR results are in Table 16.

6.3. UACI

The Unified Average Changing Intensity (UACI) is another important metric used to assess the use of the image encryption algorithm to measure the average intensity difference between the original and the encrypted images. Higher UACI values quantify the impact of small changes in the plaintext image on the encrypted image, i.e., the stronger the diffusion properties. For the encryption over quaternion integers in multiple RGB images, UACI is used to evaluate how efficiently the encryption spoils the overall pixel intensity distribution in different color channels. As quaternion-based encryption encrypts the scalar and vector components of an image independently and applies modular arithmetic, affine mappings, and quaternion rotations to the transformed form independent of each other, the slight changes in the input will have a large variation in pixel intensity after encryption. Using this enhanced diffusion mechanism, attackers are prevented from building statistical correlations between the encrypted and unencrypted images for security. Typically, an optimal quaternion-based encryption scheme achieves a high UACI value, indicating that the mean of change across the encrypted image is sufficiently high with substantial change in pixel intensity, which is the most important factor in resisting statistical and differential attacks [5, 16, 21, 34]. The UACI results are in Table 16.

Table 16: NPCR and UACI analysis

	NPCR			UACI		
Images	Red	Green	Blue	Red	Green	Blue
Image I_1	0.9962	0.9962	0.9961	0.2999	0.3145	0.3185
Image I_2	0.9960	0.9961	0.9963	0.2956	0.3094	0.3112
[16]	0.9960	0.9961	0.9961	0.3347	0.3347	0.3346
[21]	0.9969	0.9969	0.9966	0.3367	0.3332	0.3367
[34]	0.9961	0.9961	0.9961	0.3544	0.3177	0.3419
[5]	0.9959	0.9964	0.9962	0.3269	0.3037	0.2762

6.4. Maximum Deviation

Maximum deviation analysis is an important statistical measure for the modelling and evaluation of the randomness and effectiveness of the encryption of quaternion integers into multiple RGB images. It quantifies the largest absolute difference between the pixel intensity distributions of the original and encrypted images and gives insight into how well the encryption algorithm disrupts the structural properties of the input data. The larger the maximum deviation value, the better the encryption scheme, as it implies that the encrypted image appears very unpredictable and significantly distinguishes from the original. Maximum deviation analysis is used to validate the diffusion capability

of quaternion-based encryption, and the argument is that where RGB images are transformed by distinct transformations on the scalar and vector parts of quaternion space, maximum deviation analysis validates the algorithm's diffusion capability. By application of quaternion multiplication, affine transformation, and, of course, nonlinear operations, the smallest fluctuation in pixel value is propagated extensively across all the color channels and makes intensity distribution drastically different. Researchers also analyze the maximum deviation between histograms of the original and encryption images to verify that the proposed encryption scheme successfully removes the pattern and is not vulnerable to statistical attacks. The maximum deviation values obtained by quaternion-based encryption signify its robustness to provide secure transmission and storage of many RGB images against crypto threats [5, 34]. Table 17 provides the results obtained from MD testing.

6.5. Irregular Deviation

As an important statistical measuring method, irregular deviation of multiple RGB image encryption over quaternion integers is carried out. This analysis checks whether the histograms of the encrypted images have been regularized to an extent comparable to that of the histogram between the histogram of the original and encrypted images by the encryption algorithm and verifies that such patterns may appear in the previous images. The irregular deviation value is a high value which implies that the encrypted image has some randomness, and thus attacks cannot guess anything about the image due to randomness. In the encryption process of quaternion-based encryption, the RGB images mapped in quaternion space are subjected to independent transformations on scalar and vector components, which disrupts pixel intensity distributions of all color channels. To achieve said variation, quaternion multiplication, nonlinear transformations and permutation substitution operations are used. By inspecting the histograms of the plaintext and ciphertext images with regard to the irregular deviation, it is shown that quaternion encryption has a very high entropy. The encryption scheme thus has an additional level of randomness that prevents statistical attacks to secure transmission and storage of multiple RGB images in cryptographic applications [5, 34]. The results regarding ID are presented in Table 17.

