International Journal of Theoretical Physics (2019) 58:2720–2743
https://doi.org/10.1007/s10773-019-04162-z

A Novel Digital Contents Privacy Scheme Based on Kramer's Arbitrary Spin

Majid Khan [1,2] · Hafiz Muhammad Waseem [3]

Received: 30 October 2018 / Accepted: 18 May 2019 / Published online: 3 June 2019

Abstract
The privacy of digital contents plays an important role in digitally advanced era. The transmission of digital information over public networks have extraordinary impact and gradually imperative due to theft and manipulation in contents. In this article, we have suggested a new encryption scheme based on Kramer's arbitrary spinning in order to provide the confidentiality to digital contents. We have implemented our offered scheme on standard digital images and performed the security performance analyses to authentic the robustness against cryptographic attacks.

Keywords Kramer's spin · Arbitrary spin · Privacy

1 Introduction

There are numerous environments in everyday existence, when the secret contents conveyed over apprehensive line of communication. Most of the outmoded cryptosystems are utilized in literature to accomplish the security of confidential information [1]. Digital contents are transferred over communication medium, such as documents, advertisements and law enforcement constituents very extensively and security of information is vibrant issue. Due to thoughtful events of hackers, these contents can easily end up in the hands of unauthorized individuals. They can excerpt or alter the data without knowledge of appropriate receiver [2]. The research is going over the years in information theory and cryptology to offer the protection for digital contents. The vibrant issue in line of communication to shelter the privacy of appropriate users [3–17].

Modern ages of cryptography point out around 1950's, when Claude Shannon produced an article 'A mathematical theory of cryptography' published in the Bell System Technical Journal in 1949 [18]. He was inspired during the World War II,

✉ Majid Khan
mk.cfd1@gmail.com

[1] Department of Applied Mathematics & Statistics, Institute of Space Technology, Islamabad, Pakistan

[2] Cyber and Information Security Lab, Institute of Space Technology, Islam0061bad, Pakistan

[3] Department of Electrical Engineering, Institute of Space Technology, Islamabad, Pakistan

when electromechanical cipher machines used very widely. He then identified the two main goals of cryptography: Confidentiality and Authenticity and wrote an article "A mathematical theory of communication" which highlights one of the most significant aspects of cryptography's importance [19].

Different algorithms proposed in different times and DES of 56-bit long key approved and adopted by US agencies and considered to be secure, but improvements in technology have made it trivial to defeat. Although DES replaced by AES, but the fact is if powerful computers may crack DES in few hours, the area of risk in public key cryptography vulnerable to the future developments. This uncertainty provides potential threat to perfect security required at national and intellectual property level.

Various schemes produced in different ages to secure the communication in public channels. In this article, we developed a novel structure based on 'Kramer's arbitrary spin' to provide security for digital contents.

In the light of quantum mechanics, Kramer's theorem states that the time reversal symmetric system with half integer total spin for every energy eigenstate, there is at least one more eigenstate with the same energy. In simple words, each energy level is at least degenerate double if it has half integer spin. If we operate Hamiltonian operator with time reversal, then the time reversed state also act as an eigenstate with the same energy for every energy eigenstate and this state might be identical to the original state. In half integer spin systems, it reverses all angular momenta and cannot produce the same state as the magnetic quantum number can never be zero. The energy levels for a system with odd numbers of fermions, such as electrons, protons and neutrons, at least degenerate double in the presence purely electric field [20].

This article is organized in 5 sections. The preliminaries of this article including derivations presented in section 2. The proposed cryptosystem and its implementation on standard images followed in section 3. Experimentation and performance analyses for the proposed scheme conveyed in section 4 and section 5 comprises the concluding remarks.

2 Basic Terminologies

This section demonstrates the fundamental concepts of orthogonal codes, Redheffer codes and the derivations of Kramer's arbitrary spin matrices.

2.1 Orthogonal Codes

Orthogonal codes introduced by Jacques Hadamard in 1893 and has a remarkable attention in coding theory. Code word set $H_k$can be constructed in dimension of $2^k \times 2^k$and can also be entitled as Hadamard matrix. k-bit data set from H_{k-1} matrix as follows [21]:

$$H_k = \begin{bmatrix} H_{k-1} & H_{k-1} \\ H_{k-1} & \overline{H_{k-1}} \end{bmatrix} \tag{1}$$

One-bit data set can be encoded by using orthogonal code words of 2 digits each, described by the rows of matrix and the 2-bit data set can be transformed by extending the one-bit set both horizontally and vertically given as follows [21]:

2.2 Bi-Orthogonal Codes

Bi-Orthogonal set of total code words *'M'* can be obtained from orthogonal set of code words *M*/2 by supplementing it with negative of each as follows [21]:

$$B_k = \left[\frac{H_{k-1}}{H_{k-1}}\right]. \tag{2}$$

2.3 Redheffer Matrices

A Redheffer matrix is $n \times n$ square (0,1) matrix with elements $a_{ij} = 1$, if $j = 1$ or $i \mid j$ (i divides j) and 0 otherwise. *For n = 1, 2, ..., k*, the first few matrices are:

$$[1], \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 \end{bmatrix}, \ldots.$$

Determinant of $n \times n$matrix equal to Mertens function $M(n)$ [22]. For $n = 1, 2, 3, \ldots$, first few values for the function are 1, 0, −1, −1, −2, −1, −2, −2, …. Eigenvalues of $n \times n$Redheffer matrix for $n > 1$ equals to $a(n) = n - \lfloor \lg n \rfloor - 1$ [23].

2.4 Kramer's Spin Matrices

Kramer's method gives high degree of naturalness. Let us introduce 2 spinor components u and v, i.e. $\xi = \begin{pmatrix} u \\ v \end{pmatrix}$ is a complex vector by nature [24]. The spinor components in Euclidean space represented as:

$$\begin{pmatrix} U \\ V \end{pmatrix} = \begin{pmatrix} \alpha & \beta \\ -\beta^* & \alpha^* \end{pmatrix} \begin{pmatrix} u \\ v \end{pmatrix}, \tag{3}$$

where $U^* U + V^* V = u^* u + v^* v$, $u = \sqrt{a_1 - i a_2}$, $v = i\sqrt{a_1 + i a_2}$and $\alpha = \cos\theta + i\, k_3 \sin\theta$, $\beta = (k_2 + i\, k_1)\sin\theta$ assign as rotational interpretations in Euclidean space. These are so called Cayley-Klein parameters [25].

By applying Kramer's method on Eq. (3), the result as follows:

$$\begin{pmatrix} UU \\ UV \\ VV \end{pmatrix} = \begin{pmatrix} (\alpha u + \beta v)(\alpha u + \beta v) \\ (\alpha u + \beta v)(-\beta^* u + \alpha^* v) \\ (-\beta^* u + \alpha^* v)(-\beta^* u + \alpha^* v) \end{pmatrix} = \begin{pmatrix} \alpha^2 & 2\alpha\beta & \beta^2 \\ -\alpha\beta^* & \alpha\alpha^* - \beta\beta^* & \beta\alpha^* \\ (\beta^*)^2 & -2\alpha^*\beta^* & (\alpha^*)^2 \end{pmatrix} \begin{pmatrix} uu \\ uv \\ vv \end{pmatrix}. \tag{4}$$

Since in this case, $\alpha_1^2 + \alpha_2^2 + \alpha_3^2 = 0$, which implies

$$\alpha_3 = \pm i\sqrt{(\alpha_1 + i\alpha_2)(\alpha_1 - i\alpha_2)}. \tag{5}$$

From the results of u, v and Eq. (5), we have

$$\alpha_1 = \frac{1}{2}\left(u^2 - v^2\right), \quad \alpha_2 = i\frac{1}{2}\left(u^2 + v^2\right), \quad \alpha_3 = -iuv.$$

2.4.1 Spin S (1)

By using Eq. (4) to develop S (1) as follows:

$$S(1) = \begin{pmatrix} \alpha^2 & \sqrt{2}\alpha\beta & \beta^2 \\ -\sqrt{2}\alpha\beta^* & \alpha\alpha^* - \beta\beta^* & \sqrt{2}\beta\alpha^* \\ \left(\beta^*\right)^2 & -\sqrt{2}\alpha^*\beta^* & \left(\alpha^*\right)^2 \end{pmatrix} \tag{6}$$

Extract the matrices σ from Eq. (6) with respect to the results of α_1, α_2 and α_3. The matrices are given as:

$$\sigma_x = \begin{pmatrix} 0 & +\sqrt{2} & 0 \\ \sqrt{2} & 0 & +\sqrt{2} \\ 0 & \sqrt{2} & 0 \end{pmatrix}, \quad \sigma_y = i\begin{pmatrix} 0 & -\sqrt{2} & 0 \\ \sqrt{2} & 0 & -\sqrt{2} \\ 0 & \sqrt{2} & 0 \end{pmatrix}, \quad \sigma_z = \begin{pmatrix} 2 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & -2 \end{pmatrix}.$$

These 3×3 matrices $\sigma_{i,\,j}$ are manifestly traceless hermitian. They are, unlike the Pauli's matrices, not closed under multiplication, but closed under commutation [24]. The case is unitary and unimodular, $S^{\dagger}(1)\,S(1) = I$ and $\det S(1) = 1$.In Pauli's ½ spin case, $\sigma_x^2 + \sigma_y^2 + \sigma_z^2 = 3I$, while in the above case of Kramer spin $\sigma_x^2 + \sigma_y^2 + \sigma_z^2 = 8I$. From the above results, we can calculate $(2\,l + 1)$ dimension traceless hermitian tuples.

