Multimedia Tools and Applications (2021) 80:26069–26091
https://doi.org/10.1007/s11042-021-10898-w

A hybrid chaotic blowfish encryption for high-resolution satellite imagery

Syed Zeeshan Abbas[1] · Haroon Ibrahim[1,2] · Majid Khan[3,4]

Received: 24 December 2019 / Revised: 18 March 2021 / Accepted: 1 April 2021 /
Published online: 27 April 2021

Abstract
In this article, we have designed a new information confidentiality mechanism based on the combination of Blowfish encryption algorithm along with Henon and Chen chaotic dynamical systems. We have authenticated our proposed encryption algorithm over satellite and other standard digital images of image processing. Our proposed encryption algorithm is equally deployed as an encrtpter and decrypter while at the sending and receiving ends in satellite communication. In satellite communication, typical wireless mediums are used for transferring heavy payloads and usual telemetry. The priciple aim of this article is to design a new mechanism for the privacy of digital contents mainly satellite images. We have authenticated our anticipated mechanism with security performace analyses.

Keywords Blowfish encryption · Digital contents privacy · Satellite imagery

1 Introduction

Securing information in a modern digital world has become more important in every field of life. Keeping the secret information away from unauthentic clients or transforming it into a format that cannot be easily deciphered by the unauthorized viewer is known as information security [13, 43, 51]. The vital security components in the field of information theory are information confidentiality algorithms. These components are used to scramble the plain information into the

✉ Majid Khan
mk.cfd1@gmail.com

[1] WiSP Lab, Department of Electrical Engineering, Institute of Space Technology, Islamabad, Pakistan

[2] iVision Lab, Department of Electrical Engineering, Institute of Space Technology, Islamabad, Pakistan

[3] Department of Applied Mathematics and Statistics, Institute of Space Technology, Islamabad, Pakistan

[4] Cyber and Information Security Lab (CISL), Institute of Space Technology, Islamabad, Pakistan

incomprehensible format (known as encryption) which afterward unscramble by using the similar or dissimilar key (known as decryption) [20, 53, 54]. Since numerous enciphering algorithms are available in the literature and deliver the utmost security strength to an unauthorized user for information break, for example, Blowfish encryption scheme for checking its feature hiding capability in a satellite acquired image. Some applications have their essential concern with quick data processing capability (rapid ciphering phenomenon) with the trade-off of more security, but on the other hand, some cases are very keenly and critically keep the requirement of strengthening security [34, 39]. Many organizations whether in business or industry are mostly focused upon security issues rather than the pace of data processing. In the running era of modern digital communication, both the sender and receiver have a significant concern with the security for mutual correspondence. Keeping the sensitivity of the information, any chance of security ruptures present in the channel would cause a real misfortune at both ends of the transmitter and the receiver. Nowadays, various key systems in cryptography are providing ultra-secure mediums for ensuring information as well as securing data [1, 22].

In symmetric cryptographic systems, the key which is used for enciphering and deciphering process remains the same at both the ends of the transmitter and the receiver [33, 41]. Hence, before starting the transmission at both ends should make sure the key distribution for information exchange. The enciphering keys play a significant role and dependent upon the nature of the key length. Various symmetric schemes are available in the literature are, data encryption standard (DES), advanced encryption standard (AES), CAST, and Blowfish encryption algorithm [12, 17].

Blowfish is one of the most popular Feistel network block cipher and symmetric in nature, and comprised of 16-rounds along with the large key-dependent substitution boxes (S-boxes) for running simple encryption algorithm upon input data. The standard input block size in this cipher is 64 bits and key-length varies in between 32 and 448 bits, however, this cipher provides variable input block size which is also key-dependent and can vary in the form of 8, 16, 32 or 64 bits depending upon machines capability to handle longer calculations. In this regard key-length also varies from 4, 8, 16, 32 bits up to 56,112,224,448 bits based on input block size. The initialization phase for any type of an encryption scheme can be more complex, but the efficiency of the algorithm must be more convenient upon large microprocessors. Blowfish cipher can be implemented upon any type of an embedded platform with a sophisticated encryption/decryption rate and it has the provision of ineffective cryptanalysis to break the hidden information [36, 39]. Arguing the input block size for this cipher can be dependent on users' requirements but nominal use of this cipher deals with the plain text of 64 bits along with key-length of 448 bits long [2].

Our principle aim of this investigation is to introduce a simple component which is based on chaotic dyanimcal systems which add more confusion and diffusion capability in tradtyional blowfish encryption algorithm. The proposed encryption algorithm reduce the number of round and increases the randomness which is one of the prime goal of modern confidentiality mechanism. Moreover, the anticipated scheme reduce the computational complexity and utimatley cost of encryption at different layers of multimedia. We have tested our suggested algorithm over satellite images and achieved reasonably favorable results in term of security analysis [3–11, 14–16, 18, 19, 21, 23–32, 35, 37, 38, 40, 42, 44–50, 52].

This article is sorted out in 6 segments to demonstrate the hybrid chaotic blowfish criteria for high-resolution imaginaries and the standard normal images. The fundamental terminologies of chaotic maps and blowfish criteria are explained in Section 2, the proposed algorithm

and the experimentation on the variety of digital data deliberated in Section 3, the performance and security evaluations assessed in Section 4, and Section 5 provides the concluding remarks.

2 Fundamental terminologies

The demonstration of the blowfish network, encryption, as well as the decryption is exhibited in this section. The anticipated methodology and its implementation is inspected in the remainder of this article.

2.1 Chaotic Dyanimcs

Chaos is gererically refered as state of disorder. As per Robert L. Devaney, dynamical system must have following properties in order to classify as a chaotic system:

i Topologically transitive must exist,
ii Initial condiation must be sensitive
iii Dense periodic orbits must exist.

These chaotic dynamical systems can be further calsseified as discret or continuous. Discrete chaotic dyanimcal system contains iterative maps, wheresas continuous chaotic system consists of differential euqations [18–20, 42, 54].

2.2 Three dimensional Henon and Chen's chaotic map

This section discusses the overview of three dimisioanl Henon and Chen chaotic maps along with mathematical expreesions and chaotic paramters. Our propsed image encryption mechanism is based on chaotic system. The mathematical expression for three dimisional Henon chaotic iterative map is give below:

$$\begin{aligned} x_{i+1} &= a - y_i^2 - bz_i, \\ y_{i+1} &= x_i, \\ z_{i+1} &= y_i. \end{aligned}$$

The mentioned chaotic attractor generates more complex Hénon map in comparison with the maps generated from other existing chaotic attractors; when $1.54 < |a| < 2,\ 0 < |b| < 1$ along with initial conditions $x_0 = 1$, $y_0 = 0$and $z_0 = 0$. Following mathematical expression represents the iterative map of chaotic Chen:

$$\begin{aligned} x_{i+1} &= a(y_i - z_i), \\ y_{i+1} &= (c - a)x_i - x_i z_i + cy_i, \\ z_{i+1} &= x_i y_i - bz_i, \end{aligned}$$

where $a > 0,\ b > 0$ and c such that $(2c > a)$ represent the system parameters. Chen's system is considered as chaotic when the values of parameters are; $a = 35,\ b = 3$ and $c \in [20, 28.4]$. Chen's system has chaotic attractor when $a = 35,\ b = 3$, and $c = 28$. The exceptional three complex dynamic property and dimentionality makes the Chen's chaotic system comparatively difficult.

2.3 Blowfish encryption

Bruce Schneider perposed blowfish in 1993 and it is generally categorized in symmetric block ciphering techniques which are viably used for scrambling the secret information [37]. As mentioned earlier that this algorithm can be utilized in a variable-length key environment, which can vary from 4 to 32 bits to secure the information. Blowfish algorithms has a Feistel network type structure, emphasizing an encryption capacity of 16 times. The operating blowfish algorithm in a 32 bits' environment, the standard block size for plain data at the input will be 64 bits long, while the key length varies up to 448 bits. Having an intricate beginning stage required before the encryption process, the extreme effectiveness of this scheme can be visualized upon the vast microchips as being a strong proof for a genuine encryption scheme for securing information [28, 32].

2.4 Blowfish decryption

The deciphering process is carried out in a quite similar fashion as ciphering is done, aside from the fact that the key sequence $P_1, P_2 \ldots P_{18}$ is utilized in reverse order. It is conspicuous that XOR operation is guaranteed to be commutative and keep acquaintance, in this regard a misguidance is created for the backward request of the enciphering process as at the beginning of the decryption algorithm. To simulate the deciphering phenomena of P_{17} and P_{18} are XORed with encrypted text at the earliest stage and the *P*-array sequence is utilized in reverse for converse request. The timetable for the Blowfish key initialization is introduced by S-boxes and *P*-array having the qualities of ***"pi"*** hexadecimal values that may contain no irrefutable example. While having the key length of 448 bits, this fact can be positively conceivable that 448 bits point of internment guarantee of making each sub-key using the entire key sequence, and in this way the last four *P*-array estimations are not enough to influence the whole cipher-text. This point must be taken into account when an alternate number of rounds are chosen for calculation, despite having the fact that security strength debilitates with reducing the number of rounds [39].

3 Proposed image encryption algorithm

Chaotic maps have a capability of quick iterations because of their simplicity in functions. Chaos-based encryption schemes are therefore faster in real-time applications, especially for developing image encryption systems. In the recent past, many researchers have found that there exist relationships between the properties of chaos and cryptography [14]. The extremely sensitive initial conditions and deterministic pseudorandom performance have similarities between the cryptographic schemes and chaotic maps. The two general principles while designing any type of cryptographic schemes are confusion and diffusion phenomena's which leads to concealing of plain image structure and reducing the statistical dependency of pixels in encrypted images. Applying the mixing property of blowfish and chaos-based encryption algorithms will enhance the security strength (complexity) of the enciphered images.