Table 17: MD and ID analysis

	NPCR			UACI		
Images	Red	Green	Blue	Red	Green	Blue
Image I_1 Encrypted	52021	61841	61742	38097	37989	37924
Image I_2 Encrypted	61424	62086	52113	38171	37937	38159
[34]	53397	48329	53529	29231	25127	28374
[5]	60210	47069	62218	26266	19443	27027

6.6. Correlation Analysis

The term evaluation metric includes correlation analysis, horizontal, vertical and diagonal correlation in order to measure the average security of utilizing multiple RGB image encryption with quaternion integers. In an unencrypted image, neighbouring pixels are strongly correlated because natural images are full of neighbouring pixels that have similar intensity values. Nevertheless, any good encryption scheme should significantly decrease these correlations so as to render the encrypted image look like nothing but a random noise. Through quaternion-based encryption techniques, RG images are converted to quaternion space, and encryption is done independently on scalar and vector components. To ensure that neighbouring pixels in horizontal, vertical, and diagonal directions all receive individual and impossible-to-predict transformations, the process of encryption involves non-linear transformations, quaternion multiplication, and substitution permutation network (SPN). Thus, although the neighbouring pixels of the encrypted image still show some correlation coefficients, they are approaching values close to zero, which means that there is no more statistical relationship between the adjacent pixels. Such reduction in correlation ensures that the encrypted image does not betray any structural information from the original image, so it is very immune to statistical attacks. Then it is found that quaternion-based encryption can significantly enhance security and thus is an effective way for secure image transmission and storage by comparing the horizontal, vertical and diagonal correlations before and after encryption [5, 16, 21, 34]. The correlation analysis is given in Figure 5 and 6 with Table 18 data.

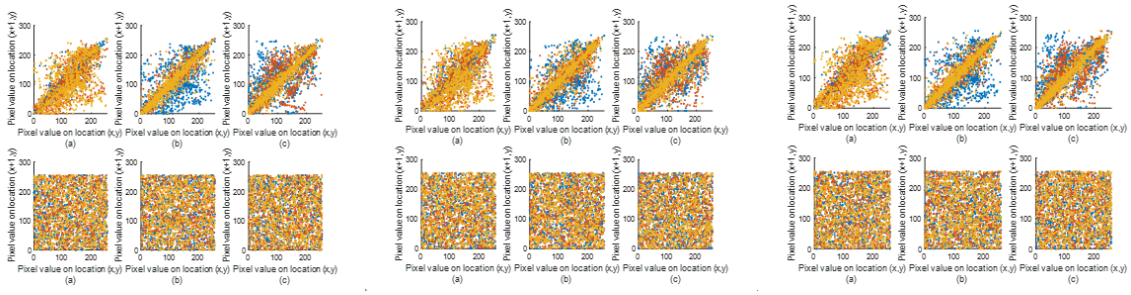

Figure 5: Vertical, diagonal and horizontal correlation analysis of image I_1

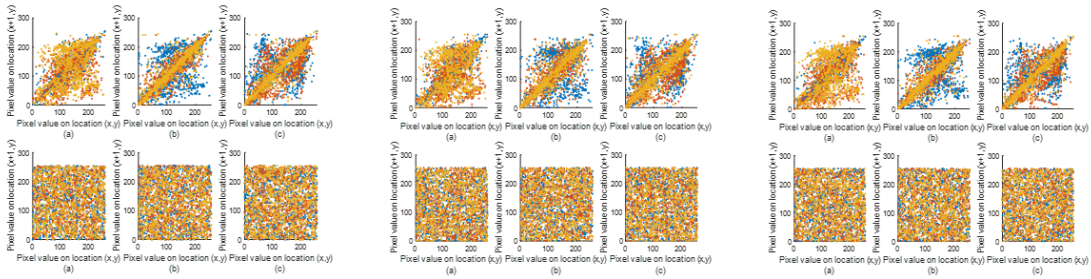

Figure 6: Vertical, diagonal and horizontal correlation analysis of image I_2

Table 18: Vertical, diagonal and horizontal correlation analysis of different images