$$S(l) = \left\{\sigma_x(l), \sigma_y(l), \sigma_z(l)\right\}, \text{for } \; l = 3/2, 2, 5/2, \ldots.$$

2.4.2 Spin S (3/2)

By applying Kramer's method for S (3/2) on Eq. (3), the result as follows:

$$\begin{pmatrix} UUU \\ UUV \\ UVV \\ VVV \end{pmatrix} = \begin{pmatrix} \alpha^3 & 3\alpha^2\beta & 3\alpha\beta^2 & \beta^3 \\ -\alpha^2\beta^* & \alpha^2\alpha^* - 2\alpha\beta\beta^* & 2\alpha\alpha^*\beta - \beta^2\beta^* & \alpha^*\beta^2 \\ \alpha\left(\beta^*\right)^2 & -2\alpha\alpha^*\beta^* + \beta\left(\beta^*\right)^2 & \alpha\left(\alpha^*\right)^2 - 2\alpha^*\beta\beta^* & \left(\alpha^*\right)^2\beta \\ -\left(\beta^*\right)^3 & 3\alpha^*\left(\beta^*\right)^2 & -3\left(\alpha^*\right)^2\beta^* & \left(\alpha^*\right)^3 \end{pmatrix} \begin{pmatrix} uuu \\ uuv \\ uvv \\ vvv \end{pmatrix},$$

$$S(3/2) = \begin{pmatrix} \alpha^3 & \sqrt{3}\alpha^2\beta & \sqrt{3}\alpha\beta^2 & \beta^3 \\ -\sqrt{3}\alpha^2\beta^* & \alpha^2\alpha^* - 2\alpha\beta\beta^* & 2\alpha\alpha^*\beta - \beta^2\beta^* & \sqrt{3}\alpha^*\beta^2 \\ \sqrt{3}\alpha\left(\beta^*\right)^2 & -2\alpha\alpha^*\beta^* + \beta\left(\beta^*\right)^2 & \alpha\left(\alpha^*\right)^2 - 2\alpha^*\beta\beta^* & \sqrt{3}\left(\alpha^*\right)^2\beta \\ -\left(\beta^*\right)^3 & \sqrt{3}\alpha^*\left(\beta^*\right)^2 & -\sqrt{3}\left(\alpha^*\right)^2\beta^* & \left(\alpha^*\right)^3 \end{pmatrix}.$$

The case is unitary and unimodular, $S^{\prime}(3/2)\,S(3/2) = I$ and $\det(S(3/2)) = 1$.By using values of α and β, we can transform the matrix S (3/2) as follows [26]:

$$S(3/2) = \begin{pmatrix} \alpha^3 & \sqrt{3}\beta & 0 & 0 \\ -\sqrt{3}\beta^* & \alpha^2\alpha^* & 2\beta & 0 \\ 0 & -2\beta^* & \alpha\left(\alpha^*\right)^2 & \sqrt{3}\beta \\ 0 & 0 & -\sqrt{3}\beta^* & \left(\alpha^*\right)^3 \end{pmatrix} \tag{7}$$

Extract σ_x, σ_y and σ_z from Eq. (7) as follows:

$$\sigma_x = \begin{pmatrix} 0 & +\sqrt{3} & 0 & 0 \\ \sqrt{3} & 0 & +2 & 0 \\ 0 & 2 & 0 & +\sqrt{3} \\ 0 & 0 & \sqrt{3} & 0 \end{pmatrix}, \quad \sigma_y = i\begin{pmatrix} 0 & -\sqrt{3} & 0 & 0 \\ \sqrt{3} & 0 & -2 & 0 \\ 0 & 2 & 0 & -\sqrt{3} \\ 0 & 0 & \sqrt{3} & 0 \end{pmatrix}, \quad \sigma_z = \begin{pmatrix} 3 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -3 \end{pmatrix},$$

where $\sigma_x^2 + \sigma_y^2 + \sigma_z^2 = 15I$..

2.4.3 Spin S (2)

By applying Kramer's method on Eq. (3), S (2) is given as:

$$S(2) = \begin{pmatrix} \alpha^4 & 2\beta & 0 & 0 & 0 \\ -2\beta^* & \alpha^3\alpha^* & \sqrt{6}\beta & 0 & 0 \\ 0 & -\sqrt{6}\beta^* & \alpha^2\left(\alpha^*\right)^2 & \sqrt{6}\beta & 0 \\ 0 & 0 & -\sqrt{6}\beta^* & \alpha\left(\alpha^*\right)^3 & 2\beta \\ 0 & 0 & 0 & -2\beta^* & \left(\alpha^*\right)^4 \end{pmatrix} \tag{8}$$

Extract σ_x, σ_y and σ_z from Eq. (8) as follows: $\sigma_x = \frac{1}{2}\begin{pmatrix} 0 & +2 & 0 & 0 & 0 \\ 2 & 0 & +\sqrt{6} & 0 & 0 \\ 0 & \sqrt{6} & 0 & +\sqrt{6} & 0 \\ 0 & 0 & \sqrt{6} & 0 & +2 \\ 0 & 0 & 0 & -2 & 0 \end{pmatrix}, \sigma_y = i\frac{1}{2}\begin{pmatrix} 0 & -2 & 0 & 0 & 0 \\ 2 & 0 & -\sqrt{6} & 0 & 0 \\ 0 & \sqrt{6} & 0 & -\sqrt{6} & 0 \\ 0 & 0 & \sqrt{6} & 0 & -2 \\ 0 & 0 & 0 & -2 & 0 \end{pmatrix}, \sigma_z = \begin{pmatrix} 2 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 0 & -2 \end{pmatrix}$, where $\sigma_x^2 + \sigma_y^2 + \sigma_z^2 = 6I$.

2.4.4 Spin S (5/2)

By applying Kramer's method on Eq. (3) and extraction of σ_x, σ_y and σ_z from S (5/2) as follows:

$$\sigma_x = \frac{1}{2}\begin{pmatrix} 0 & +\sqrt{5} & 0 & 0 & 0 & 0 \\ \sqrt{5} & 0 & +\sqrt{8} & 0 & 0 & 0 \\ 0 & \sqrt{8} & 0 & +\sqrt{9} & 0 & 0 \\ 0 & 0 & \sqrt{9} & 0 & +\sqrt{8} & 0 \\ 0 & 0 & 0 & \sqrt{8} & 0 & +\sqrt{5} \\ 0 & 0 & 0 & 0 & \sqrt{5} & 0 \end{pmatrix}, \sigma_y = i\frac{1}{2}\begin{pmatrix} 0 & -\sqrt{5} & 0 & 0 & 0 & 0 \\ \sqrt{5} & 0 & -\sqrt{8} & 0 & 0 & 0 \\ 0 & \sqrt{8} & 0 & -\sqrt{9} & 0 & 0 \\ 0 & 0 & \sqrt{9} & 0 & -\sqrt{8} & 0 \\ 0 & 0 & 0 & \sqrt{8} & 0 & -\sqrt{5} \\ 0 & 0 & 0 & 0 & \sqrt{5} & 0 \end{pmatrix}, \quad \sigma_z = \begin{pmatrix} \frac{5}{2} & 0 & 0 & 0 & 0 & 0 \\ 0 & \frac{3}{2} & 0 & 0 & 0 & 0 \\ 0 & 0 & \frac{1}{2} & 0 & 0 & 0 \\ 0 & 0 & 0 & -\frac{1}{2} & 0 & 0 \\ 0 & 0 & 0 & 0 & -\frac{3}{2} & 0 \\ 0 & 0 & 0 & 0 & 0 & -\frac{5}{2} \end{pmatrix},$$

where $\sigma_x^2 + \sigma_y^2 + \sigma_z^2 = \frac{35}{4}I$..

3 Proposed Algorithm

We develop arbitrary spin matrices by using Kramer's transformation. In this section, we transformed these matrices to encrypt the data as well as key with the help of Hadamard and Redheffer matrices. Orthogonal or biorthogonal and Redheffer codes use to encrypt the key with respect to key length. Hadamard codes are singular, convert it into nonsingular by taking compliment before encryption. Redheffer matrix of order 2×2 and spin (1, 2, 3, ..., n, where $n \in \mathbb{N}$)matrices cannot be used because of following the singular property, while spin (1/2, 3/2, 5/2, ..., n/2), where n is odd number are nonsingular matrices and can be used to encrypt the data.

