Applied Physics B (2019) 125:27
https://doi.org/10.1007/s00340-019-7142-y

Applied Physics B
Lasers and Optics

A new approach to digital content privacy using quantum spin and finite-state machine

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

Received: 26 June 2018 / Accepted: 18 January 2019 / Published online: 28 January 2019

Abstract

Transmission of digital contents over public channel with access restricted to intended beneficiary even the contents are intercepted by others. In technological ages, cryptography plays a vital role in broadcasting, network communication, cell phones, etc. for transmitting sensitive information. The era of quantum information processing has many applications in daily life and one of its implications in data security. The data security and quantum information are two different modules of information processing that uses the notion of qubit model instead of classical information theory. It uses quantum mechanics instead of classical mechanics for information processing (covert communication). Elements of quantum theory have energy and angular momentum called spin, which carries the polarization. The purpose of writing this article is to introduce the concept spinning from quantum dynamics in data security, which leads to the development of quantum cryptography. The scope of this article is to protect contents' privacy by polarized spin matrices passed by finite-state machine at secret phase information.

1 Introduction

Propagation of communication over public channels becomes very much popular and ensures that authorized access is essential [1]. The rapid growth in multimedia technology, and digital contents such as images, video, audio, etc. play imperative role in communication [2]. To fulfill the privacy prerequisite of such contents, worthy security tools have to be developed [3]. The traditional number theory-based algorithms, such as AES and DES, projected for encryption, but these algorithms rely on higher computational power and time complexity, so these found to be not suitable for digital images. Images possess resistance and redundancy among neighboring pixels, which mark difficulties for number theory-based procedures to tackle the real-time protection performance due to necessity of high computational complexity. In literature review, AES is vulnerable to square, side-channel, and differential attacks [4].

Different algorithms have been developed in the literature to provide the security to digital contents based on confusion and diffusion with multiple rounds and chaos theory [5–17]. The idea of quantum computers evolves nowadays and it is a serious threat for classical number theory-based algorithms. The conventional communication is a fine submission of 0 or 1 through public channels and several algorithms [18–22, 23] have been proposed that prevent the leakage of information as well as provide defense against information attacks. These algorithms were considered to be secure as long as quantum computers not available publically. In the age of quantum information, the idea of fast computation with several complication levels gets more legalistic due to quantum parallelism. The performance of a single-quantum computing machine is much better than hundreds of classical computers perform operation parallel. Quantum parallelism is performed by spin operations of quantum mechanics and this leads to a new paradigm of computing. The cryptography of prime factorization will fall as the computational complexity resolved by quantum machines in m-seconds [24]. Thirty classical machines having CPU 2.2 Ghz perform parallel operations for a year to factor 193 digits, while a single-quantum computer with the same specification as classical machine to calculate factors 193 digits in 0.1 s [25]. Quantum calculations allied in several

✉ Majid Khan
mk.cfd1@gmail.com

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

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

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

branches of science nowadays and a novelty in image processing, computational complications, and pattern recognition. The feasibility of quantum mechanics properties of superposition and entanglement applied on the traditional cryptosystem at fundamental level has been discovered in scientific ages.

The first key distribution using quantum protocol was published in 1984 by Charles Bennet and Gilles Brassard named as BB84 [26]. Further advancement took place in 1991, when Ekert proposed the Einstein–Podolsky–Rosen (EPR) entanglement theory, whose security was based on Bell's inequality [27, 28]. To transfer a qubit into an elementary particle form one side to another, either on free-space or fiber optics utilized by quantum channels, whereas both sides cannot be protected from illegitimate attempts [29]. Quantum channels are considered to be useful for traditional system security in the light of quantum standards of uncertainty principle by Heisenberg and no-cloning theorem that keeps the whole communication system unbroken [30–40].

Quantum algorithms processed into two channels; one is ERP (entangled state) channel and the second is qubit channel. In this article, we perform entanglement phenomenon on spin matrices to provide security to digital contents. Section 2 of this article provides the basic concept of spin matrices and their entanglement, and finite-state machine at which the entangled matrices applied. Section 3 demonstrates the experimentation of algorithm on standard images. Section 4 comprises of different analyses' measures and comparison with the existing techniques. The final remarks about the article are presented in Sect. 5.