Images		Vertical			Diagonal			Horizontal		
	Red	Green	Blue	Red	Green	Blue	Red	Green	Blue	
Image I_1 Original	Red	0.9340	0.7323	0.5096	0.9038	0.6895	0.5161	0.9235	0.7030	0.5486
	Green	0.5420	0.9474	0.9431	0.5494	0.9068	0.9054	0.5506	0.9410	0.9388
	Blue	0.5423	0.7284	0.9462	0.5679	0.7200	0.8945	0.5530	0.7589	0.9408
Image I_1 Encrypted	Red	-0.0400	0.0067	-0.0234	-0.0026	0.0017	0.0312	0.0284	0.0115	0.0365
	Green	0.0462	-0.0158	0.0145	-0.0186	0.0074	-0.0144	0.0040	-0.0168	0.0035
	Blue	0.0306	0.0039	-0.0308	-0.0472	-0.0077	0.0103	-0.0190	0.0102	0.0321
Image I_2 Original	Red	0.8956	0.6007	0.3919	0.8669	0.5082	0.3964	0.9201	0.6211	0.3671
	Green	0.3843	0.9275	0.9250	0.3603	0.8285	0.9071	0.3508	0.9142	0.9258
	Blue	0.3805	0.7224	0.9174	0.3655	0.7086	0.8968	0.3911	0.7223	0.9323
Image I_2 Encrypted	Red	-0.0027	-0.0324	0.0205	-0.0136	0.0149	0.0055	0.0033	-0.0675	-0.0665
	Green	0.0164	-0.0081	-0.0133	-0.0217	-0.0512	0.0539	-0.0260	0.0179	0.0124
	Blue	0.0425	-0.0180	0.0351	0.0162	-0.0239	0.0115	0.0013	-0.0432	-0.0107

6.7. Information Entropy

It is an important figure of speech for multiple RGB image encryption over quaternion integers and randomness and security. It is the measure of uncertainty of the encrypted image; in an ideal encryption scheme, the entropy value for such an image with 8 bits of greyscale or color should be close to 8, thus indicating a uniform distribution of pixel intensities. In quaternion-based encryption, RGB images are mapped to quaternion space, followed by the independent transformation of scalar and vector components of each image according to substitution, permutation, quaternion multiplication and modular arithmetic. Therefore, these processes make the pixel intensity values of the encrypted image distributed as randomly as possible, without having any inherent patterns of the original image. A large entropy value indicates that the image content is well obfuscated by the encryption method, and he or she is highly resistant to statistical attack, information leakage and cryptanalysis. The entropy of the image if considerably lower than 8 implies that the image carries redundant information which could be used by the attackers to deduce the original image. The quaternion-based encryption achieves entropy values close to the theoretical maximum, thereby securing the encrypted multiple RGB images by creating the maximum randomness for transmission and storage in cryptographic applications [5, 16, 35]. A comparison of the proposed work's entropy evaluation is made to the existing research noted in Table 19.

Table 19: Information Entropy comparison

Images	Information Entropy			Average
	Red	Green	Blue	
Image I_1	7.9992	7.9994	7.9993	7.9993
Image I_2	7.9993	7.9994	7.9992	7.9993
[16]	7.9913	7.9914	7.9916	7.9916
[35]	7.9888	7.9896	7.9890	7.9892
[21]	7.9995	7.9995	7.9994	7.9995
[5]	7.9976	7.9967	7.9976	7.9987

6.8. MSE

Mean Squared Error (MSE) is employed to compare the original encrypted images in multiple RGB image encryption over quaternion integers. The MSE quantifies the average squared differences between the corresponding pixel intensities, and the higher values of MSE mean that stronger encryption is achieved through ensuring a significant deviation from the original image. In a quaternion-based encryption, i.e., transforming images to quaternion space to allow scalar and vector components of each pixel to be independently processed by substitution, permutation, and quaternion multiplication operations, in the quaternion-based encryption process, the pixel intensity variation is maximized. For a well-designed encryption scheme, the MSE measures should be high such that the encrypted image has no similarity to the original one, which makes the image resistant to visual attacks as well as statistical analysis. On the one hand, quaternion-based encryption with large MSE values both guarantees good diffusion and confusion so as to avoid attackers obtaining any meaningful pattern or reconstructing the original image [34]. The data collected MSE are given in Table 20.