Chaotic maps can be assigned to both the continuous and discrete time-domains. The discrete maps usually occur in an iterated function scenario, which are considered as the rounds of cryptosystems. This type of similarity between the chaotic systems and

cryptography is utilized to propose cryptosystems based on chaotic maps [7, 19, 26, 46]. Developing a certain chaotic map is based on some parameters which are equivalent to the ciphering keys in the cryptographic system, whereas by applying the chaotic system in a stream cipher, a long pseudorandom keystream is generated for enciphering each bit of the plain image but on the other hand, block ciphers introduced differently, as the initial controlling parameter is the secret key which is used for confusion at the beginning of encryption process. Finally, a chaotic system iterates upon the plain information for a serval times to obtain the cipher-text. The significant concern in a cryptosystem is the security and complexity which is created by the algorithm for information scrambling. This agenda is considered more deeply when map parameters are selected to use in cryptography. In the proposed chaos-based encryption scheme, we have encrypted the hyperspectral imaginary, airplane and the pepper images of size 512×512 with only two rounds (see Figs. 2, 3 and 4). These figures reveal that the histogram of our proposed encryption scheme (see Figs. 8, 9 and 10) achieved the uniformity in encrypted information having a high degree of randomness with no clue to eavesdropper where is the major information places.

3.1 Experimentation of proposed algorithm

The experimentation of Blowfish cipher has been carried out upon plain image $P(i, j)$ having $M \times N$ dimension, where ***"i"*** represents the i^{th} row and ***"j"*** is the j^{th} column of an image pixel.

1. Take a digital image with three layers
2. Take two three dimensional chaotic dynamical systems
3. Iterate the both dynamical system upto the size of digital image
4. Perform bitwise xor operation on each one dimensional preudo random number generators (PRNG)
5. Transform the images into corresponding layers and then transform each layer into 1×n direction.
6. Define the criteria of word length collection for piecewise processing of plain image and encryption key.
7. Specify the number of blowfish rounds to be run.
8. Initialize the S-boxes depending upon input word size. The S-box contents can be initialized by users' own choice, as there are 2^{32} binary combinations among which user has to choose 4×256 entries for the four S-boxes.
9. After the encryption transformation, the dimensions of the ciphered layers are converted into the plain image dimensions.
10. Combine all the ciphered layers for the formation of a single enciphered image.
11. Apply bitwise xor of obtained chaos based PRNG in step 4 with cipher image obtained in step 10 and display the final encrypted image.

We investigate the performance of the blowfish algorithm by implementing the abovementioned algorithm steps on the hyperspectral image and the standard Airplane and Pepper images with a constant number of variable key lengths and rounds. We examined the standard blowfish encryption algorithm against randomness by fixing the number of encryption rounds.

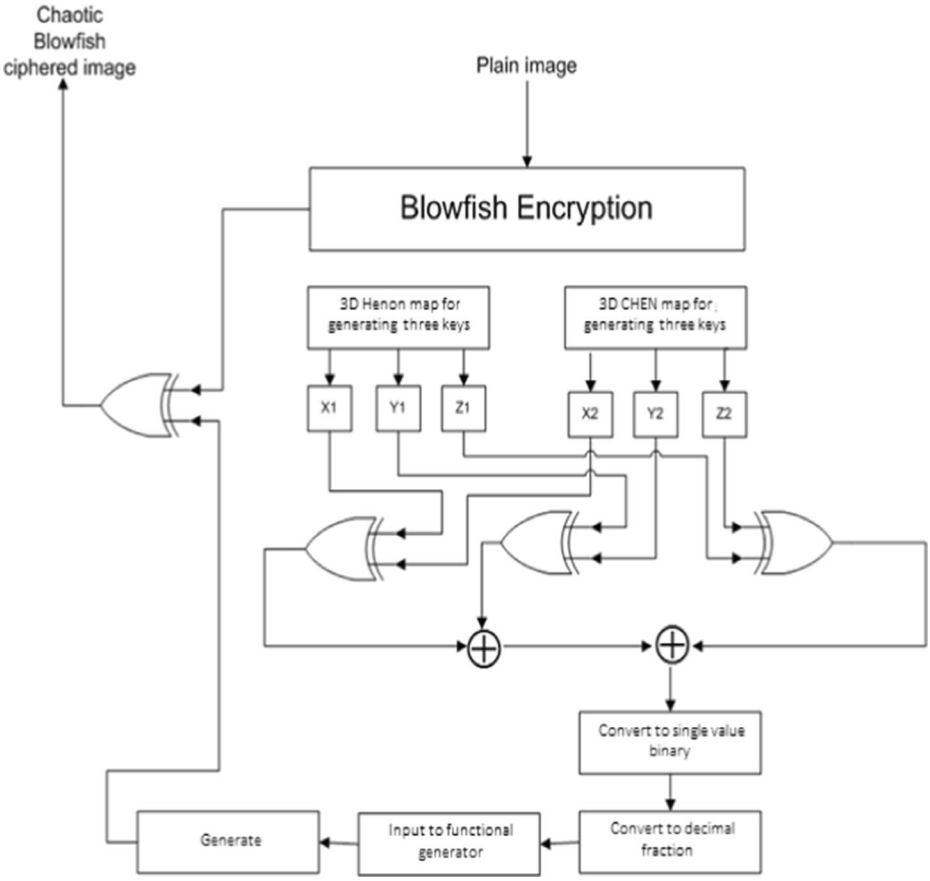


Fig. 1 Proposed Henon and Chen chaotic dynamical systems

4 Performance and security evaluations

To observe the affectability of the anticipated algorithm of Fig. 1, distinctive standard analyses (factual examination, uncertainty test, and sensibility assessment) are performed on the standard as well as hyperspectral imaginaries. The orginal images are taken from the 'signal and image processing institute (SIPI) database [50]. In order to validate the perposed scheme, we performed few trials on another satellite acquired in terms of the number of rounds by keeping key length constant (See Table 1 and Fig. 6). As seen even after encryption of satellite images with maximum rounds and having a different key length, some patches exist in encrypted images reflects the weakness of the blowfish algorithm for satellite imagery (see Fig. 5).

We encrypt a satellite images given in Fig. 6 with our modified Bowfish encryption algorithm that shows desirous encrypted image along with the flat histograms which is one of the vital element of any robust encryption scheme. The performance results for the Fig. 2 depicted in Table 2. It is quite evident from the numerical investigation of our obtained results available in Table 2 that antipated encryption mechanism gives reasonably good encryption strength (Figs. 3, 4 and 5).

Table 1 Security measurements for standard Blowfish algorithm for a satellite image of size 1028 × 766

Entropy	Max key length	Max encryption rounds
7.9794	64 Bits	16
7.9801	128 Bits	16
7.9567	192 Bits	16
7.9806	256 Bits	16
7.9653	320 Bits	16
7.9651	384 Bits	16

4.1 Histograms uniformity analysis

To measure the security strength of enciphered images, histograms consistency is the most important parameter to perform [24]. We computed enciphered image histrogram which are independently processed by the blowfish algorithm at different rounds, later on, the hybrid solution of chaos and blowfish will be tested. A 256 color level images of size 1026 × 765 and 1028 × 766 having varied ingredients experimented in Figs. 6, 7 and 8. Plain image histograms of Figs. 6, 7 and 8 occur with extremely sharp rising and decreasing shapes but in case of ciphered images (which are processed at different rounds of Blowfish), the histograms are not strongly uniformed but look much better compared to the histograms of the plain images. These type of histograms which are not flat enough even after the ciphering process, make some attacks a bit easier to recover the hidden information. On the other hand, a chaotic enciphered histogram makes this thing almost impossible to recover the original digital contents (Fig. 7).

We have examined the plain and enciphered images and found the consequences of the enciphered contents of Figs. 7, 8, 9 and 10 follow the consistency, which indicates the factual assaults hard.

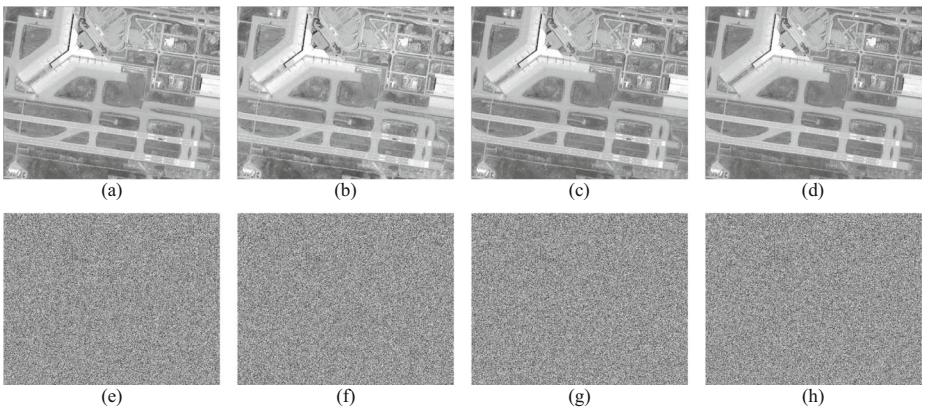


Fig. 2 Plain and enciphered hyperspectral imaginary. **a-d** Plain hyperspectral imaginary at a gray level and corresponding layers, **e-h** Enciphered hyperspectral imaginary at a gray level and corresponding layers

Table 2 Statisitical analyses at grayscale of Hyperspectral image of Fig. 2

Content	Entropy	Correlation			Gray level co-occurrence matrix		
		Horizontal	Vertical	Diagonal	Contrast	Homogeneity	Energy
Plain	7.2281	0.96719	0.964654	0.9373792	251.312765	0.182389	0.019005
Enciphered	7.9993	−0.005148	0.008568	0.000950671	11,001.4961	0.012479	0.004524

4.2 Randomness analysis

The most prominent feature to measure the randomness in enciphered information are entropy and NIST analyses [4, 40]. Entropy is characterized as follows:

$$H = -\sum_{i=0}^{2^N-1} p(x_i)\log_2 p(x_i), \tag{1}$$

where x_i is the pixel of an image (whether plain or encrypted) and $2^N$is all samples numbers. For the perfect indiscrimination of the digital information, the Shannon entropy should be 8 for 8-bit digital contents. Entropy readings the satellite acquired images of Fig. 11 in their plain and enciphered form are accounted in Table 3, whereas the results of standard RGB images accounted in Table 4. By achieving the randmonmess in encryption mechanism is one of the fundamental criteira which can be achived through entropy metric which is given in Tables 3 and 4 respectively. The comparative investigations of Table 4 clearly elucidates the effectiveness of our suggested encryption over digital medium. Our proposed digital privacy mechanism has high entropy values shows that there is no leakages in digital images with hight degree of randomness.