3.1 Spin S (1/2)

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = a, \quad \sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = b, \; i\sigma_y = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = c, \quad \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = d.$$

3.2 Spin S (3/2)

$$I = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} = a, \quad \sigma_x = \begin{pmatrix} 0 & +\sqrt{3} & 0 & 0 \\ \sqrt{3} & 0 & +2 & 0 \\ 0 & 2 & 0 & +\sqrt{3} \\ 0 & 0 & \sqrt{3} & 0 \end{pmatrix} = b, \; i\sigma_y = \begin{pmatrix} 0 & -\sqrt{3} & 0 & 0 \\ \sqrt{3} & 0 & -2 & 0 \\ 0 & 2 & 0 & -\sqrt{3} \\ 0 & 0 & \sqrt{3} & 0 \end{pmatrix} = c, \quad \sigma_z = \begin{pmatrix} 3 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -3 \end{pmatrix} = d.$$

3.3 Spin S (5/2)

$$I = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix} = a, \quad \sigma_x = \frac{1}{2}\begin{pmatrix} 0 & +\sqrt{5} & 0 & 0 & 0 & 0 \\ \sqrt{5} & 0 & +\sqrt{8} & 0 & 0 & 0 \\ 0 & \sqrt{8} & 0 & +\sqrt{9} & 0 & 0 \\ 0 & 0 & \sqrt{9} & 0 & +\sqrt{8} & 0 \\ 0 & 0 & 0 & \sqrt{8} & 0 & +\sqrt{5} \\ 0 & 0 & 0 & 0 & \sqrt{5} & 0 \end{pmatrix} = b,$$

$$i\sigma_y = \frac{1}{2}\begin{pmatrix} 0 & -\sqrt{5} & 0 & 0 & 0 & 0 \\ \sqrt{5} & 0 & -\sqrt{8} & 0 & 0 & 0 \\ 0 & \sqrt{8} & 0 & -\sqrt{9} & 0 & 0 \\ 0 & 0 & \sqrt{9} & 0 & -\sqrt{8} & 0 \\ 0 & 0 & 0 & \sqrt{8} & 0 & -\sqrt{5} \\ 0 & 0 & 0 & 0 & \sqrt{5} & 0 \end{pmatrix} = c, \quad \sigma_z = \begin{pmatrix} \frac{5}{2} & 0 & 0 & 0 & 0 & 0 \\ 0 & \frac{3}{2} & 0 & 0 & 0 & 0 \\ 0 & 0 & \frac{1}{2} & 0 & 0 & 0 \\ 0 & 0 & 0 & -\frac{1}{2} & 0 & 0 \\ 0 & 0 & 0 & 0 & -\frac{3}{2} & 0 \\ 0 & 0 & 0 & 0 & 0 & -\frac{5}{2} \end{pmatrix} = d.$$

Let entangle these $n \times n$ matrices to form a set *'A'* of $2n \times 2n$ matrices [1].

$$A = [A_1, A_2, A_3, ..., A_{24}], \textit{where } A_1 = \begin{bmatrix} a & b \\ c & d \end{bmatrix}, A_2 = \begin{bmatrix} a & b \\ d & c \end{bmatrix}, ..., A_{23} = \begin{bmatrix} d & b \\ c & a \end{bmatrix}, A_{24} = \begin{bmatrix} d & b \\ a & c \end{bmatrix}.$$

3.4 Experimentation of Proposed Scheme

We have performed experimentation with key [00110 10,100] on standard images of size 512×512. The entangled matrices with respect to key are A_6 and A_{14} and performed experiment on spin systems S (3/2) and S (5/2) respectively.

4 Performance Analyses for Anticipated Structure

Different standard performance analyses accomplished in this section on standard digital contents to assert the performance and security of anticipated algorithm (see Figs. 1, 2 and 3). These outcomes contain the factual investigation, sensibility examination and loophole test for encrypted data. Different analyses discussed in subsection of 4 in detail to examine the sensitivity of offered encryption mechanism.

4.1 Randomness Analyses

With a specific end goal to justify the prerequisites of long period, uniform scattering, high complexity and efficiency for proposed cryptosystem, we execute NIST SP 800–22 analysis to testify the randomness of digital contents [27]. The enciphered Lena image at S (5/2) is employed to accomplish the NIST tests and the aftereffects results presented in Tables 1, 2 and 3.

By analyzing the outcomes, the anticipated encryption scheme effectively passes all the NIST tests. The production of random ciphers using projected scheme are irregular in the light of accomplished outcomes.

4.2 Uniformity Analyses

Histograms uniformity of enciphered images estimates the security of encryption framework [28]. We have computed the histograms of 256 dark level original and encrypted images of size 512×512, that have different contents. The plain image histograms contain sharp upsurges took after sharp decline, while both enciphered images contain uniformity shown in Figs. 4, 5, 6, 7, 8 and 9, which makes statistical attacks tough.

4.3 Pixels' Correlation Analyses

The neighboring pixels of an image are tremendously associated in horizontal, vertical and diagonal directions. The encrypted data must unrestraint this affiliation to improve

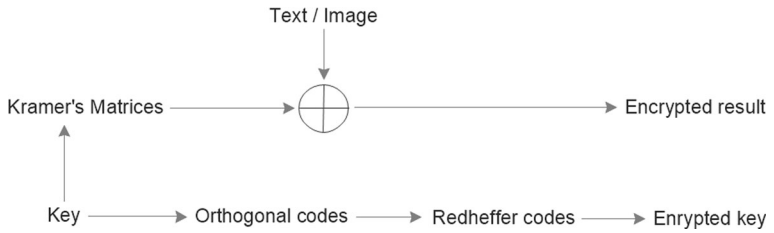

Fig. 1 Proposed encryption strategy

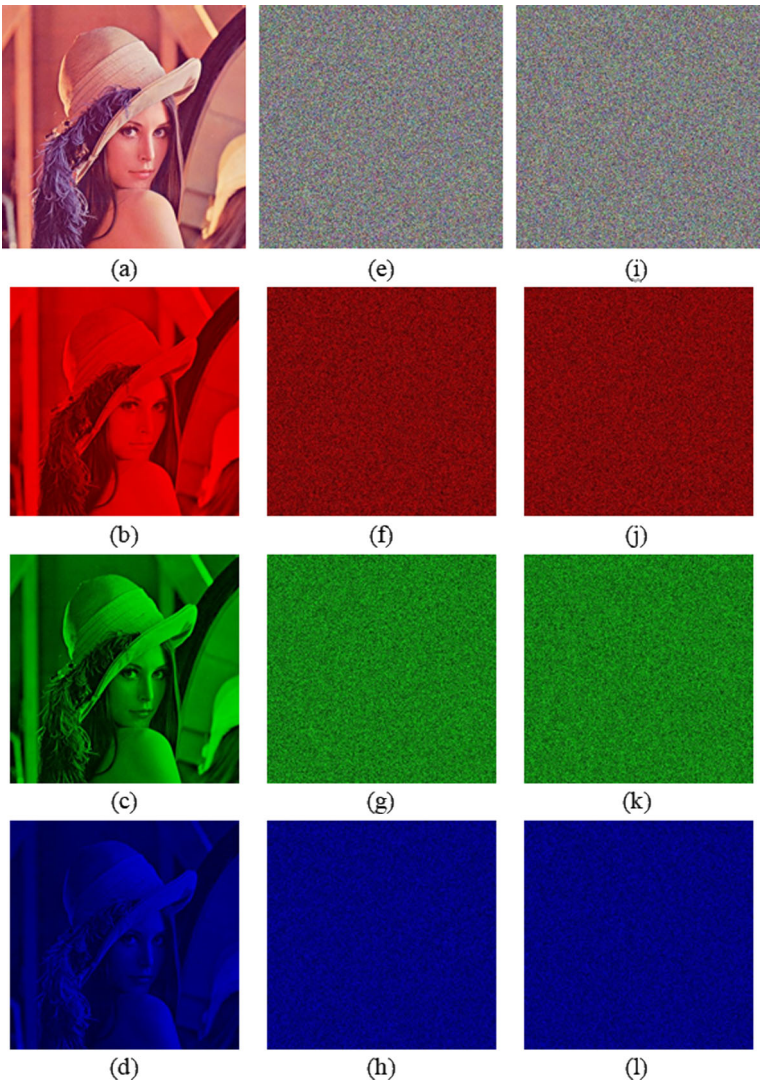

Fig. 2 Plain and encrypted layer wise contents of Lena image. (**a**-**d**) Plain image and its corresponding layer wise contents, (**e**-**h**) Encrypted image and its corresponding layer wise contents at S (3/2), (**i**-**l**) encrypted image and its corresponding layer wise contents at S (5/2)

the barrier contrary to quantifiable analysis. To testify the association among nearby pixels in plain and enciphered images, 10,000 sets of two nearby pixels from each digital content initially selected [29]. It is demonstrated by the following expression:

$$r_{x,y} = \frac{\sigma_{x,y}}{\sqrt{\sigma_x^2 \sigma_y^2}}, \tag{9}$$

where x and y are values of two nearby pixels at gray scale, while $\sigma_x{}^2$ and σ_y^2 represents the variances and $\sigma_{x,\,y}$ is the covariance of random variables x and y.

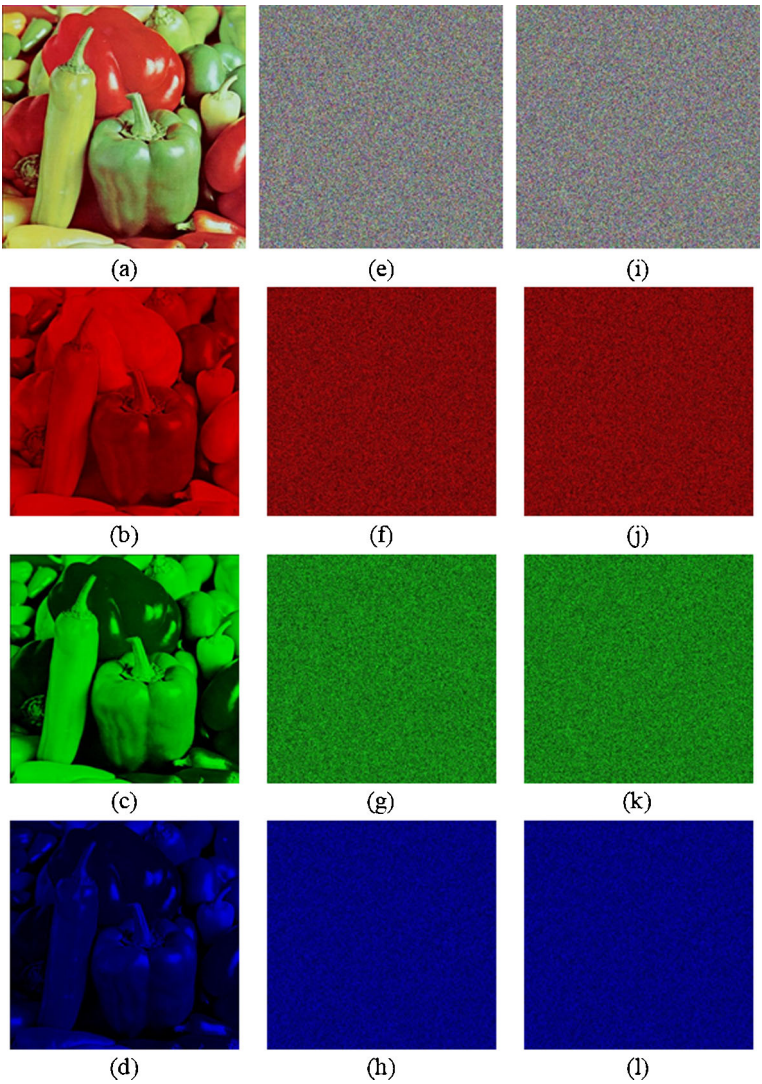

Fig. 3 Plain and encrypted layer wise contents of Pepper image. (**a**-**d**) Plain image and its corresponding layer wise contents, (**e**-**h**) Encrypted image and its corresponding layer wise contents at S (3/2), (**i**-**l**) encrypted image and its corresponding layer wise contents at S (5/2)