6.9. PSNR

The Peak Signal to Noise Ratio (PSNR) is an important metric to evaluate the quality degradation between the original encrypted images in many RGB image encryptions over quaternion integers. PSNR inversely relates to MSE, and a lower PSNR means the encryption has better performance, meaning that the encrypted image is much distorted and can't be recognized from the original. Since quaternion-based encryption is an independent transformation of the scalar and vector components of an image using nonlinear and algebraic operations, it increases pixel randomness and hence reduces the PSNR value significantly. The lower PSNR indicates that the encrypted image went through extreme modifications, and those kinds of modifications would be beyond the capability for attackers to decode the original image by means of standard signal processing. PSNR values are found to be low, also indicating that the encryption is effective in validating the encryption's robustness and the resistance to inverse attacks [34]. Table 20 contains the collected PSNR and MSE data.

Table 20: MSE and PSNR analysis

	MSE			PSNR		
Images	Red	Green	Blue	Red	Green	Blue
Image I_1 Original	2.50	2.33	2.53	44.1849	44.4965	44.1297
Image I_1 Encrypted	2.54	2.48	2.38	44.1080	44.2180	44.3952
Image I_2 Original	2.53	2.62	2.48	44.1320	43.9747	44.2144
Image I_2 Encrypted	2.44	2.53	2.36	44.2969	44.1377	44.4353
Original Image [34]	2.23	2.47	2.10	44.6746	44.2313	44.9505
Encrypted Image [34]	2.43	2.42	2.38	44.3020	44.3185	44.4057

6.10. Contrast

The parameter of multiple RGB image encryption over quaternion integers is contrast analysis, which is the difference of intensity between two adjacent pixels. To prevent the encrypted image from displaying any identifiable features of the plaintext image, the original contrast levels of the plaintext image should be disrupted by encrypting them in a secure encryption algorithm. Quaternion encryption provides an additional source of randomness and distorts the contrast distribution by mapping RGB images to quaternion space and performing independent transformations of the scalar and vector components. Encryption with strong encryption is indicated by high intensity currents in the encrypted image by eliminating the structural consistency and the sensitivity to statistical attacks. The encrypted images should have their contrast values that do not correlate with those of the original images to ensure secure image transmission and storage as well [21, 34]. Table 21 presents the result of contrast evaluation in the proposed work.

6.11. Energy

Energy is a texture analysis measure to determine if pixel intensity distribution in the image is one of repetitive pattern (with a high value) or random (with a low value). The purpose of multiple RGB image encryption over quaternion integers is to obtain an energy value of a disordered and unpredictable pixel distribution. The quaternion based encryption is built upon substitution permutation networks (SPN), quaternion multiplication and nonlinear transformation mechanisms to disrupt original energy distribution such that encrypted image is with a uniform and random texture. The encryption process is effective if there is a significant deviation in energy values between the original and encrypted images and therefore no recognizable patterns can be exploited by the attackers. By thoroughly encrypting an image, its energy value to its plaintext counterpart should be drastically different, as a confirmation that encryption can perform visual data obfuscation [21, 34]. The presented energy data is shown in Table 21.

Table 21: Contrast and energy analysis

	Contrast			Energy		
Images	Red	Green	Blue	Red	Green	Blue
Image I_1 Original	0.5693	0.6411	0.6196	0.0752	0.0735	0.0713
Image I_1 Encrypted	10.5357	10.4913	10.4710	0.0156	0.0156	0.0156
Image I_2 Original	0.6062	0.7930	0.6063	0.0828	0.0748	0.0906
Image I_2 Encrypted	10.4667	10.5053	10.5311	0.0156	0.0156	0.0156
Original Image [21]	0.5439	0.5000	0.4726	0.5439	0.5000	0.4726
Encrypted Image [21]	10.5114	10.4770	10.4894	10.5114	10.4770	10.4894
Original Image [34]	0.4717	0.4879	0.4261	0.0838	0.0834	0.1242
Encrypted Image [34]	10.4878	10.4861	10.5034	0.0156	0.0156	0.0156

6.12. Statistical Homogeneity

Statistical homogeneity relates to the uniformity of a gray image's texture and is determined based on successive pixel intensities. For the scheme of multiple RGB image encryption over quaternion integers, it needs to break pixel similarity so that the encrypted image will be more homogenous. Quaternion based encryption does this by separately transforming the scalar and vector part of each pixel by modular arithmetic, affine transformation, and quaternion rotation. These transformations also bring randomness thus neighboring pixels of encrypted image not related in any steady way. A lower homogeneity value in the encrypted image means the encryption algorithm adversely disturbs the structural consistency of the image rendering it very indomitable to statistical as well as differential attacks. The security of quaternion based encryption is enhanced because it reduces homogeneity and the encrypted image cannot be meaningfully extracted by the attacker [34]. The results of the proposed work for homogeneity are presented in Table 22.