2 Initiations

The brief demonstration of spin matrices specified in this section, which have been devised in the light of rotation operators in quantum dynamics literature [41–43]. We pass the entangled matrices through finite-state machine [43, 44]. The spin matrices for rotation operators *x*, *y*, and *z* are as follows:

$$R_x(\theta) = \begin{pmatrix} \cos\frac{\theta}{2} & i\sin\frac{\theta}{2} \\ i\sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{pmatrix},\ R_y(\theta) = \begin{pmatrix} \cos\frac{\theta}{2} & \sin\frac{\theta}{2} \\ -\sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{pmatrix},\ R_z(\theta) = \begin{pmatrix} e^{i\frac{\theta}{2}} & 0 \\ 0 & e^{-i\frac{\theta}{2}} \end{pmatrix}.$$

The image encryption algorithm design appeared in Fig. 1 and entanglement of spin matrices in two dimensions are as follows:

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},\ X = \begin{pmatrix} \cos\frac{\theta}{2} & \sin\frac{\theta}{2} \\ \sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{pmatrix},\ Y = \begin{pmatrix} \cos\frac{\theta}{2} & \sin\frac{\theta}{2} \\ -\sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{pmatrix},\ Z = \begin{pmatrix} e^{\frac{\theta}{2}} & 0 \\ 0 & e^{-\frac{\theta}{2}} \end{pmatrix}.$$

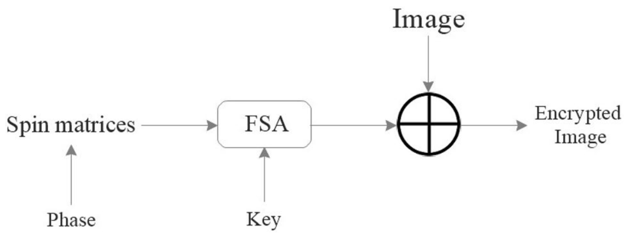


Fig. 1 Proposed encryption algorithm

Entangle these 2×2 spin matrices to produce a set F of 4×4 entangled matrices, $F = \{F_i \in F_{4\times4}(I, X, Y, Z), i = 1, 2, ..., 24\}$.

We will get 24 matrices $F = \{F_1, F_2, F_3, ..., F_{24}\}$.

The phase and key were kept secret. FSM or FSA (finite-state automation) used here with a limited number of conditions. The input symbols are digits defined by key. String belongs to image can be treated by deterministic finite-state or non-deterministic finite-state automaton (NDFA). We considered here NDFA whose output depends on the transitions [43].

3 Experimentation

The dimension of plain image $P(i,j)$ is $M \times N$, where $P(i,j)$ is the *i*th row and *j*th column pixel value.

1. Transform the image layers dimension into $4 \times n$ direction.
2. Specify the criteria for the selection of phase or simply phase kept secret between two parties for encryption and decryption and resolve the entangled matrices by placing phase information.
3. Distribute the key secretly to encrypt or decrypt the data. Different spin matrices operated by FSM with respect to key.
4. Transform the encrypted layers direction into plain image dimension.

5. All the encrypted layers combine together to form a single ciphered image.

We consider here the phase value $\theta = 365.86$ and key $K=68$. FSM converts the key into bits and performs encryption under 24 spin matrices, as shown in Table 1.