The coefficients of correlation for plain and encrypted images having dissimilar contents conveyed in Table 4. The association among various couples of original and encrypted images evaluated by calculating the two dimensional correlation coefficients among the original encrypted images [30]. The succeeding calculation is employed to compute the correlation coefficients. The mathematical expression for correlation coefficient is given below:

$$r = \frac{\sum_{i,j=1}^{M,N} \left(P_{ij} - \overline{P}\right)\left(C_{ij} - \overline{C}\right)}{\sqrt{\left(\sum_{i,j=1}^{M,N} \left(P_{ij} - \overline{P}\right)^2\right)\left(\sum_{i,j=1}^{M,N} \left(C_{ij} - \overline{C}\right)^2\right)}}, \tag{10}$$

Table 1 Orthogonal code words set

Orthogonal set	Code words	Data bits
H_1	$\begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}$	$\begin{bmatrix} 0 \\ 1 \end{bmatrix}$
$H_2 = \begin{bmatrix} H_1 & H_1 \\ H_1 & \overline{H_1} \end{bmatrix}$	$\begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 \end{bmatrix}$	$\begin{bmatrix} 0 & 0 \\ 0 & 1 \\ 1 & 0 \\ 1 & 1 \end{bmatrix}$
$H_3 = \begin{bmatrix} H_2 & H_2 \\ H_2 & \overline{H_2} \end{bmatrix}$	$\begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{bmatrix}$	$\begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{bmatrix}$
.	.	.
.	.	.
.	.	.

where P and C signifies the plain and cipher images, $\overline{P}$ and $\overline{C}$represents the mean values of P and C, M and N demonstrates the height and width of original / cipher images.

The plain and cipher contents are significantly dissimilar from each other as the coefficients of cipher images are very close to zero. The valuation for coefficients of correlation for anticipated design with recent approaches using standard images specified in Tables 5 and 6.

The outcomes of our proposed structure have inferior values coefficients, which meet the necessities for competent technique in real time application for enciphering.

4.4 Pixels' Resemblance Analyses

The resemblance measures primarily reveal the similarity among diverse digital contents. The normalized cross correlation (NCC) and structural contents (SC) values are quite closed to 1

Table 2 Bi-Orthogonal code words set

Bi-Orthogonal set	Code words	Data bits
$B_2 = \begin{bmatrix} H_1 \\ \overline{H_1} \end{bmatrix}$	$\begin{bmatrix} 0 & 0 \\ 0 & 1 \\ 1 & 1 \\ 1 & 0 \end{bmatrix}$	$\begin{bmatrix} 0 & 0 \\ 0 & 1 \\ 1 & 0 \\ 1 & 1 \end{bmatrix}$
$B_3 = \begin{bmatrix} H_2 \\ \overline{H_2} \end{bmatrix}$	$\begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 \end{bmatrix}$	$\begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{bmatrix}$
.	.	.
.	.	.
.	.	.

Table 3 NIST test results for enciphered Lena image at S (5/2)

Tests		Layer wise enciphered image p - values				Remarks
		Gray	Red	Green	Blue	
Frequency		0.36110	0.16410	0.46703	0.25495	Pass
Block frequency		0.24862	0.64862	0.53145	0.17988	Pass
Rank		0.39181	0.29191	0.29191	0.29191	Pass
Runs (M = 10,000)		0.51765	0.21762	0.90595	0.54043	Pass
Long runs of ones		0.64524	0.67514	0.71270	0.71270	Pass
Overlapping templates		0.74489	0.85988	0.85988	0.85988	Pass
No overlapping templates		0.99289	0.92285	0.54825	0.99989	Pass
Spectral DFT		0.78464	0.88464	0.38399	0.02952	Pass
Approximate entropy		0.36074	0.16074	0.33744	0.69469	Pass
Universal		0.99892	0.99445	0.99292	0.99659	Pass
Serial	*p values 1*	045133	0.17143	0.03998	0.65972	Pass
Serial	*p values 2*	0.77835	0.87464	0.00606	0.98104	Pass
Cumulative sums forward		0.45823	0.36470	0.34767	0.35256	Pass
Cumulative sums reverse		0.66215	0.35221	0.89099	0.77967	Pass
Random excursions	$X=-3$	0.99314	0.77296	0.00446	0.066231	Pass
	$X=-2$	0.98624	0.61069	0.054643	0.2397	Pass
	$X=-1$	0.97465	0.78256	0.4719	0.69271	Pass
	$X=1$	0.97465	0.97787	0.53038	0.91026	Pass
	$X=2$	0.14465	0.72112	0.52621	0.032984	Pass
	$X=3$	0.0000082	0.59346	0.33854	0.091826	Pass

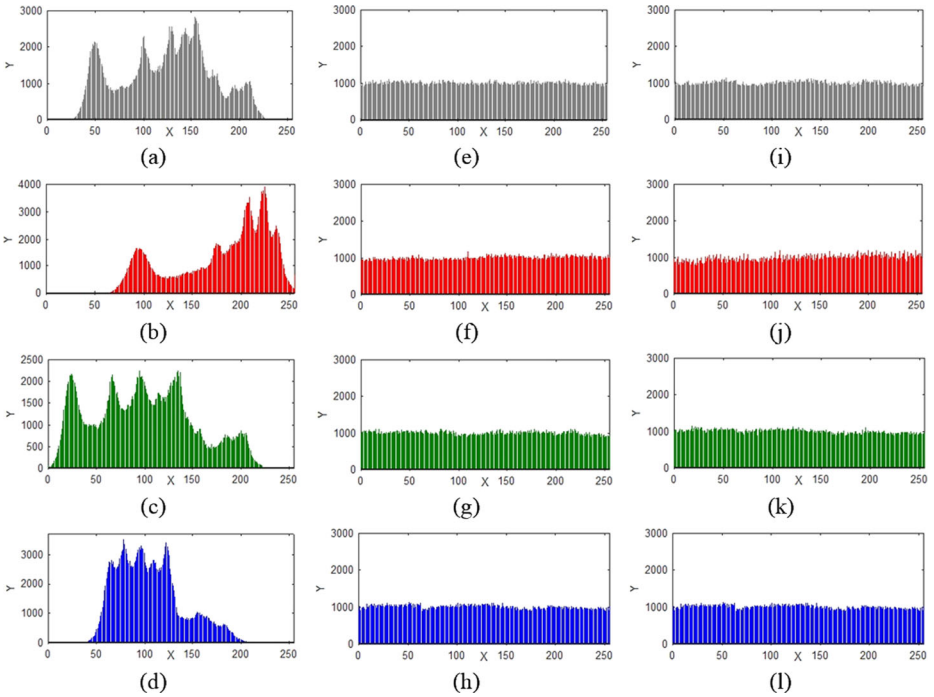

Fig. 4 Plain and enciphered layer wise histograms of Lena image. (**a**-**d**) Plain image and its corresponding layer wise histograms, (**e**-**h**) Encrypted image at S (3/2) and its corresponding layer wise histograms, (**i**-**l**) Encrypted image at S (5/2) and its corresponding layer wise histograms