6.13. Standard Deviation

The SD is a necessary statistical index for the evaluation of dispersion of pixel intensities in multiple RGB image encryption over quaternion integers. The greater the value of an encrypted image's SD, the broader the spread of pixel intensities, since this indicates a strong encryption process that has removed all patterns and correlations present in the original image. Quaternion based encryption uses separate scalar and vector components upon which they interleave nonlinear transforms, quaternion multiplication and permutation-substitution networks in order to distribute pixel values uniformly across color channels. This dispersion is required for achieving a very high randomness in the encrypted image so it can be resistant to statistical attacks. If the chosen encryption process is secure, we should observe a greatly different SD between the original and the encrypted images, which ensures that the encryption has successfully masked the structural consistency. Through a high SD, quaternion based encryption not only increases security for multiple RGB images, but prevents these images from being decrypted or pattern recognized by any unauthorized user [34]. Table 22 shows a description of the SD test results of the proposed work.

Table 22: Homogeneity and standard deviation

	Homogeneity			Standard Deviation		
Images	Red	Green	Blue	Red	Green	Blue
Image I_1 Original	0.8335	0.8324	0.8293	57.4332	64.5652	65.8041
Image I_1 Encrypted	0.3891	0.3892	0.3899	73.8951	73.9193	73.9622
Image I_2 Original	0.8384	0.8198	0.8499	54.7737	63.0304	63.5231
Image I_2 Encrypted	0.3801	0.3897	0.3897	73.9140	73.8647	73.9488
Original Image [34]	0.8855	0.8726	0.8855	9.5315×10^3	8.5820×10^3	1.0732×10^4
Encrypted Image [34]	0.3892	0.3897	0.3889	72.3821	67.0023	61.9652

6.14. NIST Test

Randomness of quaternion integer multiple RGB image encryption: The NIST statistical test suite is a standard method for testing random and security strength of the encryption scheme, especially for the multiple RGB image encryption over integers. This suite exercises several tests of various aspects of randomness to check that the encrypted images have highly unpredictable pixel distributions. Frequency test is used to determine that whether the amount of ones and zeros in the encrypted image is the same and therefore the randomness is uniform. However, the block frequency test expands this idea by analyzing certain blocks in the encrypted image, ensuring that there is randomness maintained between segments of the encrypted image. The rank test ensures that the encryption breaks down structured relationships of values in the image, and the linear dependence is examined between pixel values. The runs test (M=10,000) and long runs of Ones test check for the consistency of sequences of like pixel values, and there is no residual of predictable pattern. Repeated patterns are analyzed in the overlapping templates and non-overlapping templates tests, which verify that quaternion based encryption would result in a large variability over the image. The spectral DFT tests evaluate the encrypted data on periodic structures, which prevents the frequency based attacks since it should not contain the dominating spectrum. The complexity of pixel arrangements is estimated by the approximate entropy test and thus verifies that the encrypted image has an irregular unpredictable structure. The universal test is a test if the encrypted image has compressible patterns with high randomness, and thus is resistant to redundancy-based attacks. The serial tests determine the independence of pixel transitions, that pixels are not next to each other and follow any pattern. The cumulative sum tests (forward and reverse) include tests that verify the uniformity of pixel distribution across the encrypted image without any directional biases. Random excursions and random excursions variants tests evaluate the randomness of the trajectory of pixel value sequence to ensure that quaternion based encryption successfully destroys patterns and continues to be unpredictable. Multiple methods of RGB image encryption over quaternion integers then pass these NIST tests and show robustness to securing image data, resisting statistical, differential and frequency based cryptanalysis techniques [34, 36]. NIST evaluates its results through Table 23.