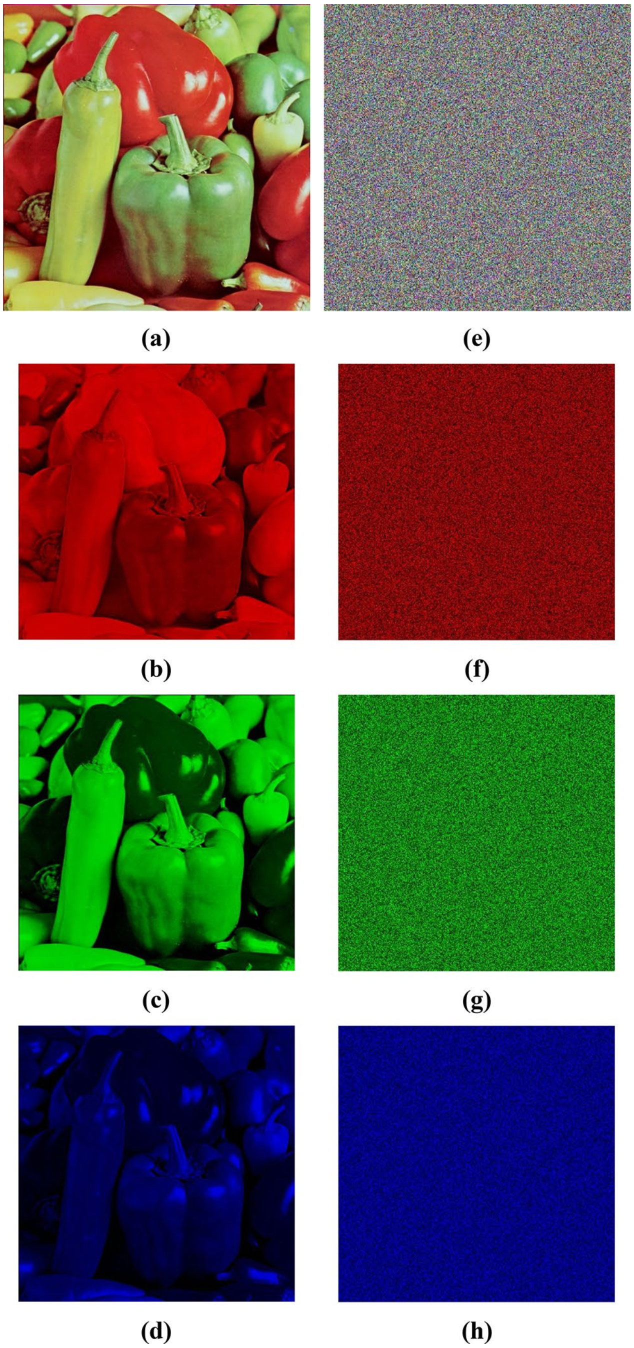


Fig. 2 Layer-wise encryption analyses of pepper image. **a** Plain pepper image, **b–d** red, green, and blue layers of plain image. **e** Encrypted pepper image, **f–h** red, green, and blue layers of encrypted image

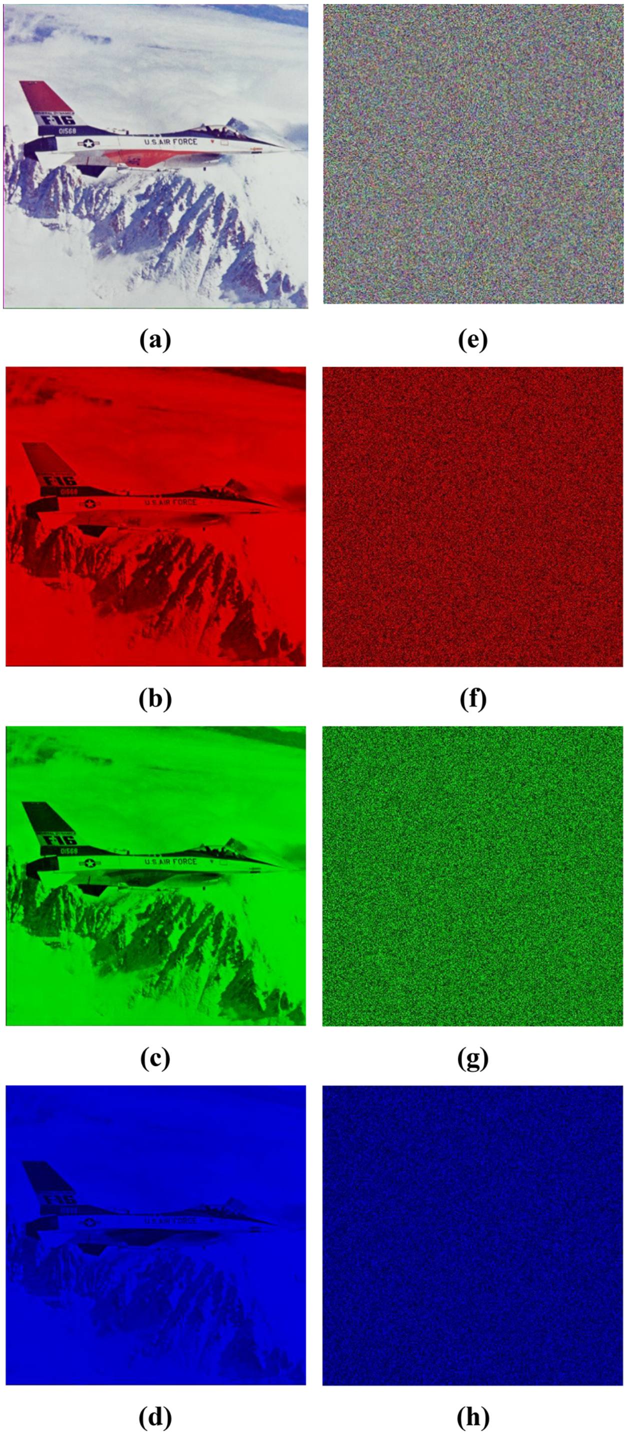


Fig. 3 Layer-wise encryption analyses of airplane image. **a** Plain airplane image, **b–d** red, green, and blue layers of plain image. **e** Encrypted airplane image, **f–h** red, green, and blue layers of encrypted image

Table 1 Finite-state machine operation perform spin matrices at given key

Key in binary	Rounds	FSM input	Decimal input under mod 24	Entangled spin matrix	Cipher image
1,000,100	1	1	1	F_1	$\mathrm{C}_1=F_1\times P$
1,000,100	2	10	2	F_2	$\mathrm{C}_2=F_2\times C_1$
1,000,100	3	100	4	F_4	$C_3=F_4\times C_2$
1,000,100	4	1000	8	F_8	$C_4=F_8\times C_3$
1,000,100	5	10,001	17	F_{17}	$C_5=F_{17}\times C_4$
1,000,100	6	100,010	10	F_{10}	$C_6=F_{10}\times C_5$
1,000,100	7	1,000,100	20	F_{20}	$C_7=F_{20}\times C_6$

Key = Binary(68) = 1000100.

where P is the plane image and the final cipher image at the output of FSM is C_7.