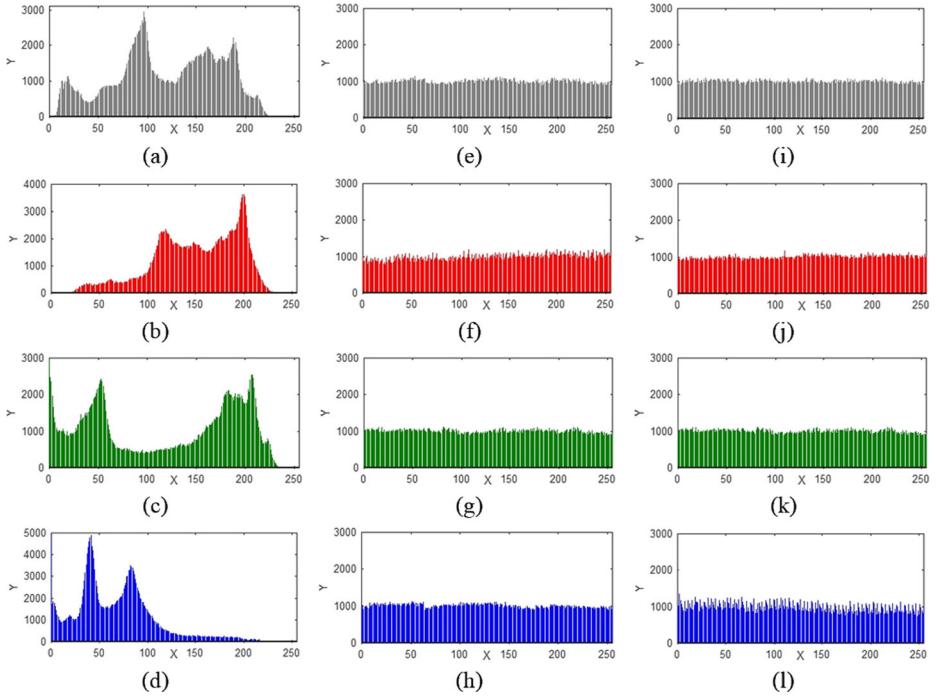

Fig. 5 Plain and enciphered layer wise histograms of Pepper image. (**a**-**d**) Plain image and its corresponding layer wise histograms, (**e**-**h**) Encrypted image at S (3/2) and its corresponding layer wise histograms, (**i**-**l**) Encrypted image at S (5/2) and its corresponding layer wise histograms

for digital contents structure similarity [29]. There are different types of resemblance coefficient are consumed in order to quantitatively find the structure dissimilarity in digital contents. We have analyzed the structural similarity index, normalized cross correlation and structural content between plain ($P_{i,\,j}$) and cipher ($C_{i,\,j}$) images in order to estimate the structure dissimilarity among different digital contents from reference. Structural similarity index metric (SSIM) used to compare the assembly, luminance and divergence between original and enciphered images.

$$SSIM = \frac{\left(2\mu_p\mu_c + C_1\right)\left(2\sigma_{pc} + C_2\right)}{\left(\mu_p^2 + \mu_c^2 + C_1\right)\left(\sigma_p^2 + \sigma_c^2 + C_2\right)}, \tag{11}$$

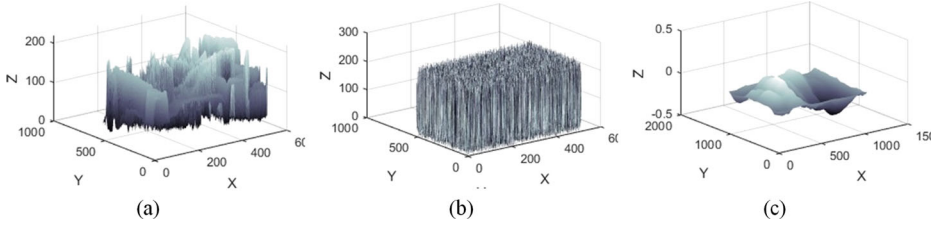

Fig. 6 Three dimensional surface plots for normalized cross-correlation of Lena image. **a** 3-D surface plot for Lena image, **b** 3-D surface plot for encrypted Lena image, **c** 3-D surface plot for cross-correlation between a-b

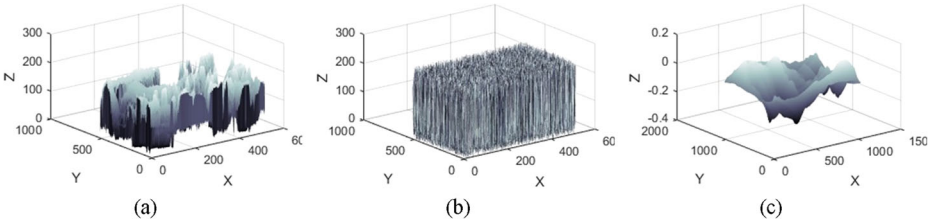

Fig. 7 Three dimensional surface plots for normalized cross-correlation of Pepper image. **a** 3-D surface plot for Pepper image, **b** 3-D surface plot for encrypted Pepper image, **c** 3-D surface plot for cross-correlation between a-b

where μ_p and μ_c are the mean values,σ_{pc} is the standard deviation of $P_{i,\,j}$ and $C_{i,\,j}$. The approximation of Eq. 11 approaches 1, if there is any resemblance between plain and cipher images. NCC measures the resemblance and traces of correlation between plain and enciphered images. We perform this test at the original and the encrypted images to analyze the similarity between them.

$$NCC = \sum_{i=0}^{M-1} \sum_{j=0}^{N-1} \frac{P_{i,j} \times C_{i,j}}{\sum_{i=0}^{M-1} \sum_{j=0}^{N-1} P^2{}_{i,j}}. \tag{12}$$

SC determines the structural details and quality of an image in terms of sharpness and noise level. The quality of an image assessed by the following equation and if the value of SC is higher, the quality of an image is poor.

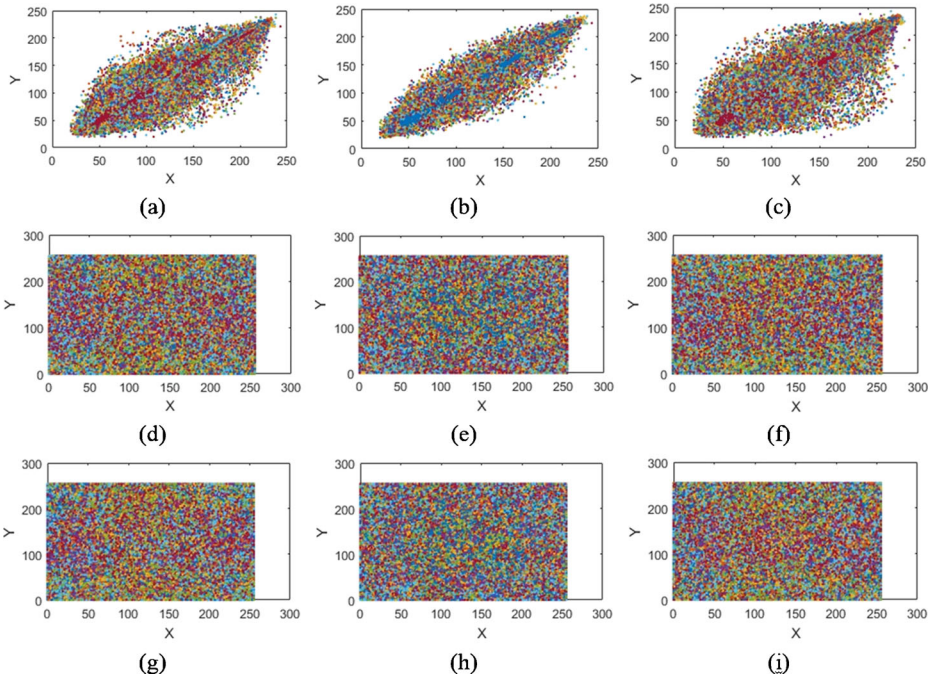

Fig. 8 Correlation between pixels' pairs for Lena image. (**a**-**c**) Correlation of Horizontal, Vertical and Diagonal directions of original image, (**d**-**f**) Correlation of Horizontal, Vertical and Diagonal directions of encrypted image at *S* (3/2), (**g**-**i**) Correlation of Horizontal, Vertical and Diagonal directions of encrypted image at *S* (5/2)

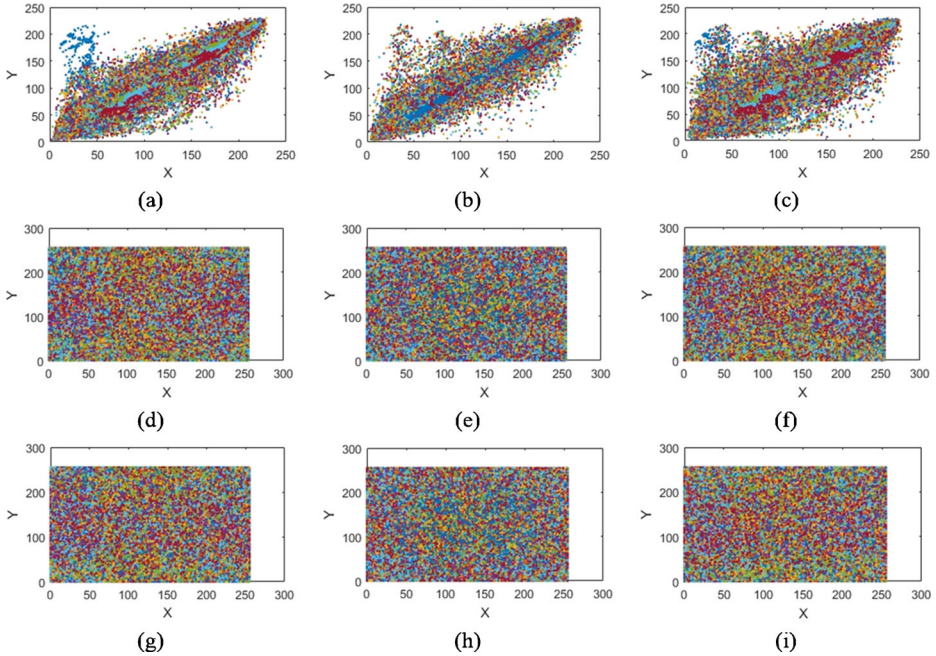

Fig. 9 Correlation between pixels' pairs for Pepper image. (**a**-**c**) Correlation of Horizontal, Vertical and Diagonal directions of original image, (**d**-**f**) Correlation of Horizontal, Vertical and Diagonal directions of encrypted image at S (3/2), (**g**-**i**) Correlation of Horizontal, Vertical and Diagonal directions of encrypted image at S (5/2)

$$SC = \sum_{i=0}^{M-1}\sum_{j=0}^{N-1} \frac{P^2{}_{i,j}}{\sum_{i=0}^{M-1}\sum_{j=0}^{N-1} C^2{}_{i,j}}. \tag{13}$$