Table 23: NIST analysis of encrypted image I_1

Tests		P-values			Remarks
		Red	Green	Blue	
Frequency		0.72795	0.52709	0.84952	✓
Block frequency		0.8214	0.94307	0.64453	✓
Rank		0.29191	0.29191	0.29191	✓
Runs (M=10,000)		0.29579	0.52292	0.020941	✓
Long runs of ones		0.7127	0.7127	0.7127	✓
Overlapping templates		0.85988	0.85988	0.81567	✓
No overlapping templates		1	0.9994	0.99981	✓
Spectral DFT		0.14679	0.77167	0.11048	✓
Approximate entropy		0.90625	0.35541	0.5992	✓
Universal		0.99668	0.98733	0.99844	✓
Serial	p values 1	0.55822	0.020917	0.030786	✓
Serial	p values 2	0.64206	0.0036093	0.92887	✓
Cumulative sums forward		0.224	0.24591	0.24146	✓
Cumulative sums reverse		0.96051	0.88005	1.0587	✓
Random excursions	X = -4	0.15244	0.30689	0.13725	✓
	X = -3	0.23199	0.46172	0.21775	✓
	X = -2	0.10689	0.25688	0.0091833	✓
	X = -1	0.83873	0.71524	0.83249	✓
	X = 1	0.82206	0.62668	0.63515	✓
	X = 2	0.052698	0.0055571	0.3526	✓
	X = 3	0.60677	0.28872	0.26048	✓
	X = 4	0.12628	0.2527	0.58195	✓
Random excursions variants	X = -5	0.7473	0.89286	0.98091	✓
	X = -4	0.89103	0.93913	0.82814	✓
	X = -3	0.95691	0.92801	0.46022	✓
	X = -2	0.91666	0.81554	0.40709	✓
	X = -1	0.67238	0.2665	0.61527	✓
	X = 1	0.46848	0.68617	0.61527	✓
	X = 2	0.23567	0.86111	0.90103	✓
	X = 3	0.19469	0.75183	0.74815	✓
	X = 4	0.22621	0.76003	0.37052	✓
	X = 5	0.28584	0.89286	0.48767	✓

7. Discussion, Conclusion, and Future Work

This paper proposes a novel encryption scheme for different ways of combining multiple RGB images which are secured by Substitution-Permutation Network (SPN)-based encryption scheme for quaternion integers. Using the mathematical properties of the quaternions integers, specifically their four dimension, the proposed method increases the

cryptographic strength of S-boxes, consequently improving nonlinearity, confusion, and diffusion properties. Using quaternion integer based S boxes in conjunction with an SPN based encryption scheme gives high security level, protected from attack by statistical, differential and cryptanalytic attacks. Furthermore, the proposed algorithm is computationally efficient, which allows for real time applications in domains where secure multimedia transmission in cloud storage, medical imaging, and such are progressing. The presented encryption framework is tested through extensive theoretical and experimental analysis and is proved to be resilient and practical compared to the conventional methods. Computational complexity in the future research can be optimized, other cryptographic primitives can be extended by the approach, and the applicability in resource constrained environment can be further explored for enhancing the digital security in modern multimedia applications.

The optimization of computational complexity of quaternion integer based encryption schemes for real time application can be one future research. These larger and more complex algebraic structures offer further security benefits including exploration of octonion or sedenion integers. It is possible to broaden the applicability of the proposed framework to other cryptographic primitives such as hash functions and digital signatures. Working together with the latest technologies like quantum cryptography and lightweight cryptographic protocols for IoT and edge computing, the process of encryption may be integrated and this would serve as a lot of help in having a good digital security in different uses.

Acknowledgements

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

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.

References

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

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

[3] Majid Khan, Tariq Shah, Hasan Mahmood, Muhammad Asif Gondal, and Iqtadar Hussain. A novel technique for the construction of strong s-boxes based on chaotic lorenz systems. *Nonlinear Dynamics*, 70:2303–2311, 2012.

[4] Naveed Ahmed Azam, Umar Hayat, and Maria Ayub. A substitution box generator, its analysis, and applications in image encryption. *Signal Processing*, 187:108144, 2021.

[5] Muhammad Sajjad, Tariq Shah, Tanveer ul Haq, Bander Almutairi, and Qin Xin. Spn based rgb image encryption over gaussian integers. *Heliyon*, 10(9), 2024.

[6] Giuliana P Davidoff, Peter Sarnak, and Alain Valette. *Elementary number theory, group theory, and Ramanujan graphs*, volume 55. Cambridge university press Cambridge, 2003.