The experimentation results of designed technique on miscellaneous images of size 512×512 of SIPI image database is as follows (Figs. 2, 3).

4 Performance analyses

We have accomplished a few trials on th standard images to affirm the performance and security for the proposed scheme. These trials involve the susceptibility enquiry, factual investigation, and loophole assessment for encoded images. Each of these trials deliberated in detail in the associated subsections.

4.1 Histogram consistency analyses

To estimate the security of digital contents, histogram consistency of enciphered images is necessary [30]. We compute the histograms of two 256 color-level images of size 512×512 that have varied ingredient. Refer to Figs. 4 and 5, plain image histograms comprise extensive sharp rises after sharp decreases and the enciphered image histograms under projected structure are genuinely uniform and pretty much change from the plain image histograms, which mark assessable attacks difficult (Figs. 6, 7, 8).

4.2 Randomness analyses

Entropy and NIST analyses are the most prominent feature of randomness. On the basis of random analysis, events from set of probable discrete events $\{x_1, x_2, \dots, x_i\}$ allied with probabilities $\{p(x_1), p(x_2), \dots, p(x_{\mathrm{i}})\}$, then the average production of basis information is called entropy:

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

where x_i is the basis image and 2^N is the collective data. The estimated Shannon entropy is 8 for perfectly indiscrimination of data. Several standard images and their ciphers entropies accounted in Table 2 and cipher images entropy esteem are very close the theoretical esteem 8. This indicates that the information leakage in encryption process is extraneous and the mechanism is protected upon entropy attacks [17]. We also compare the information entropies of enciphered images under the proposed scheme with latest developed techniques in Table 2.

The security of cryptosystem has a few possessions, e.g., extensive period, identical delivery, extraordinary complexity, and efficiency. With a definite aim to accomplish these requisites, we perform NIST analyses' test. National Institute of Standards and Technology (NIST) develops Special Publication (SP) 1800 series and FIPS (Federal information Processing Standard) for cyber-security community to verify randomness introduced in their cryptosystems. We perform NIST SP 800-22 test to analyze the randomness in digital images. The enciphered Pepper image is utilized to analyze the results of NIST test and after effects of the test are appeared in Table 3.

4.3 Correlation analyses

It is prominent that adjoining pixels are extremely allied in directions either horizontal, vertical, or diagonal. Therefore, the strategy of encryption must abandon this bond to improve barrier contrary to assessable exploration. To affirm the affiliation among adjacent plain and ciphered image pixels, the associated technique is accomplished. Initially, 10,000 sets of two adjoining pixels from plain and corresponding ciphered image randomly selected [47]. The coefficients of correlation for each chain pairs determined by applying the following expression:

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

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

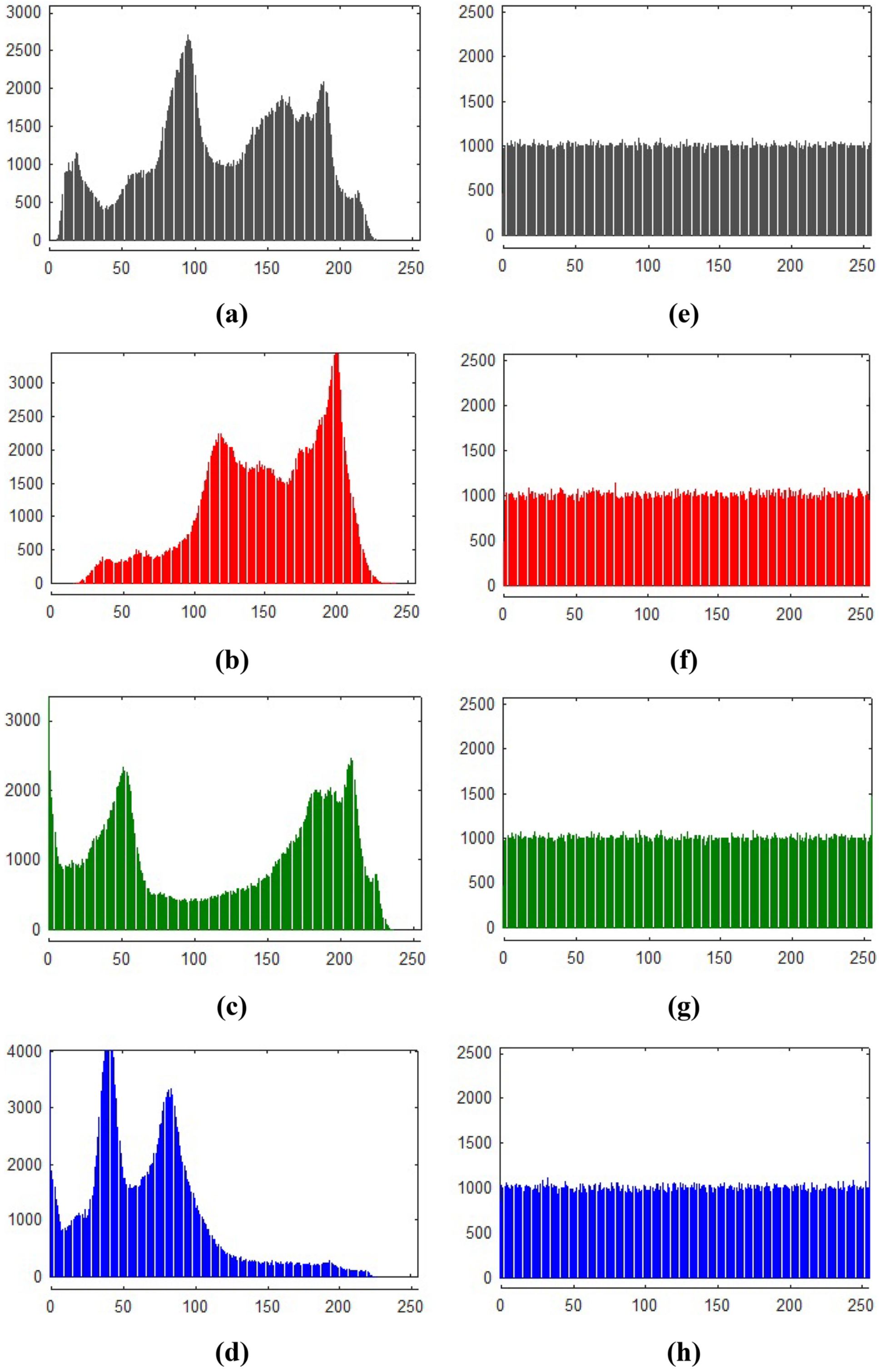
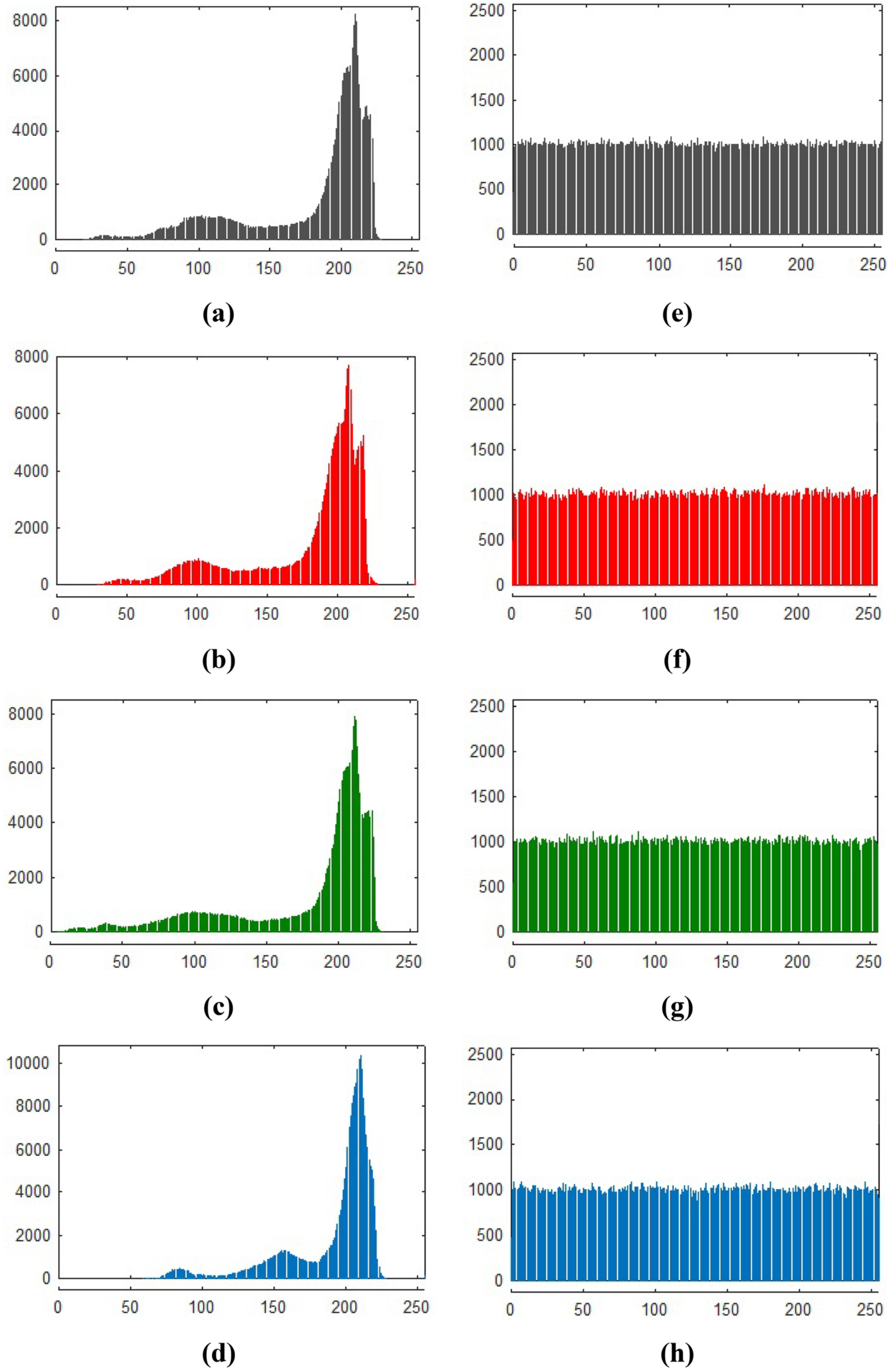