The proposed structure results in Table 4 have a predominant effect over and the existing techniques and legitimately close to the perfect estimation of Shannon entropy. These results clarify the release of data inconsequential and the structure of Fig. 1 is secured upon entropy assaults.

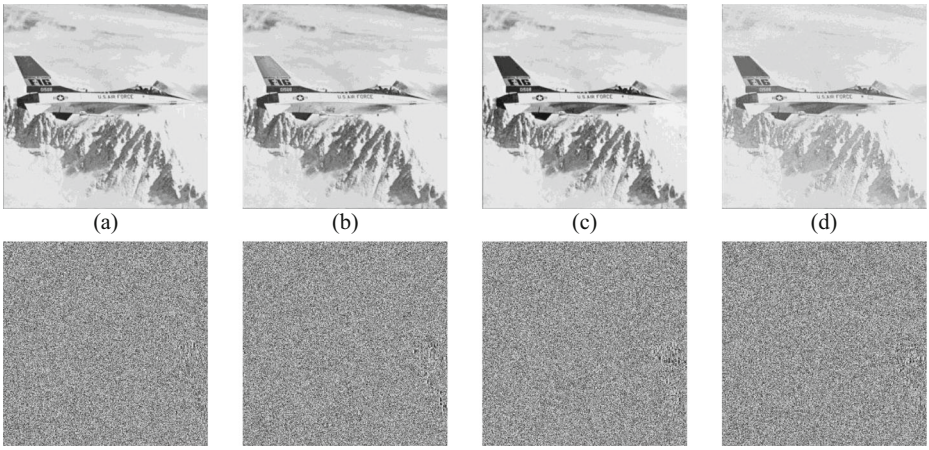


Fig. 3 Plain and enciphered Airplane images. **a**-**d** Plain Airplane image at a gray level and corresponding layers, **e**-**h** Enciphered Airplane image at a gray level and corresponding layers

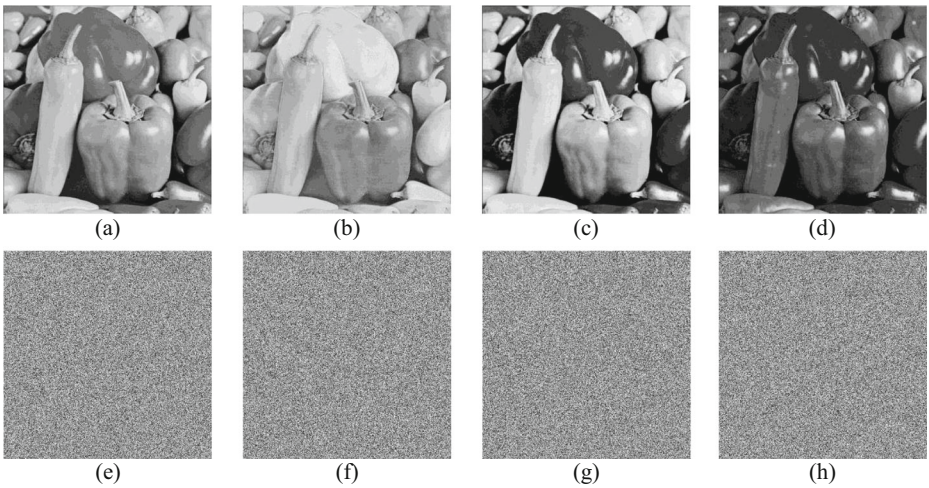


Fig. 4 Plain and enciphered Pepper images. **a**-**d** Plain Pepper image at a gray level and corresponding layers, **e**-**h** Enciphered Pepper image at a gray level and corresponding layers

4.3 NIST (SP 800–22)

Evaluating security in a ciphered image for a certain algorithm, we need to consider extraordinary complex image structure, identical delivery, extensive period, and efficiency. With the agenda of these parameters for the crucial test of a cipher, we perform the NIST (National Institute of Standards and Technology) suite over the encrypted data [16, 21]. we performed the NIST (SP 800–22) test to analyze the randomness created in digital content by the blowfish scheme. The numerical values of all randomness measurements are given in Table 5 which was proposed by NIST as a benchmakrs. According to NIST criteria, the numerical values of

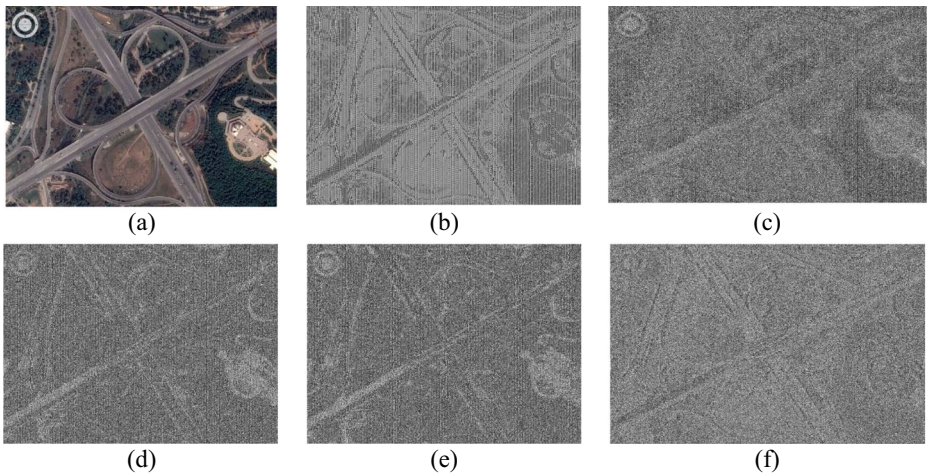


Fig. 5 Proposed chaos-based encryption algorithm with variable key lengths and a fixed number of rounds. **a** Plain satellite image, **b** Encrypted image with two rounds and key length 384 bits, **c** Encrypted image with four rounds and key length 384 bits, **d** Encrypted image with eight rounds and key length 384 bits, **e** Encrypted image with ten rounds and key length 384 bits, **f** Encrypted image with twelve rounds and key length 384 bits

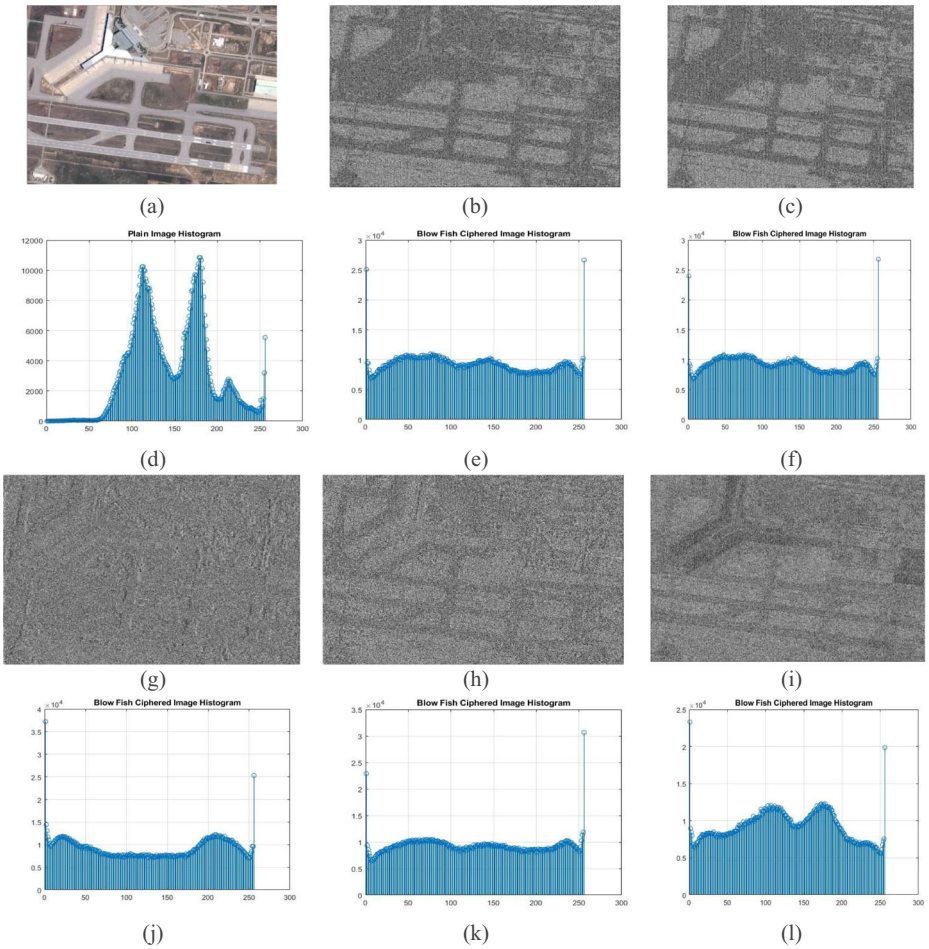


Fig. 6 Blowfish ciphered satellite image with random key lengths. **a** Plain satellite image, **b**-**c**, **g**-**i** Encrypted images with sixteen rounds and key lengths of 64 bits, 128 bits, 192 bits, 256 bits, and 320 bits, **d** Histogram analysis of plain image, **e**-**f**, **j**-**l** Histogram analysis of encrypted images with sixteen rounds and key lengths of 64 bits, 128 bits, 192 bits, 256 bits, and 320 bits

all measurments must be greater than 0.01 in order to pass this criteria effectively. Our suggested scheme confidently passed all the existing standard randomness metrics of NIST.