4.5 Pixels' Discrepancy Analyses

The eminence assessment of an image based on pixels' discrepancy process analyzed here by evaluating the mean absolute error (MAE), mean square error (MSE) and peak signal to noise ratio

Table 4 Plain and enciphered images correlation coefficients at gray scale

Image	Plain			Encrypted at S (3/2)			Encrypted at S (5/2)		
	Horizontal	Vertical	Diagonal	Horizontal	Vertical	Diagonal	Horizontal	Vertical	Diagonal
Lena	0.9737	0.9869	0.9610	−0.0024	0.0007	−0.0065	−0.0005	−0.0007	0.0003
Pepper	0.9814	0.9833	0.9665	−0.0009	0.0003	−0.0047	−0.0008	0.0005	0.0001
Baboon	0.8534	0.7598	0.7300	−0.0003	−0.0045	0.0034	0.0005	−0.0002	−0.0008
Airplane	0.9662	0.9639	0.9368	0.0040	0.0018	−0.0086	−0.0006	−0.0009	0.0002
House	0.9479	0.957	0.9132	0.0011	0.0065	−0.0074	−0.0008	0.0007	−0.0004
Jelly beans	0.9787	0.982	0.9646	−0.0019	0.0028	−0.0063	0.0007	−0.0003	−0.0003
Sail boat	0.9737	0.9700	0.9569	0.0004	−0.0057	0.0025	0.0002	−0.0003	−0.0004
Splash	0.9840	0.9915	0.9773	0.0008	−0.0023	−0.0048	−0.0004	0.0007	0.0006
Tree	0.9669	0.9441	0.9294	−0.0007	0.0015	0.0023	0.0006	−0.0004	−0.0005

Table 5 Comparisons for coefficients of correlation of proposed scheme with modern approaches

Image	Proposed encryption at S (5/2)			Ref. [31]			Ref. [32]		
	Horizontal	Vertical	Diagonal	Horizontal	Vertical	Diagonal	Horizontal	Vertical	Diagonal
Lena	−0.0005	−0.0007	0.0003	–	–	–	0.0009	0.0021	−0.0007
Pepper	−0.0008	0.0005	0.0001	–	–	–	0.0007	−0.0012	0.0001
Baboon	0.0005	−0.0002	−0.0008	0.0039	−0.0045	0.0039	−0.0001	0.0003	0.0008
Airplane	−0.0006	−0.0009	0.0002	−0.0016	0.0008	0.0033	0.0007	0.0003	−0.0005
House	−0.0008	0.0007	−0.0004	−0.0028	−0.0041	0.0045	0.0009	0.0051	0.0001
Jelly beans	0.0007	−0.0003	−0.0003	−0.0033	0.0018	−0.0045	–	–	–
Sail boat	0.0002	−0.0003	−0.0004	−0.0040	−0.0051	0.0001	–	–	–
Splash	−0.0004	0.0007	0.0006	0.0017	−0.0041	0.0015	–	–	–
Tree	0.0006	−0.0004	−0.0005	0.0019	−0.0021	0.0036	–	–	–

(PSNR) [29]. MAE is the most communal method used to measure the accuracy for continues variables. The average absolute difference between original and encrypted images calculated by MAE and its esteem must be greater to enhance the encryption security and defined as:

$$MAE = \frac{1}{M \times N} \sum_{i=0}^{M-1} \sum_{j=0}^{N-1} |P_{i,j} - C_{i,j}|. \tag{14}$$

Essentially encrypted digital contents have dissimilarity concerning the plain image. Both MSE and PSNR used to relate the image encryption quality, while MSE signifies the cumulative square error measure and PSNR indicates the peak error measurement between the original and ciphered image. By higher the MSE esteem and lower the PSNR values or vice versa signifies the better encryption quality.

$$MSE = \frac{\sum_{i=1}^{M} \sum_{j=1}^{N} \left(P_{ij} - C_{ij}\right)^2}{M \times N}, \tag{15}$$

where P_{ij} and C_{ij} refers the pixels position at i^{th} row and j^{th} column of plain and ciphered images distinctly. Superior the MSE esteem represents the enhancement of encryption strategy [30]. PSNR ratio determines the quality measure between plain and enciphered image described by the succeeding expression:

Table 6 Pixels resemblance analyses between plain and enciphered images and comparison with existing approach

Image	Similarity analyses for S (3/2)			Similarity analyses for S (5/2)			Ref. [29]		
	SSIM	SC	NCC	SSIM	SC	NCC	SSIM	SC	NCC
Lena	0.00308	0.0051	0.0205	0.00108	0.0009	0.0030	0.0047	0.0020	0.0041
Pepper	0.00699	0.0016	0.0160	0.00018	0.0002	0.0029	0.0030	0.0029	0.0044
Baboon	0.00438	0.0094	0.0381	0.00060	0.0053	0.0061	0.0010	0.0019	0.0070
Airplane	0.00221	0.0011	0.0219	0.00008	0.0006	0.0015	0.0016	0.0017	0.0011
House	0.00046	0.0187	0.0164	0.00013	0.0001	0.0068	0.0112	0.0018	0.0062
Jelly beans	0.00119	0.0021	0.0460	0.00041	0.0009	0.0036	0.0154	0.0081	0.0046
Sail boat	0.00264	0.0012	0.0153	0.00045	0.0007	0.0012	0.0030	0.0020	0.0026
Splash	0.00121	0.0170	0.0484	0.00048	0.0008	0.0077	0.0114	0.0089	0.0088
Tree	0.00563	0.0003	0.0411	0.00190	0.0002	0.0068	0.0019	0.0072	0.0032

Table 7 Pixels' discrepancy analyses between plain and enciphered images and comparison with existing approach

Image	Difference analyses for S (3/2)			Difference analyses for S (5/2)			Ref. [29]		
	MAE	MSE	PSNR	MAE	MSE	PSNR	MAE	MSE	PSNR
Lena	86.66	7666.51	9.4409	87.84	8715.76	8.8570	85.48	8992.82	8.8917
Pepper	81.25	6839.19	10.5672	86.45	9392.82	8.5917	87.97	8853.77	8.8954
Baboon	87.11	6201.74	10.7934	88.56	9219.66	8.6865	79.88	8765.76	8.9570
Airplane	76.38	7984.73	9.2165	89.95	9553.77	8.2954	81.53	8619.66	8.9865
House	76.72	6215.08	10.7212	89.22	8978.88	8.7195	89.23	8924.86	8.8919
Jelly beans	75.38	6438.93	10.7211	84.89	8896.29	8.8854	66.83	8566.12	8.8954
Sail boat	78.28	7656.78	9.4939	88.32	9142.86	8.6962	88.34	8142.86	9.1162
Splash	75.23	6998.14	10.4904	82.11	8106.73	8.9852	78.17	9106.73	8.1152
Tree	81.34	6578.77	10.6685	87.98	9436.10	8.4345	78.99	7436.10	9.4345

$$\mathrm{PSNR} = 20\log_{10}\left[\frac{I_{MAX}}{\sqrt{MSE}}\right], \tag{16}$$

where I_{MAX} is the utmost pixel's estimation of image. On comparing with immense difference between the plain and ciphered images, PSNR should be low esteem. The feasibility of proposed approach assessed for MSE and PSNR for standard digital images presented in Table 7.

4.6 Entropy Analyses

The leading feature for specifying the randomness quantified by Entropy. Specified an independent source of random trials from set of probable distinct trials $\{x_1, x_2, x_3, ..., x_n\}$ with allied possibilities, the average output of source evidence called entropy [33]. Entropy of an image can be calculated as:

$$H = -\sum_{n=0}^{2^N-1} p(x_n)\log_2 p(x_n), \tag{17}$$

where x_i is the source image and 2^N is the aggregate of data. For perfectly indiscrimination in digital contents, the ideal Shannon entropy is 8. The entropies of different standard plain images and their encrypted contents accounted in Table 8.

The entropy esteems of encrypted images are very close to ideal Shannon esteem, which implies the leakage of data in proposed encryption algorithm is inappropriate and the mechanism is secure upon entropy attacks [34]. The information entropies of suggested scheme for encrypted images have superior results, when compared with existing approaches. Table 9 demonstrate the comparison of proposed technique with existing approaches for standard images.