Fig. 4 Layer-wise histograms of pepper image. **a** Plain pepper image histogram, **b**–**d** Red, Green and Blue layers' histogram of pepper image. **e** Encrypted pepper image histogram, **f**–**h** Red, Green and Blue layers' histogram of encrypted pepper image

The quantitative analysis of correlation coefficient for RGB layers is deliberated in Table 4, and presented the distribution in horizontal, vertical, and diagonal directions.

The above-calculated coefficients among numerous pairs of enciphered images are very close to zero, and hence, the plain and ciphered images are significantly diverged from each other. The assessment of correlation coefficients calculated by anticipated scheme at gray scale with the modern techniques using the standard images are presented in Table 5.



(a) (e)

(b) (f)

(c) (g)

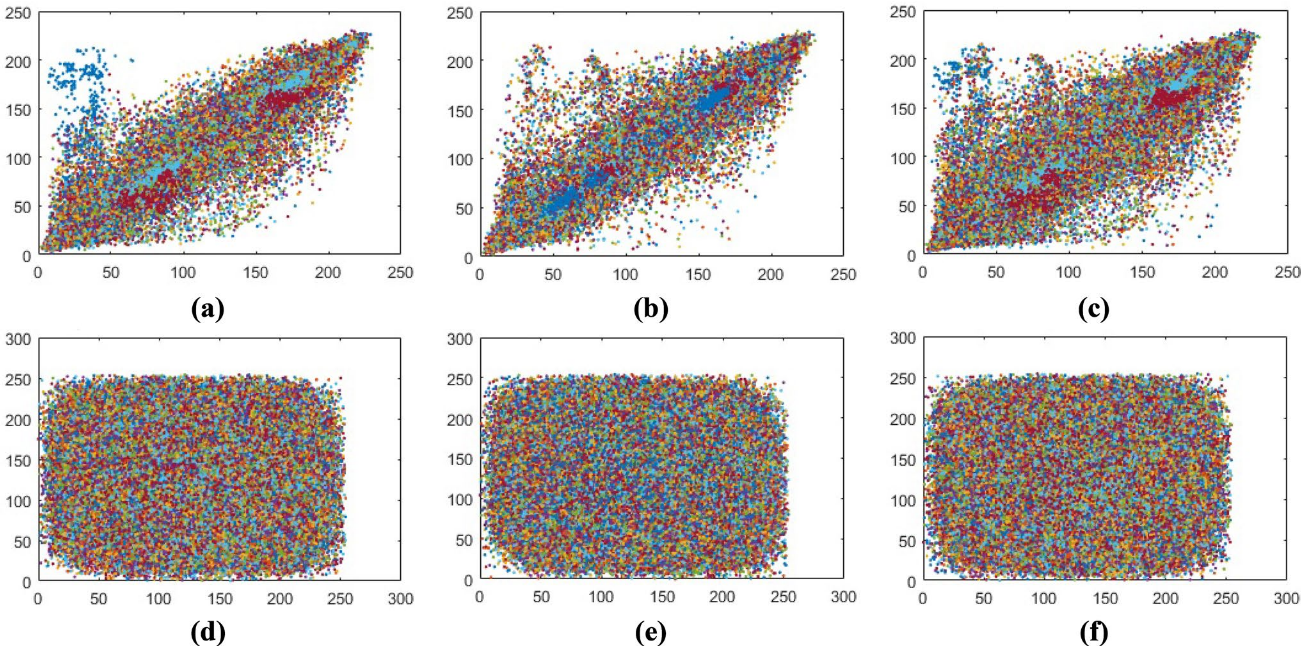
(d) (h)

Fig. 5 Layer-wise histograms of airplane image. **a** Plain airplane image histogram, **b–d** red, green, and blue layers' histogram of airplane image. **e** Encrypted airplane image histogram, **f–h** red, green, and blue layers' histogram of encrypted airplane image

The outcomes of correlation analysis from anticipated scheme have smaller values than the projected techniques in the literature, which qualify the security measures for real-time applications.