4.4 Correlation coefficient analysis

Correlation analysis is an extensive study to evaluate the connection between the plain and the corresponding encrypted image [5, 9]. This analysis also highlights the capability of the proposed encryption scheme in terms of the utmost content changing of the input information. The correlation between two different data sets (plain image data set and corresponding encrypted image at different rounds of Blowfish) evaluated horizontally, vertically, and diagonally adjacent pixels as shown in Figs. 11, 12, 13 and 14.

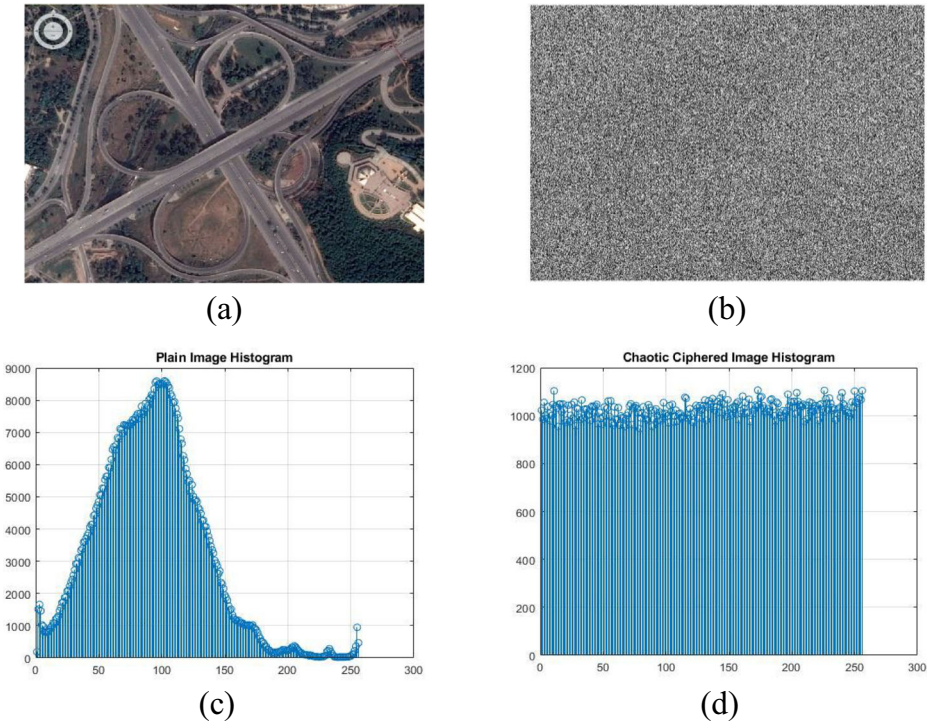


Fig. 7 Histogram analysis of proposed hybrid chaos-based blowfish encryption algorithm with two rounds for satellite images

$$r_{xy} = \frac{\sigma_{xy}}{\sqrt{{\sigma_x}^2 {\sigma_y}^2}}, \tag{2}$$

where $y$and x are the adjacent pixel values at grayscale, $\sigma_y^2$and σ_x^2 are the variances, and σ_{xy} is the covariance of random variables x and y.

We have calculated the numerous encrypted and plain pairs of the image by estimating their two dimensional coefficients of correlation with the following expression:

$$r = \frac{\sum_{i,j=1}^{M,N} \left(P_{ij} - \overline{P}\right)\left(C_{ij} - \overline{C}\right)}{\sqrt{\left(\sum_{i,j=1}^{M,N} \left(P_{ij} - \overline{P}\right)^2\right)\left(\sum_{i,j=1}^{M,N} \left(C_{ij} - \overline{C}\right)^2\right)}}, \tag{3}$$

where $C$and $P$are the plain and encrypted contents with their mean approximations are $\overline{C}$and $\overline{P}$, and M, N are the height and width of the content respectively. The corresponding coefficients for the original and encoded contents for the foreseen structure of Fig. 1 and their evaluations with the most recent strategy portrayed in Tables 6.

Table 6 indicates the coefficients of pixels' affiliation at grayscale, which are exceptionally near zero and has better outcomes over the most recent approach.

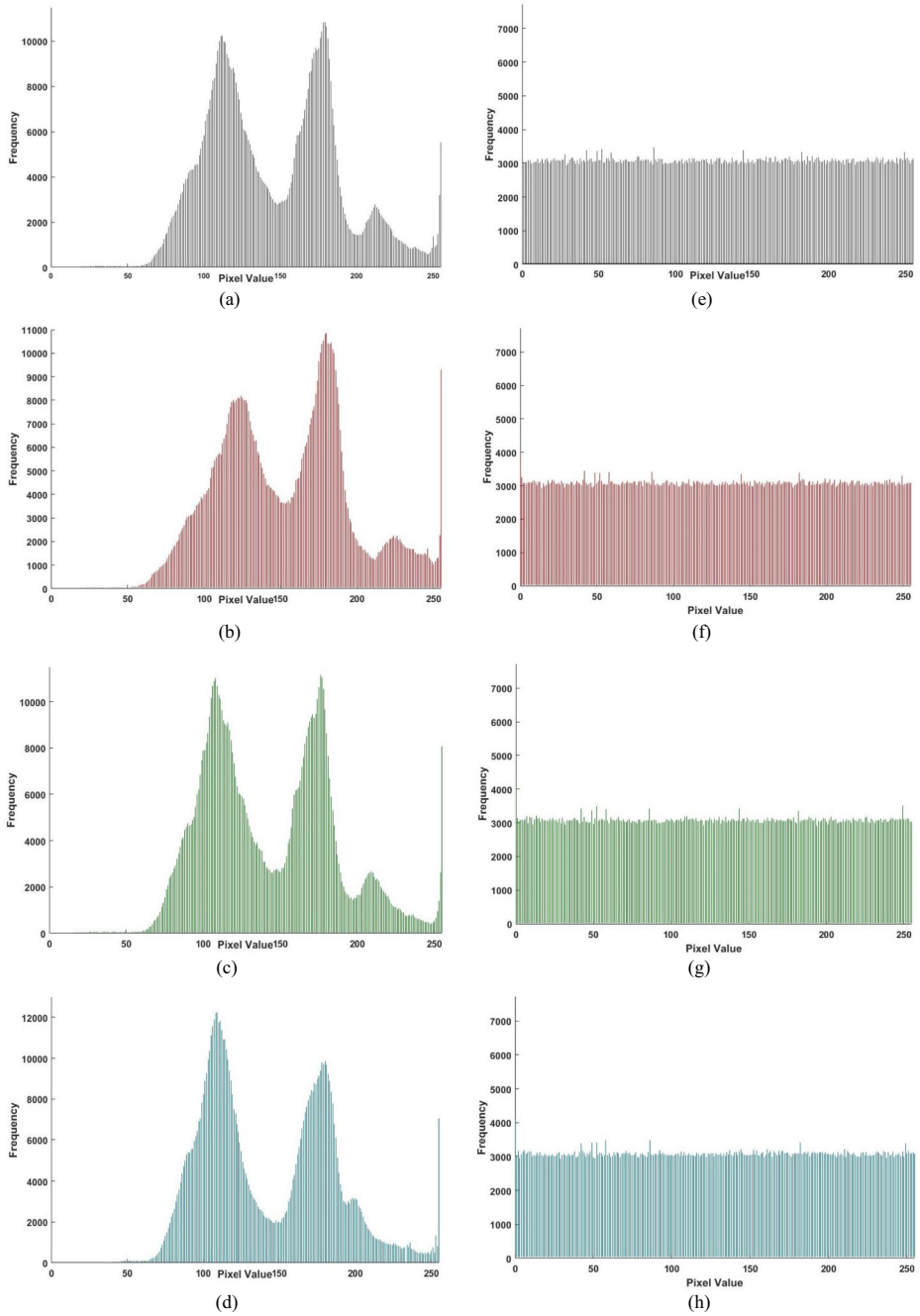


Fig. 8 Histograms of plain and enciphered hyperspectral images of Fig. 2 for the proposed hybrid chaos-based blowfish criteria with two rounds. **a**-**d** Pain images histograms at gray and corresponding three scales, **e**-**h** Encrypted images histograms at gray and corresponding three scales