4.7 Gray Level Co-Occurrence Matrix (GLCM) Analyses

The visual strength of anticipated scheme analyzed here by homogeneity, contrast and energy assessments [35]. The image assessed by homogeneity defined as:

$$H_g = \sum_{i,j} \frac{\rho(i,j)}{1+|i-j|}, \tag{18}$$

Table 8 Information entropies analyses for plain and encrypted images of size 512 × 512

Image	Plain				Encrypted at S (3/2)				Encrypted at S (5/2)			
	Gray	Red	Green	Blue	Gray	Red	Green	Blue	Gray	Red	Green	Blue
Lena	7.4455	7.2703	7.5881	7.0026	7.9991	7.9976	7.9981	7.9926	7.9991	7.9991	7.9998	7.9901
Pepper	7.5835	7.3587	7.6157	7.1495	7.9986	7.9953	7.9970	6.9903	7.9991	7.9993	7.9996	7.9911
Baboon	7.7666	7.7444	7.4493	7.7513	7.9976	7.9911	7.9993	7.9932	7.9998	7.9994	7.9991	7.9998
Airplane	6.6879	6.7489	6.8106	6.2682	7.9901	7.9910	7.9912	7.9949	7.9995	7.9992	7.9994	7.9997
House	7.6212	7.3522	7.3682	7.5852	7.9954	7.9964	7.9984	7.9912	7.9998	7.9994	7.9995	7.9992
Jelly beans	6.8837	5.4811	5.9294	6.5942	7.9957	7.9903	7.9931	7.9959	7.9991	7.9997	7.9995	7.9998
Sail boat	7.8645	7.4129	7.7156	7.4538	7.9918	7.9942	7.9924	7.9950	7.9997	7.9991	7.9993	7.9997
Splash	7.2396	7.1853	7.1815	6.5192	7.9916	7.9916	7.9911	7.9951	7.9993	7.9992	7.9991	7.9993
Tree	7.5634	7.2798	7.4610	6.9923	7.9914	7.9998	7.9936	7.9905	7.9992	7.9995	7.9994	7.9992

Table 9 Comparison of information entropies of proposed scheme with modern approaches

Image	Encrypted at S (5/2)				Ref. [29]				Ref. [32]		Ref. [31]	
	Gray	Red	Green	Blue	Gray	Red	Green	Blue	Gray	Red	Green	Blue
Lena	7.9991	7.9991	7.9998	7.9901	7.9995	7.9994	7.9993	7.9994	7.9991	7.9992	7.9992	7.9993
Pepper	7.9991	7.9993	7.9996	7.9911	7.9993	7.9994	7.9991	7.9992	7.9991	7.9993	7.9993	7.9993
Baboon	7.9998	7.9994	7.9991	7.9998	7.9989	7.9968	7.9986	7.9984	7.9998	–	–	–
Airplane	7.9995	7.9992	7.9994	7.9997	7.9991	7.9992	7.9993	7.9990	7.9995	7.9993	7.9993	7.9992
House	7.9998	7.9994	7.9995	7.9992	7.9993	7.9991	7.9993	7.9991	7.9998	7.9993	7.9993	7.9993
Jelly beans	7.9991	7.9997	7.9995	7.9998	7.9984	7.9975	7.9968	7.9972	7.9991	7.9971	7.9962	7.9973
Sail boat	7.9997	7.9991	7.9993	7.9997	7.9994	7.9991	7.9993	7.9993	7.9997	7.9992	7.9993	7.9992
Splash	7.9993	7.9992	7.9991	7.9993	7.9982	7.9979	7.9973	7.9983	7.9993	–	–	–
Tree	7.9992	7.9995	7.9994	7.9992	7.9988	7.9975	7.9974	7.9982	7.9992	7.9971	7.9973	7.9971

where i, j indicates the row and column position of image's pixel. This analysis performs the closeness of distribution in GLCM to GLCM diagonally. Its range lies in between 0 and 1. The identification of an object in texture of image observed by contrast analysis and it is defined as:

$$C = \sum_{i,j} |i-j|^2 \rho(i,j). \tag{19}$$

The contrast test range lies in between 0 and $(size\,(image) - 1)^2$. Greater the contrast value illustrates the large number of variations in the pixels of an image while constant image has 0 contrast value. The energy analysis of an image returns the sum of squared elements in GLCM and defined as:

$$E = \sum_{i,j} \rho(i,j)^2. \tag{20}$$

The constant image has 1 energy, while range of energy lies in-between 0 and 1. GLCM analyses for plain and enciphered images for S (3/2) and S (5/2) demonstrated in Table 10.

4.8 Linear Attacks Analyses

To perform linear attacks, cryptanalyst has to identify the linear relation between some bits of plain image, cipher image and key. By considering this relation, cryptanalyst can easily understand the structure used in encryption and decryption [36]. The analyst decrypts each cipher using all possible keys to predict the sequence similarity in ciphers, but in our case, the analyst has no idea what spin system used for encryption. Either the message pass by one or multiple spin systems and each spin system has 24! states, and in each state there are infinite positions for encryption. All the spin matrices create confusion and also have infinite possibilities to create the keys. The analyst can focus on statistical analyses against multiple rounds of decryption but each time the results produced with proposed structure has no relation with any previous outcome.

4.9 Differential Attacks Analyses

To testify the robustness against differential attacks for anticipated scheme, an adjustment of one pixel in plain image modifies the encrypted image for comparing, with a probability of half pixel altering. For a change in i^{th} chunk of permuted digital image affects the i^{th} chunk of ciphered image directly. We certify that our structure has suitable affectability to plain images to affirm the impact of altering a single pixel in a plain image and the whole enciphered image. For a specific objective to measure the impact of minor alteration in plain image on its encrypted one, the number of pixels changing rate (NPCR) bound together to originate the unified average change intensity (UACI) [37, 38]. The NPCR and UACI can be assessed by utilizing the succeeding expressions for two encoded images $C_1(i,j)$ and $C_2(i,j)$, in which one have source image just varied by one pixel. The expression for NPCR and UACI are given below:

$$\mathrm{NPCR} = \textstyle\sum_{i,j} \dfrac{D(i,j)}{W \times H} \times 100\%, \tag{21}$$

Table 10 GLCM analyses among original and encrypted standard images and comparison with existing approach

Image	Encryption at S (3/2)			Encryption at S (5/2)			Ref. [29]		
	Homogeneity	Contrast	Energy	Homogeneity	Contrast	Energy	Homogeneity	Contrast	Energy
Lena	0.9891	10.4363	0.0097	0.9921	10.9876	0.0097	0.9856	10.6103	0.0156
Pepper	0.9894	10.5103	0.0148	0.9899	10.7659	0.0093	0.9893	10.6231	0.0156
Baboon	0.9794	10.5001	0.0151	0.9897	11.1127	0.0099	0.9891	10.4963	0.0157
Airplane	0.9896	10.6231	0.0156	0.9898	11.0135	0.0102	0.9890	10.5001	0.0155
House	0.9898	10.4498	0.0158	0.9981	10.9692	0.0124	0.9791	10.4421	0.0158
Jelly beans	0.9799	10.5521	0.0167	0.9972	10.8823	0.0095	0.9796	10.5101	0.0157
Sail boat	0.9885	10.3136	0.0152	0.9964	10.6963	0.0097	0.9894	10.5136	0.0157
Splash	0.9798	10.4354	0.0149	0.9915	10.6651	0.0106	0.9795	10.5006	0.0159
Tree	0.9793	10.6651	0.0098	0.9899	10.9263	0.0096	0.9895	10.5001	0.0156

Table 11 NPCR analyses between original and encrypted images and comparison with existing approach

Image	NPCR for S (3/2)				NPCR for S (5/2)				Ref. [29]			
	Gray	Red	Green	Blue	Gray	Red	Green	Blue	Gray	Red	Green	Blue
Lena	99.86	99.76	99.81	99.89	99.96	99.94	99.91	99.89	99.92	99.72	99.82	99.61
Pepper	99.92	99.82	99.83	99.81	99.94	99.92	99.92	99.91	99.84	99.81	99.86	99.77
Baboon	99.88	99.89	99.82	99.87	99.95	99.95	99.92	99.97	99.86	99.86	99.81	99.89
Airplane	99.84	99.81	99.86	99.87	99.94	99.91	99.96	99.95	99.88	99.85	99.72	99.87
House	99.79	99.75	99.66	99.88	99.97	99.95	99.93	99.96	99.79	99.65	99.68	99.86
Jelly beans	99.85	99.85	99.85	99.84	99.98	99.89	99.89	99.89	99.81	99.82	99.83	99.77
Sail boat	99.89	99.86	99.81	99.83	99.92	99.96	99.92	99.91	99.89	99.86	99.78	99.81
Splash	99.75	99.72	99.77	99.79	99.91	99.92	99.88	99.92	99.74	99.62	99.72	99.58
Tree	99.87	99.78	99.72	99.89	99.92	99.86	99.87	99.90	99.82	99.76	99.67	99.87

where

$$D(i,j) = \begin{cases} 0, & C_1(i,j) = C_2(i,j) \\ 1, & C_1(i,j) \neq C_2(i,j) \end{cases}$$
$$UACI = \sum_{i=0}^{M-1} \sum_{j=0}^{N-1} \frac{\left| C_1(i,j) - C_2(i,j) \right| / 255}{W \times H \times 100\%.} \tag{22}$$

To evaluate the sensitivity of plain image, encrypt the plain image and randomly choose and altered one pixel in plain image. Tables 11, 12 and 13 provides the experimental outcomes for encrypted results of NPCR and UACI and their comparison with existing latest approaches.

Table 11 validates the NPCR esteems are correspondent to the perfect estimation of 1, while Table 12 correspond the UACI esteems which have better results than existing approaches. These outcomes show that projected technique has great degree sensitive to minor change in plane image, irrespective of whether the two ciphered images have one-bit alteration [30]. The anticipated structure has superior ability to hostile the differential assaults in investigation with alternative approaches.