4.4 Similarity analyses

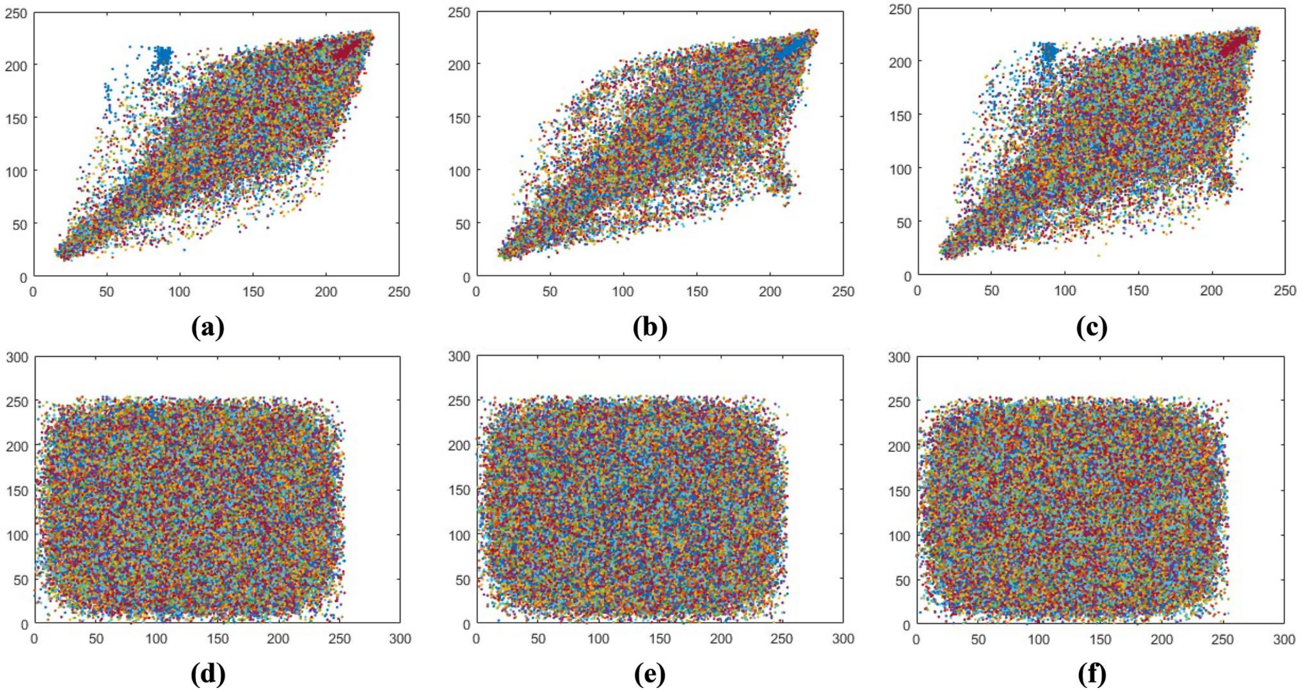
Similarity analyses fundamentally expose the resemblance among different digital contents and the simplest digital content is image. The values of normalized cross-correlation and structure contents are quite closed to 1 for structurally



(a) (b) (c)

(d) (e) (f)

Fig. 6 Correlation of plain and encrypted Pepper image. **a**–**c** Correlation of plain image in horizontal, vertical, and diagonal direction. **d**–**f** Correlation of encrypted image in horizontal, vertical, and diagonal direction



(a) (b) (c)

(d) (e) (f)

Fig. 7 Correlation of plain and encrypted Airplane image. **a**–**c** Correlation of plain image in horizontal, vertical, and diagonal direction. **d**–**f** Correlation of encrypted image in horizontal, vertical, and diagonal direction

similar digital contents. There are different sorts of similarity coefficient are utilized here to quantitatively find the structurally dissimilar digital contents. We investigated here different similarity measures between plain image $P_{i,j}$ and cipher images $C_{i,j}$ to approximate the structure dissimilarity among different digital contents from reference.