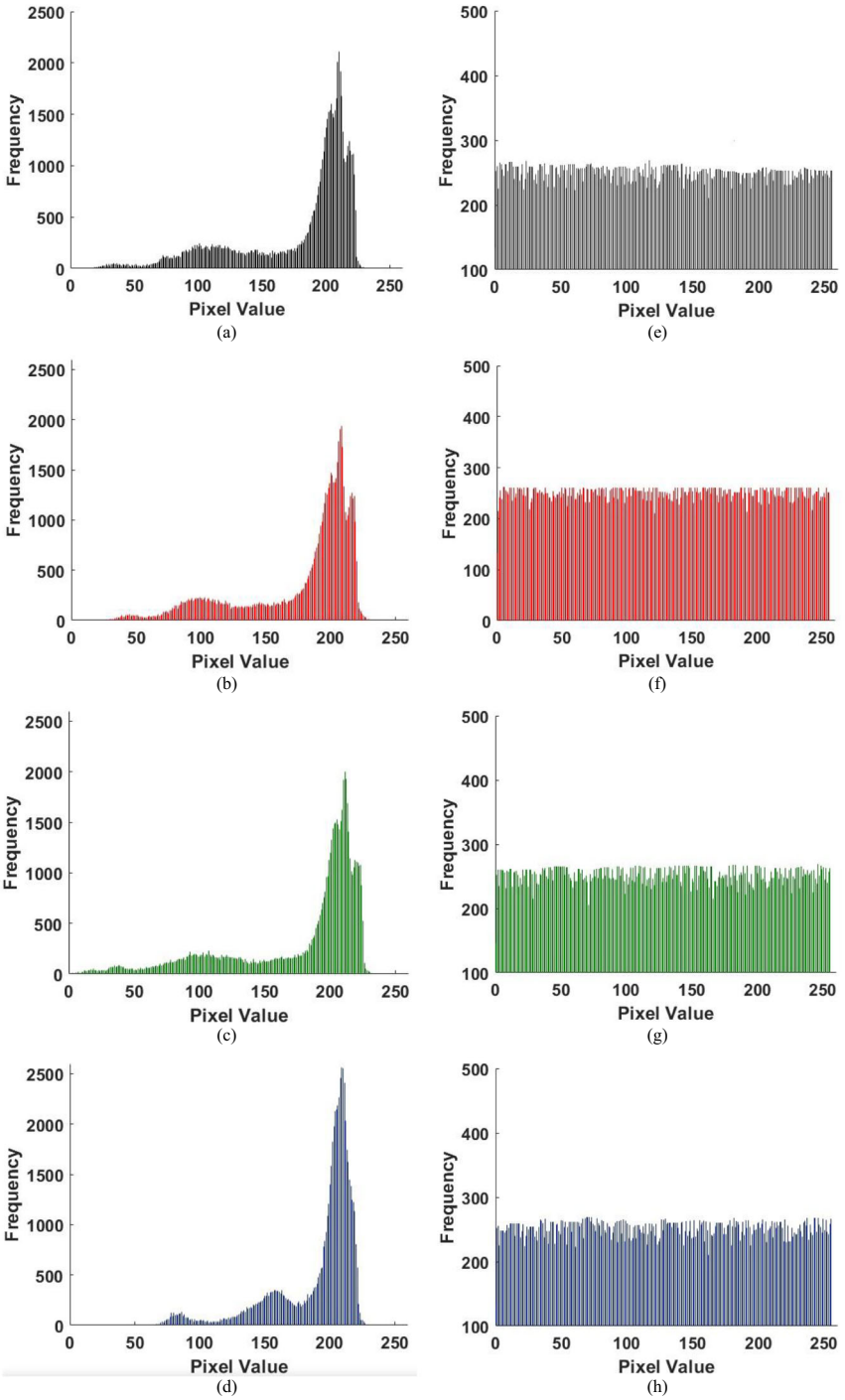


Fig. 9 Histograms of plain and enciphered Airplane images of Fig. 3 for the proposed hybrid chaos-based blowfish criteria with two rounds. **a**-**d** Pain images histograms at gray and corresponding three scales, **e**-**h** Encrypted images histograms at gray and corresponding three scales

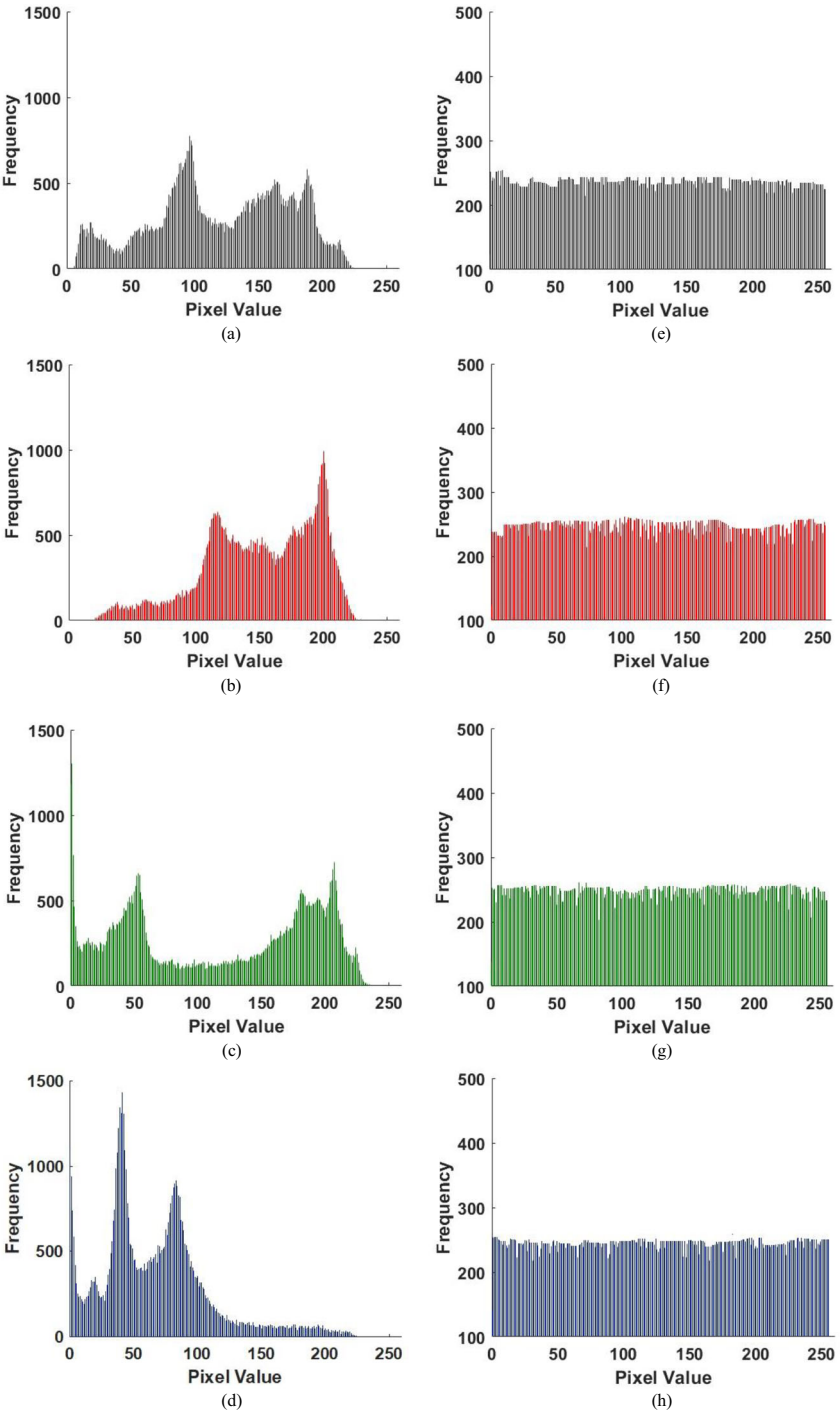
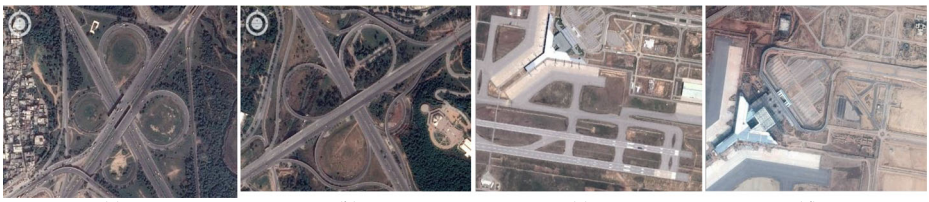


Fig. 10 Histograms of plain and enciphered Pepper images of Fig. 4 for the proposed hybrid chaos-based blowfish criteria with two rounds. **a**-**d** Pain images histograms at gray and corresponding three scales, **e**-**h** Encrypted images histograms at gray and corresponding three scales



(a) (b) (c) (d)

Fig. 11 Satellite acquired images for experimentation of our proposed encryption scheme

4.5 Pixels' similarity analyses

The resemblance of digital contents in an image (plain or encrypted) can be exposed by performing similarity analyses. We have evaluated the structural content (SC), structure similarity index measure (SSIM) and normalized cross-correlation (NCC) to observe the variation in structure between the plain and enciphered contents [15, 35]. The NC mearse correlation between resemblance and traces, whereas SC regulates the noise level and sharpness, and SSIM relates the luminance, divergence and assembly among the encrypted and plain contents. The utmost resemblance value of the adjacent pixels in an image may approach 1, and the extreme dissimilarity with neighboring contents will generate the similarity reading approaching to 0. While doing similarity analysis our prime agenda is to investigate the different similarity measures which may occur between cipher $C_{i,j}$ and plain $P_{i,j}$ images to approximate the structural dissimilarity after encryption. These analyses are deliberated in Table 7 by using the following expressions.