Table 12 UACI analyses between original and encrypted images and comparison with existing approach

Image	UACI for S (3/2)				UACI for S (5/2)				Ref. [29]			
	Gray	Red	Green	Blue	Gray	Red	Green	Blue	Gray	Red	Green	Blue
Lena	33.58	34.97	33.16	33.81	33.68	35.32	34.32	33.42	33.58	36.39	33.14	35.26
Pepper	33.48	36.39	33.14	34.26	33.59	37.16	35.17	35.23	33.44	38.33	34.26	34.21
Baboon	33.64	35.48	33.29	34.11	33.84	35.02	34.16	33.51	33.68	34.97	33.06	33.81
Airplane	33.44	35.33	33.26	34.21	33.71	36.33	33.24	34.26	33.64	35.48	33.06	34.81
House	33.33	33.34	33.19	32.89	33.53	33.37	34.11	33.92	33.25	32.37	33.21	32.41
Jelly beans	33.24	32.99	32.95	33.11	33.57	33.92	32.98	33.46	33.21	32.94	31.85	33.18
Sail boat	33.52	32.92	34.06	33.09	33.66	34.16	34.32	33.23	33.47	32.56	34.11	32.25
Splash	33.18	34.56	32.93	33.04	33.54	33.72	32.93	33.18	33.04	34.42	30.14	32.29
Tree	33.11	33.81	32.65	33.36	33.58	33.21	33.68	34.19	33.31	33.64	31.55	33.23

Table 13 Pixels difference analyses by introducing noise between plain and enciphered standard images

Image	Encrypted image at S (5/2)		Noise intensity							
			0.000001		0.000003		0.000005		0.000007	
	MSE	PSNR	MSE	PSNR	MSE	PSNR	MSE	PSNR	MSE	PSNR
Lena	8715.76	8.8570	8653.77	8.8676	8611.69	8.8843	8565.42	8.9672	8498.99	8.9978
Pepper	9392.82	8.5917	9298.88	8.5997	9184.75	8.6329	8992.75	8.7421	8897.98	8.7953
Baboon	9219.66	8.6865	8987.86	8.6516	8879.66	8.6115	8798.96	8.7986	8698.96	8.8265
Airplane	9553.77	8.2954	9454.68	8.5524	9103.77	8.6454	8995.89	8.7052	8867.72	8.7954
House	8924.86	8.7195	8621.34	8.8393	8312.82	9.0013	8103.43	9.1982	7921.92	9.8953
Jelly beans	8566.12	8.8854	8325.11	8.9987	8109.62	9.1107	7874.54	9.9143	7634.35	10.0051
Sail boat	9142.86	8.6962	8943.35	8.7942	8756.43	8.8422	8546.84	8.9923	8499.29	8.9979

4.10 Noise Attacks Analyses

It is possible that encrypted data affected by noises during transmission. The robustness of the proposed structure against Gaussian noise considered here. The normalized intensities of noise are set as 0.000001, 0.000003, 0.000005 and 0.000007 respectively.

As the intensity of noise change from 0.000001 to 0.000007, the PSNR value has very minute change or we can say its approximately same to the original, which depicts the proposed design has good robustness against noise attacks.

5 Conclusion

The proposed scheme is appropriate for real time applications due to small processing time and superior capacity to hostile the attacks and appropriate performance than other encryption systems. The Kramer's spin system not only valid for RGB contents but it can be applied at variety of digital contents like audio, video, medical images and satellite images. In future, we would like to use quantum iterative maps instead of Redheffer and orthogonal codes to enhance security level.

Acknowledgments Both authors Hafiz Muhammad Waseem and Dr. Majid Khan are highly grateful to Vice Chancellor Dr. Syed Wilayat Husain, Dean Iqbal Rasool Memon, and Director cyber and information security Lab Prof. Dr. Muhammad Amin, Institute of Space Technology, Islamabad Pakistan, for providing decent atmosphere for research and development.

Compliance with Ethical Standards

Conflict of Interest Both authors have no conflict concerning the publication of this article.

References

1. Waseem, H.M., Khan, M.: Information confidentiality using quantum spinning, rotation and finite state machine. Int. J. Theor. Phys. **57**(11), 3584–3594 (2018)
2. Premaratne, P., Premaratne, M.: Key-based scrambling for secure image communication. In: International Conference on Intelligent Computing, pp. 259–263. Springer, Berlin, Heidelberg (2012)

3. Unnikrishnan, G., Joseph, J., Singh, K.: Optical encryption by double-random phase encoding in the fractional Fourier domain. Opt. Lett. **25**(12), 887–889 (2000)
4. Zhu, B., Liu, S., Ran, Q.: Optical image encryption based on multifractional Fourier transforms. Opt. Lett. **25**(16), 1159–1161 (2000)
5. Peng, X., Yu, L., Cai, L.: Double-lock for image encryption with virtual optical wavelength. Opt. Express. **10**(1), 41–45 (2002)
6. Nishchal, N.K., Joseph, J., Singh, K.: Securing information using fractional Fourier transform in digital holography. Opt. Commun. **235**(4–6), 253–259 (2004)
7. Situ, G., Zhang, J.: A lensless optical security system based on computer-generated phase only masks. Opt. Commun. **232**(1–6), 115–122 (2004)
8. Chen, L., Zhao, D.: Optical image encryption based on fractional wavelet transform. Opt. Commun. **254**(4–6), 361–367 (2005)
9. Meng, X.F., Cai, L.Z., He, M.Z., Dong, G.Y., Shen, X.X.: Cross-talk-free double-image encryption and watermarking with amplitude–phase separate modulations. J. Opt. A Pure Appl. Opt. **7**(11), 624–631 (2005)
10. La Mela, C., Iemmi, C.: Optical encryption using phase-shifting interferometry in a joint transform correlator. Opt. Lett. **31**(17), 2562–2564 (2006)
11. Hwang, H.E., Han, P.: Fast algorithm of phase masks for image encryption in the Fresnel domain. JOSA A. **23**(8), 1870–1874 (2006)
12. Tao, R., Xin, Y., Wang, Y.: Double image encryption based on random phase encoding in the fractional Fourier domain. Opt. Express. **15**(24), 16067–16079 (2007)
13. Liu, Z., Liu, S.: Double image encryption based on iterative fractional Fourier transform. Opt. Commun. **275**(2), 324–329 (2007)
14. Ge, F., Chen, L., Zhao, D.: A half-blind color image hiding and encryption method in fractional Fourier domains. Opt. Commun. **281**(17), 4254–4260 (2008)
15. Liu, Z., Li, Q., Dai, J., Sun, X., Liu, S., Ahmad, M.A.: A new kind of double image encryption by using a cutting spectrum in the 1-D fractional Fourier transform domains. Opt. Commun. **282**(8), 1536–1540 (2009)
16. Wang, B., Zhang, Y.: Double images hiding based on optical interference. Opt. Commun. **282**(17), 3439–3443 (2009)
17. Meng, X.F., Cai, L.Z., Wang, Y.R., Yang, X.L., Xu, X.F., Dong, G.Y., Shen, X.X.: Digital image synthesis and multiple-image encryption based on parameter multiplexing and phase-shifting interferometry. Opt. Lasers Eng. **47**(1), 96–102 (2009)
18. Shannon, C.E.: Communication theory of secrecy systems. Bell system technical journal. **28**(4), 656–715 (1949)
19. Shannon, C.E.: A mathematical theory of communication. Bell system technical journal. **27**(3), 379–423 (1948)
20. Kramers, H.A., 1930. HA Kramers Proc. roy. Acad. Amsterdam, 32 (1929). In *Proc. roy. Acad.* Amsterdam (Vol. 33, p. 959)
21. Sklar, B., 2001. Digital Communications: Fundamentals and Applications
22. Barrett, W.W., Jarvis, T.J.: Spectral properties of a matrix of Redheffer. Linear Algebra Appl. 162–164 (1992)
23. Will Dana. Eigenvalues of the Redheffer Matrix and their Relation to the Mertens Function, 2015
24. Wheeler, N., 2000. Spin matrices for arbitrary spin. *Reed College Physics Department, Portland*
25. Dresden, M.H.A.: Kramer's: between Tradition and Revolution. springer (1987) ISBN 978-1-4612-4622-0
26. Umezawa, H., 1956. Quantum Field Theory
27. Younas, I., Khan, M.: A new efficient digital image encryption based on inverse left almost semi group and Lorenz chaotic system. Entropy. **20**(12), 913 (2018)
28. Khan, M., Asghar, Z.: A novel construction of substitution box for image encryption applications with Gingerbreadman chaotic map and S 8 permutation. Neural Comput. & Applic. **29**(4), 993–999 (2018)
29. Waseem, H.M., Khan, M.: A new approach to digital content privacy using quantum spin and finite-state machine. Applied Physics B. **125**(2), 27 (2019)
30. Khan, M., Waseem, H.M.: A novel image encryption scheme based on quantum dynamical spinning and rotations. PLoS One. **13**(11), e0206460 (2018)
31. Stoyanov, B., Kordov, K.: Image encryption using Chebyshev map and rotation equation. Entropy. **17**(4), 2117–2139 (2015)
32. Khan, M., Shah, T.: An efficient chaotic image encryption scheme. Neural Comput. & Applic. **26**, 1137–1148 (2015)
33. Waseem, H.M., Khan, M., Shah, T.: Image privacy scheme using quantum spinning and rotation. Journal of Electronic Imaging. **27**(6), 063022 (2018)

34. Munir, N. and Khan, M., 2018. A Generalization of Algebraic Expression for Nonlinear Component of Symmetric Key Algorithms of Any Characteristic p. In *2018 International Conference on Applied and Engineering Mathematics (ICAEM)* (pp. 48–52). IEEE
35. Hussain, I., Anees, A., Aslam, M., Ahmed, R., Siddiqui, N.: A noise resistant symmetric key cryptosystem based on S 8 S-boxes and chaotic maps. The European Physical Journal Plus. **133**, 1–23 (2018)
36. Blondeau, C., Leander, G., Nyberg, K.: Differential-linear cryptanalysis revisited. J. Cryptol. **30**(3), 859–888 (2017)
37. Khan, M., Shah, T.: A construction of novel chaos base nonlinear component of block cipher. Nonlinear Dynamics. **76**(1), 377–382 (2014)
38. Khan, M., Shah, T., Batool, S.I.: A new implementation of chaotic S-boxes in CAPTCHA. SIViP. **10**(2), 293–300 (2016)