[7] Muhammad Sajjad and Tariq Shah. Decoding of cyclic codes over quaternion integers by modified berlekamp–massey algorithm. *Computational and Applied Mathematics*, 43(2):102, 2024.

[8] Tariq Shah and Summera Said Rasool. On codes over quaternion integers. *Applicable Algebra in Engineering, Communication and Computing*, 24(6):477–496, 2013.

[9] Mehmet Ozen and Murat Guzeltepe. Codes over quaternion integers. *European Journal of Pure and Applied Mathematics*, 3(4):670–677, 2010.

[10] Mehmet Özen and Murat Güzeltepe. Cyclic codes over some finite quaternion integer rings. *Journal of the Franklin Institute*, 348(7):1312–1317, 2011.

[11] Muhammad Sajjad, Tariq Shah, Mohammad Mazyad Hazzazi, Adel R Alharbi, and Iqtadar Hussain. Quaternion integers based higher length cyclic codes and their decoding algorithm. *Computers, Materials & Continua*, 73(1), 2022.

[12] MohammadMazyad Hazzazi, Muhammad Sajjad, Zaid Bassfar, Tariq Shah, and Ashwag Albakri. Nonlinear components of a block cipher over eisenstein integers. *Computers, Materials & Continua*, 77(3), 2023.

[13] Muhammad Sajjad, Tariq Shah, and Robinson Julian Serna. Designing pair of nonlinear components of a block cipher over gaussian integers. *Computers, Materials & Continua*, 75(3), 2023.

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

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

[16] Ahmed A Abd EL-Latif, Bassem Abd-El-Atty, and Salvador 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.

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

[18] Zeba Shamsi and Dolendro Singh Laiphrakpam. Securing encrypted image information in audio data. *Multimedia Tools and Applications*, 82(21):33063–33085, 2023.

[19] Xingyuan Wang, Le Feng, and Hongyu Zhao. Fast image encryption algorithm based on parallel computing system. *Information sciences*, 486:340–358, 2019.

[20] Guangfeng Cheng, Chunhua Wang, and Hua 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.

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

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

[23] Xing-Yuan Wang, Ying-Qian Zhang, and Xue-Mei Bao. A novel chaotic image encryption scheme using dna sequence operations. *Optics and Lasers in Engineering*, 73:53–61, 2015.

[24] SiCheng Wang, ChunHua Wang, and Cong 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.

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

[26] Xing-Yuan Wang and Zhi-Ming Li. A color image encryption algorithm based on hopfield chaotic neural network. *Optics and Lasers in Engineering*, 115:107–118, 2019.

[27] Xingyuan Wang and Suo Gao. Image encryption algorithm for synchronously updating boolean networks based on matrix semi-tensor product theory. *Information sciences*, 507:16–36, 2020.

[28] Wei Liu, Zhenwei Xie, Zhengjun Liu, Yan Zhang, and Shutian Liu. Multiple-image encryption based on optical asymmetric key cryptosystem. *Optics Communications*, 335:205–211, 2015.

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

[30] Pingke Deng, Ming Diao, Mingguang Shan, Zhi Zhong, and Yabin Zhang. Multiple-image encryption using spectral cropping and spatial multiplexing. *Optics Communications*, 359:234–239, 2016.

[31] Chun-Lai Li, Hong-Min Li, Fu-Dong Li, Du-Qu Wei, Xuan-Bing Yang, and Jing Zhang. Multiple-image encryption by using robust chaotic map in wavelet transform domain. *Optik*, 171:277–286, 2018.

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

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

[34] Muhammad Sajjad, Tariq Shah, Rafik Hamza, Bander Almutairi, and Robinson Julian Serna. Multiple color images security by spn over the residue classes of gaussian integer. *Scientific Reports*, 15(1):6425, 2025.

[35] Hongjun Liu, Jian Liu, and Chao Ma. Constructing dynamic strong s-box using 3d chaotic map and application to image encryption. *Multimedia Tools and Applications*, 82(16):23899–23914, 2023.

[36] Lingfeng Qu, Fan Chen, Shanjun Zhang, and Hongjie He. Cryptanalysis of reversible data hiding in encrypted images by block permutation and co-modulation. *IEEE Transactions on Multimedia*, 24:2924–2937, 2021.