$$SSIM = \frac{\left(2\mu_p\mu_c + C_1\right)\left(2\sigma_{pc} + C_2\right)}{\left(\mu_p^2 + \mu_c^2 + C_1\right)\left(\sigma_p^2 + \sigma_c^2 + C_2\right)}, \tag{4}$$

$$NCC = \sum_{k=0}^{M-1}\sum_{l=0}^{N-1} \frac{P_{k,l} \times C_{k,l}}{\sum_{k=0}^{M-1}\sum_{l=0}^{N-1} P^2{}_{k,l}}, \tag{5}$$

Table 3 Randomness analysis of the proposed image encryption scheme for satellite imagery

Rounds	Plain satellite imagery				Encrypted satellite imagery			
	Image 1 7.2291	Image 2 7.2789	Image 3 7.2281	Image 4 7.2963	Image 1 –	Image 2 –	Image 3 –	Image 4 –
2	–	–	–	–	7.9617	7.9761	7.9794	7.9778
4	–	–	–	–	7.9563	7.9598	7.9801	7.9681
6	–	–	–	–	7.9653	7.9625	7.9567	7.9627
8	–	–	–	–	7.9727	7.9779	7.9806	7.9801
10	–	–	–	–	7.9661	7.9627	7.9653	7.9577
12	–	–	–	–	7.9523	7.9839	7.9651	7.9534

Table 4 Entropy analysis of plain and enciphered contents and its comparative analysis with existing encryption scheme

Images	Color componets	Plain image	Enciphered	Ref. [49]
Pepper	Red	7.3516	7.9991	7.9984
	Green	7.5812	7.9993	7.9983
	Blue	7.1347	7.9993	7.9984
	Gray	7.5889	7.9994	7.9986
Airplane	Red	6.7489	7.9988	7.9984
	Green	6.8106	7.9990	7.9987
	Blue	6.2682	7.9991	7.9981
	Gray	6.7056	7.9989	7.9986
Baboon	Red	7.7444	7.9989	7.9986
	Green	7.4493	7.9991	7.9985
	Blue	7.7513	7.9994	7.9982
	Gray	7.3485	7.9992	7.9984
Lena	Red	7.2531	7.9991	7.9981
	Green	7.5940	7.9992	7.9983
	Blue	6.9684	7.9992	7.9974
	Gray	7.4451	7.9994	7.9987
Sailboat	Red	7.3166	7.9988	7.9984
	Green	7.6443	7.9992	7.9983
	Blue	7.3030	7.9990	7.9984
	Gray	7.4939	7.9989	7.9986

Table 5 NIST analysis for encrypted satellite image in 10-b with multiple rounds

Test		Maximum encryption rounds					Remarks
		2	4	6	8	10	
Frequency		0.70434	0.22949	0.09373	0.00112	0.94957	Pass
Block frequency		0.85115	0.31871	0.52221	0.32216	0.87424	Pass
Rank		0.29191	0.29191	0.29191	0.29191	0.29191	Pass
Runs (M = 10,000)		0.59242	0.0.3805	0.28772	0.23688	0.13719	Pass
Long runs of ones		0.7127	0.7127	0.7127	0.7127	0.7127	Pass
Overlapping template		0.81656	0.85988	0.85988	0.85988	0.85988	Pass
Spectral DFT		0.19161	0.88464	0.30979	0.1916	0.38399	Pass
Approximate entropy		0.67177	0.2278	0.77957	0.03918	0.67888	Pass
Universal		0.98958	0.98893	0.99312	0.97715	0.99237	Pass
Serial	*p values 1*	0.04680	0.3114	0.00804	0.50326	0.42669	Pass
Serial	*p values 2*	0.00676	0.66153	0.15727	0.02238	0.85506	Pass
Cumulative sums forward		0.24091	0.15801	0.0.0399	0.72955	0.2423	Pass
Cumulative sums reverse		0.82313	0.09619	1.8054	1.4415	1.0152	Pass
Random excursions	$X=-3$	0.57589	0.72881	0.6029	0.98523	0.17959	Pass
	$X=-2$	0.81216	0.63321	0.65601	0.37693	0.28296	Pass
	$X=-1$	0.98276	0.69637	0.7373	0.95053	0.11161	Pass
	$X=1$	0.89889	0.22396	0.14868	0.87691	0.79704	Pass
	$X=2$	0.20748	0.77752	0.02251	0.37693	0.53961	Pass
	$X=3$	0.07443	0.90922	0.21883	0.98523	0.16416	Pass
Random excursions variants	$X=-3$	0.4795	0.50965	0.41422	0.52709	0.40246	Pass
	$X=-2$	0.36131	0.60952	0.39908	0.41422	0.44689	Pass
	$X=-1$	0.59816	0.46933	0.14413	0.28884	0.83522	Pass
	$X=1$	0.52709	0.0.3763	0.36131	0.59682	0.5791	Pass
	$X=2$	0.58388	0.17319	0.4606	0.83826	0.74877	Pass
	$X=3$	0.88754	0.0.2623	0.14164	0.63526	0.92588	Pass

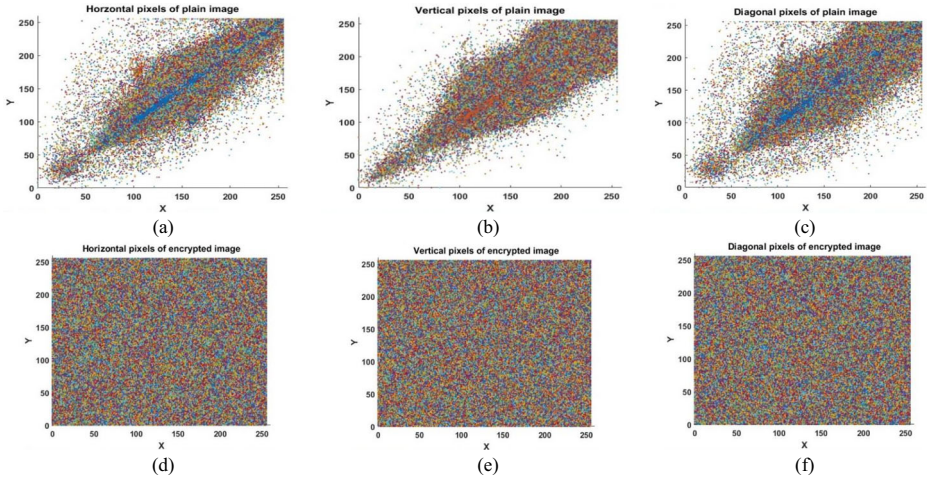


Fig. 12 Plain and enciphered grayscale images of Fig. 2 at 8th round correlation analyses for the pixels' pairs in horizontal, vertical, and diagonal orders. **a-c** Plain hyperspectral imaginary analyses, **d-f** Enciphered hyperspectral imaginary analyses

$$SC = \sum_{k=0}^{M-1} \sum_{l=0}^{N-1} \frac{{P_{k,l}}^2}{\sum_{k=0}^{M-1} \sum_{l=0}^{N-1} {C^2}_{k,l}}. \tag{6}$$

The plain and enciphered contents specified by $P_{k,\,l}$ and $C_{k,\,l}$, the standard deviation is $\sigma_{p\,c}$ and mean values are $\mu_c$and μ_p. The SSIM, SC, and NCC esteem approaches 1 if there are numerous traces of associations or structural resemblance found between the contents. The

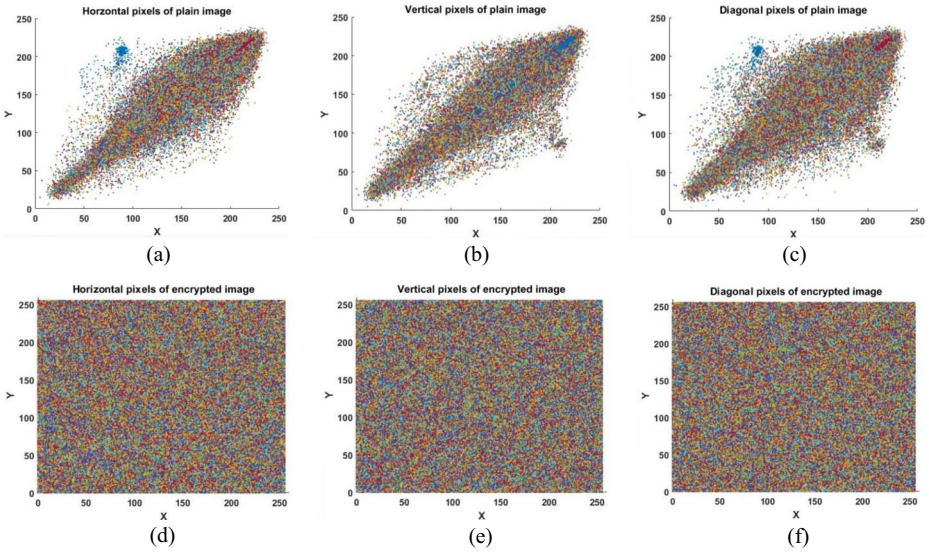


Fig. 13 Plain and enciphered grayscale images of Fig. 3 at 8th round correlation analyses for the pixels' pairs in horizontal, vertical, and diagonal orders. **a-c** Plain Airplane image analyses, **d-f** Enciphered Airplane image analyses

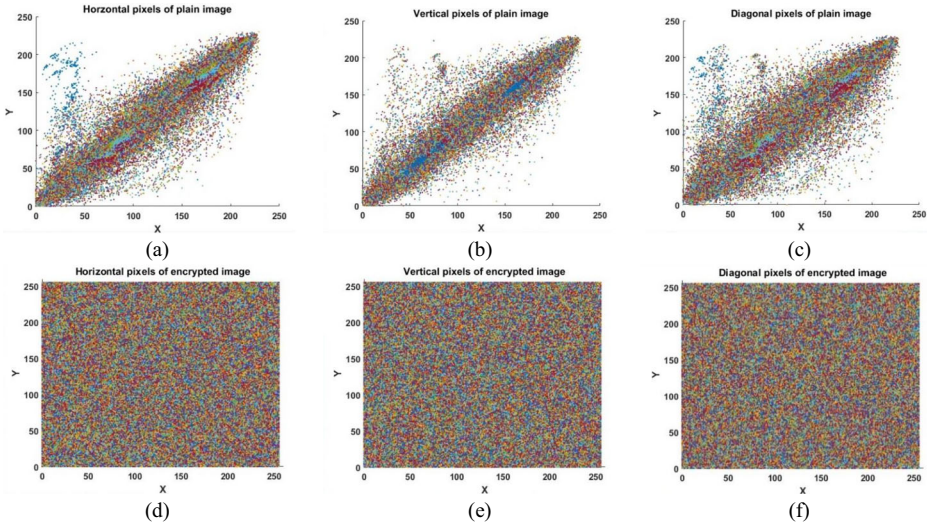


Fig. 14 Plain and enciphered grayscale images of Fig. 4 at 8th round correlation analyses for the pixels' pairs in horizontal, vertical, and diagonal orders. **a**-**c** Plain Pepper image analyses, **d**-**f** Enciphered Pepper image analyses

similarity evaluations for the plain-encoded contents with the foreseen structure of Fig. 1 and their valuations with the most recent approaches outlined in Tables 7 and 8.

4.6 Pixels' difference analyses

To assess the error in digital contents, we evaluate mean square error (MSE), peak signal to noise ratio (PSNR) and mean absolute error (MAE) [29, 44]. The deviation of encrypted contents concerning the plain contents and the accuracy of interminable variables are evaluated here by MAE. The prominence of the encoded contents can be quantified by MSE and PSNR. Smaller the MSE esteem concerning PSNR identifies the similarity between the contents. The evaluations of these investigations examined here by assessing the succeeding expressions:

Table 6 Coefficients of Pixels' association for the plain and enciphered contents at grayscale, and their analyses with the most existing approach

Image	Plain			Enciphered contents			Ref. [11]		
	H	V	D	H	V	D	H	V	D
Pepper	0.9812	0.9662	0.9832	−0.0052	−0.0005	−0.0057	−0.0115	−0.0032	0.0036
Airplane	0.9672	0.9647	0.9374	−0.0051	0.0086	0.0010	−0.0127	−0.0172	−0.0038
Baboon	0.8621	0.7653	0.7614	0.0071	−0.0035	−0.0047	0.0131	0.0139	−0.0141
Lena	0.9685	0.9798	0.9621	−0.0063	−0.0038	0.0017	0.0031	−0.0122	0.0039
Sailboat	0.9526	0.9803	0.9589	0.0013	0.0025	−0.0051	0.0011	−0.0119	0.0106

Table 7 Pixels' similarity analysis for the satellite image in Fig. 8b

Rounds	Proposed scheme		
	SSIM	NCC	SC
2	0.9853	0.7247	1.3327
4	0.9868	0.8016	1.1977
6	0.9861	0.8111	1.1469
8	0.9665	0.7415	1.3224
10	0.9841	0.8076	1.1473
12	0.9863	0.6720	1.4636

$$MAE = \frac{1}{M \times N} \sum_{k=0}^{M-1} \sum_{l=0}^{N-1} \left| P_{k,l} - C_{k,l} \right|, \tag{7}$$

$$MSE = \frac{\sum_{k=1}^{M} \sum_{l=1}^{N} \left(P_{k\,l} - C_{k\,l} \right)^2}{M \times N}, \tag{8}$$

$$\mathrm{PSNR} = 20 \log_{10} \left[\frac{I_{MAX}}{RMSE} \right], \tag{9}$$

where $P_{k,l}$ and $C_{k,l}$ are the pixels' location for the plain and encoded contents at k^{th} row and l^{th} column respectively, and I_{MAX} is the estimation of the maximum conceivable pixel of the digital content.

The quality of encryption for the digital content can be improved by more prominent the MSE regard and flat the PSNR, or vice-versa [27]. These error assessments are displayed in Table 9 for the attainability of the anticipated plan on standard digital content.

4.7 Differential assaults analysis

To measure differential assault for a certain image encryption scheme, we require the alteration impact of a solo pixel in a plain image and overall enciphered image for calculating two parameters namely.

Table 8 Pixels based similarity examinations for the plain-enciphered contents, and their assessments with most recent methodologies

Image	Pixels' congruity analyses			Ref. [10]			Ref. [8]		
	SSIM	SC	NCC	SSIM	SC	NCC	SSIM	SC	NCC
Pepper	0.010165	0.7949	0.8854	0.016996	0.8042	0.8360	0.0070	0.2932	1.3265
Airplane	0.009621	1.5831	0.6642	0.012219	0.7126	0.8819	0.0094	1.7005	0.6538
Baboon	0.009193	0.8576	0.9126	0.014385	0.8353	0.8681	0.0101	0.7696	0.8620
Lena	0.010526	0.7247	0.8995	0.023086	0.8179	0.87005	–	–	–
Sailboat	0.008716	0.9624	0.7271	0.023646	0.8057	0.8553	0.0087	0.8843	0.7597

Table 9 Analyzation of pixels discrepancy for the plain-enciphered images, and their assessments with most recent approaches

Image	Discrepancy analyses			Ref. [6]			Ref. [3]		
	MAE	MSE	PSNR	MAE	MSE	PSNR	MAE	MSE	PSNR
Pepper	75.739	8457.6	8.8923	81.37	8356.7	8.8865	82.14	8626.15	8.9328
Airplane	83.369	10,392.2	7.9979	88.14	8870.2	8.8815	79.88	8812.58	8.8667
Baboon	79.286	9664.7	8.2432	78.49	8918.7	8.9365	81.28	8942.21	8.7982
Lena	77.914	10,174.2	7.9753	82.54	8654.6	8.8921	75.91	8588.39	8.9152
Sailboat	82.628	9842.8	8.1783	83.48	8125.3	8.9984	84.62	8462.57	8.8217

- Number of Pixels Change Rate (NPCR)
- Unified Average Intensity (UACI)

The NPCR and UACI for two ciphered images $C_1(i,j)$ and $C_2(i,j)$ can be assessed by the following expressions are given below:

$$\mathrm{NPCR} = \frac{1}{W \times H} \sum_{i,j} x(i,j), \tag{13}$$

where $x(i,j) = \begin{cases} 0, & C_1(i,j) = C_2(i,j) \\ 1, & C_1(i,j) \neq C_2(i,j) \end{cases}$.

$$UACI = \frac{1}{W \times H} \sum_{i=0}^{M-1} \sum_{j=0}^{N-1} \left| \frac{C_1(i,j) - C_2(i,j)}{255} \right|. \tag{14}$$

In order to understand the plain image sensitivity, we cipher it first and then alter one pixel randomly [30, 31, 52]. Tables 10, 11 and 12 presents the aforementioned assessments. The values of NPCR and UACI are quite closed to standard estimates which shows that our encryption mechanism rubost agains plaintext sensitivity attacks (see Table 11). The small change two plain image with one pixel change and encrypting these plain images results statistically different images is clearly relecting from the close examination of Tables 10, 11 and 12. These plaintext sensitivity is one

Table 10 NPCR and UACI analyses for the enciphered results of satellite images in Figs. 14 (a-d) for multiple rounds

Max rounds	NPCR				UACI			
	Image 14(a)	Image 14(b)	Image 14(c)	Image 14(d)	Image 14(a)	Image 14(b)	Image 14(c)	Image 14(d)
2	1.0527	1.0568	9.9201	9.9600	4.1654	0.2895	0.6395	0.5415
4	1.0527	1.0568	9.9201	9.9600	4.5908	2.0736	1.8496	2.7273
6	1.0527	1.0568	9.9201	9.9600	4.2862	3.0788	3.1237	2.1316
8	1.0527	1.0568	9.9201	9.9600	1.3762	2.4893	1.8939	1.8116
10	1.0527	1.0568	9.9201	9.9600	2.8890	1.9788	1.8792	2.7519
12	1.0527	1.0568	9.9201	9.9600	3.8397	2.1572	2.7843	2.1070

Table 11 NPCR and UACI outcomes for encoded contents, and their assessments with most recent approaches

Image	Proposed scheme outcomes		Ref. [10]		Ref. [48]	
	NPCR	UACI	NPCR	UACI	NPCR	UACI
Pepper	99.6078	29.7017	99.53	28.21	–	–
Airplane	99.6093	32.6937	99.64	30.31	–	–
Baboon	99.6182	33.1104	99.61	30.41	99.52	33.01
Lena	99.6098	32.9168	99.42	31.71	99.53	33.07
Sailboat	99.5993	31.5853	99.32	31.88	–	–

of the important aspect of any robust encryption tool which is achived through these two measuments namely NPCR and UACI for suggested scheme (See Tables 10, 11).

5 Conclusion and future recommendations

We have deviced a new digital information confidentialy scheme for different digital mediums namely satellite images and standard color images with three bands. The new anticipated scheme utilized two different chaotic dynamical systems which are responsible for creating confusion capabiittes at layers level in standard and satellite images. Morover, these chaotic dynamical systems are further joined with standard blowfish algorithm which reduce the computational cost and adding more confusuion and diffusion charactetisics in our proposed mechanism. With this simple and ronust combination we have reduced the rounds of standard fiestal based ciper. The proposed mechanism can also be implemented in a real roposed mechanism. With this simple and ronust combination we have reduced the rounds of standard fiestal based ciper. The proposed mechanism can also be implemented in a real time audio and video streams with its lightweight version due to evolution of new emerging idea of internet of thing (IoTs).

Declarations

Conflict of interest It is declared that we have no conflict concerning the publication of this article.

References

1. Abd Ulkareem Nasser M, Abduljaleel IQ (2013) Speech encryption using chaotic map and blowfish algorithms. J Basrah Res (Sciences) 39(2A):68–76
2. Ahmad R, Manaf AA, Ismail W (2016) Implementation of a high-performance blowfish for secure wireless communication. J Telecom Electronic Comput Eng (JTEC) 8(6):147–151
3. Alghafis A, Waseem HM, Khan M (2019) A hybrid cryptosystem for digital contents confidentiality based on rotation of quantum spin states. Physica A: Statistical Mechanics and its Applications:123908
4. Alghafis A, Munir N, Khan M, Hussain I (2020) An encryption scheme based on discrete quantum map and continuous chaotic system. Int J Theor Phys:1–14
5. Alghafis A, Firdousi F, Khan M, Batool SI, Amin M (2020) An efficient image encryption scheme based on chaotic and deoxyribonucleic acid sequencing. Math Comput Simul 177:441–466
6. Alghafis A, Waseem HM, Khan M, Jamal SS, Amin M, Batool SI (2020) A novel digital contents privacy scheme based on quantum harmonic oscillator and schrodinger paradox. Wireless Networks

7. Ali KM, Khan M (2019) Application based construction and optimization of substitution boxes over 2D mixed chaotic maps. Int J Theor Phys 58(9):3091–3117
8. Arshad U, Batool SI, Amin M (2019) A novel image encryption scheme based on Walsh compressed quantum spinning chaotic Lorenz system. Int J Theor Phys 58(10):3565–3588
9. Arshad U, Khan M, Shaukat S, Amin M, Shah T (2020) An efficient image privacy scheme based on nonlinear chaotic system and linear canonical transformation. Physica A: Statistical Mechanics and its Applications 546:123458
10. Batool SI, Waseem HM (2019) A novel image encryption scheme based on Arnold scrambling and Lucas series. Multimed Tools Appl 78(19):27611–27637
11. Batool SI, Amin M, Waseem HM (2020) Public key digital contents confidentiality scheme based on quantum spin and finite state automation. Physica A: Statistical Mechanics and its Applications 537:122677
12. Blömer J, Seifert JP (2003, January). Fault based cryptanalysis of the advanced encryption standard (AES). In International Conference on Financial Cryptography (pp. 162-181). Springer, Berlin, Heidelberg.
13. Bulgurcu B, Cavusoglu H, Benbasat I (2010) Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. MIS Q 34(3):523–548
14. Buscarino A, Fortuna L, Frasca M, Sciuto G (2014) A concise guide to chaotic electronic circuits. Springer International Publishing, Heidelberg, Germany
15. Çataltaş Ö, Tütüncü K (2017, September) Comparison of LSB image steganography technique in different color spaces. In 2017 international artificial intelligence and data processing symposium (IDAP) (pp. 1-6). IEEE.
16. Çavuşoğlu Ü, Kaçar S, Pehlivan I, Zengin A (2017) Secure image encryption algorithm design using a novel chaos based S-box. Chaos, Solitons Fractals 95:92–101
17. Coppersmith D (1994) The data encryption standard (DES) and its strength against attacks. IBM J Res Dev 38(3):243–250
18. Erdmann D, Murphy S (1992) Hénon stream cipher. Electron Lett 28(9):893–895
19. Fridrich J (1998) Symmetric ciphers based on two-dimensional chaotic maps. Int J Bifurc Chaos 8(06): 1259–1284
20. Guo JI (2000, May). A new chaotic key-based design for image encryption and decryption. In 2000 IEEE International Symposium on Circuits and Systems (ISCAS) (Vol. 4, pp. 49-52). IEEE.
21. Hamza R (2017) A novel pseudo random sequence generator for image-cryptographic applications. J Inform Secur Appl 35:119–127
22. Jawad LM, Sulong G (2015) Chaotic map-embedded blowfish algorithm for security enhancement of colour image encryption. Nonlinear Dynamics 81(4):2079–2093
23. Khan M, Shah T (2014) A novel image encryption technique based on Hénon chaotic map and S 8 symmetric group. Neural Comput & Applic 25(7–8):1717–1722
24. Khan M, Waseem HM (2018) A novel image encryption scheme based on quantum dynamical spinning and rotations. PLoS One 13(11):e0206460
25. Khan M, Waseem HM (2019) A novel digital contents privacy scheme based on Kramer's arbitrary spin. Int J Theor Phys 58(8):2720–2743
26. Khan M, Masood F, Alghafis A, Amin M, Batool Naqvi SI (2019) A novel image encryption technique using hybrid method of discrete dynamical chaotic maps and Brownian motion. PLoS One 14(12): e0225031
27. Khan M, Hussain I, Jamal SS, Amin M (2019) A privacy scheme for digital images based on quantum particles. Int J Theor Phys 58(12):4293–4310
28. Krishnamurthy GN, Ramaswamy V (2010) Encryption quality analysis and security evaluation of CAST-128 algorithm and its modified version using digital images. arXiv preprint arXiv:1004.0571.
29. Lee CS, Kuo YH, Yu PT (1997) Weighted fuzzy mean filters for image processing. Fuzzy Sets Syst 89(2): 157–180
30. Liao X, Lai S, Zhou Q (2010) A novel image encryption algorithm based on self-adaptive wave transmission. Signal Process 90(9):2714–2722
31. Liu H, Wang X (2010) Color image encryption based on one-time keys and robust chaotic maps. Comput Math Appl 59(10):3320–3327
32. Mousa A (2005, June) Data encryption performance based on blowfish. In 47th International Symposium ELMAR, 2005. (pp. 131-134). IEEE.
33. Nath A, Ghosh S, Mallick MA (2010, July) Symmetric key cryptography using random key generator. In Security and Management (pp. 234-242).
34. Nie T, Zhang T (2009, January) A study of DES and blowfish encryption algorithm. In Tencon 2009-2009 IEEE Region 10 Conference (pp. 1-4). IEEE.
35. Pal K, Ghosh G, Koley S, Bhattacharya M (2013, December) A new combined crypto-watermarking technique using RSA algorithm and discrete cosine transform to retrieve embedded EPR from noisy bio-

medical images. In 2013 IEEE 1st International Conference on Condition Assessment Techniques in Electrical Systems (CATCON) (pp. 368-373). IEEE.
36. Prasetyo KN, Purwanto Y, Darlis D (2014, May) An implementation of data encryption for internet of things using blowfish algorithm on FPGA. In 2014 2nd International Conference on Information and Communication Technology (ICoICT) (pp. 75-79). IEEE.
37. Schneier B (1993, December) Description of a new variable-length key, 64-bit block cipher (blowfish). In International Workshop on Fast Software Encryption (pp. 191-204). Springer, Berlin, Heidelberg.
38. Shah T, Hussain I, Gondal MA, Mahmood H (2011) Statistical analysis of S-box in image encryption applications based on majority logic criterion. International Journal of Physical Sciences 6(16):4110–4127
39. Singh P, Singh K (2013) Image encryption and decryption using blowfish algorithm in MATLAB. Int J Sci Eng Res 4(7):150–154
40. Tariq S, Khan M, Alghafis A, Amin M (2020) A novel hybrid encryption scheme based on chaotic Lorenz system and logarithmic key generation. Multimed Tools Appl:1–23
41. Thakur J, Kumar N (2011) DES, AES and blowfish: symmetric key cryptography algorithms simulation based performance analysis. Int J Emerg Technol Adv Eng 1(2):6–12
42. Ueta T, Chen G (2000) Bifurcation analysis of Chen's equation. Int J Bifurc Chaos 10(08):1917–1931
43. Von Solms R, Van Niekerk J (2013) From information security to cyber security. Comput Secur 38:97–102
44. Wang Q, Gao J, Lin W, Yuan Y (2019) Learning from synthetic data for crowd counting in the wild. In Proceedings of the IEEE conference on computer vision and pattern recognition (pp. 8198-8207).
45. Wang X, Feng L, Zhao H (2019) Fast image encryption algorithm based on parallel computing system. Inf Sci 486:340–358
46. Waqas UA, Khan M, Batool SI (2020) A new watermarking scheme based on Daubechies wavelet and chaotic map for quick response code images. Multimed Tools Appl 79(9):6891–6914
47. Waseem HM, Khan M (2019) A new approach to digital content privacy using quantum spin and finite-state machine. Appl Phys B 125(2):27
48. Waseem HM, Khan M, Shah T (2018) Image privacy scheme using quantum spinning and rotation. J Electron Imag 27(6):063022
49. Waseem HM, Alghafis A, Khan M (2020) An efficient public key cryptosystem based on dihedral group and quantum spin states. IEEE Access 8:71821–71832
50. Weber A (1997) The USC-SIPI image database. Signal and Image Processing Institute of the University of Southern California. URL: http://sipi.usc.edu/services/database.
51. Whitman ME, Mattord HJ (2011). Principles of information security. Cengage Learning.
52. Wu Y, Noonan JP, Agaian S (2011) NPCR and UACI randomness tests for image encryption. Cyber journals: multidisciplinary journals in science and technology. J Selected Areas Telecomm (JSAT) 1(2):31–38
53. Yanling W (2009, March). Image scrambling method based on chaotic sequences and mapping. In 2009 First International Workshop on Education Technology and Computer Science (Vol. 3, pp. 453-457). IEEE.
54. Ye G (2010) Image scrambling encryption algorithm of pixel bit based on chaos map. Pattern Recogn Lett 31(5):347–354