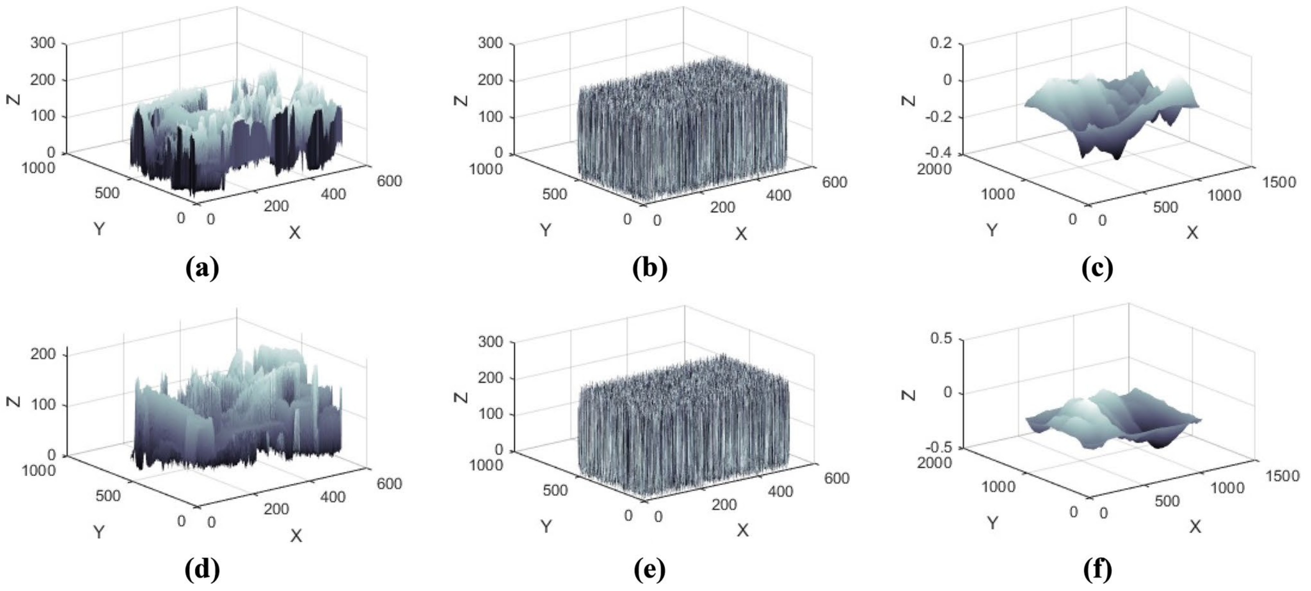


Fig. 8 Normalized cross-correlation surface plots of Pepper and Airplane image. **a**–**c** Surface plot of plain, encrypted, and cross-correlation of plain and encrypted Pepper image. **d**–**f** Surface plot of plain, encrypted, and cross-correlation of plain and encrypted Airplane image

Table 2 Entropy analyses of standard plain and ciphered images of size 512 × 512

Image	Plain				Encrypted				Ref. [45]	Ref. [46]		
	Gray	Red	Green	Blue	Gray	Red	Green	Blue	Gray	Red	Green	Blue
Pepper	7.5835	7.3587	7.6157	7.1495	7.9995	7.9994	7.9993	7.9994	7.9974	7.9992	7.9992	7.9993
Airplane	6.6879	6.7489	6.8106	6.2682	7.9993	7.9994	7.9991	7.9992	7.9972	7.9993	7.9993	7.9993
Lena	7.4455	7.2703	7.5881	7.0026	7.9989	7.9968	7.9986	7.9984	7.9979	–	–	–
Baboon	7.7666	7.7444	7.4493	7.7513	7.9991	7.9992	7.9993	7.9990	7.9974	7.9993	7.9993	7.9992
House	7.5112	7.4493	7.2632	7.4891	7.9993	7.9991	7.9993	7.9991	7.9973	7.9993	7.9993	7.9993
Jelly beans	6.6098	5.3111	5.7424	6.5942	7.9984	7.9975	7.9968	7.9972	–	7.9971	7.9962	7.9973
Sail boat	7.7675	7.3166	7.6443	7.3030	7.9994	7.9991	7.9993	7.9993	–	7.9992	7.9993	7.9992
Splash	7.3232	7.0807	6.9771	6.2126	7.9982	7.9979	7.9973	7.9983	–	–	–	–
Tree	7.5634	7.2798	7.4610	6.9923	7.9988	7.9975	7.9974	7.9982	–	7.9971	7.9973	7.9971

Structural similarity index metric (SSIM) compares the structure, luminance, and contrast between plain and cipher image. Consider the two images $P_{i,j}$ and $C_{i,j}$ with their mean values μ_p, μ_c, and the standard deviation σ_{pc}. If there is any similarity between images, the value approaches 1, while value away from 1 or approaches 0 represent the dissimilarity:

$$\text{SSIM} = \frac{(2\mu_p\,\mu_c + C_1)\,(2\sigma_{pc} + C_2)}{(\mu_p^2 + \mu_c^2 + C_1)\,(\sigma_p^2 + \sigma_c^2 + C_2)}.$$

Normalized cross-correlation (NCC) measures the similarity of pixels between two images. It is determined by the following expression:

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

Structural content (SC) determines the amount of structural details as well as the quality of images in terms of sharpness and noise level. Higher value of SC shows the poor quality of image and it is calculated as follows (Table 6):

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

Table 3 NIST analyses for encrypted Pepper image

Test		Layer-wise *p* values of encrypted images				Remarks
		Gray	Red	Green	Blue	
Frequency		0.25103	0.13139	0.36543	0.24916	Pass
Block frequency		0.21153	0.46886	0.43132	0.12108	Pass
Rank		0.28198	0.28171	0.28194	0.29051	Pass
Runs ($M=10{,}000$)		0.42635	0.33721	0.67959	0.44218	Pass
Long runs of ones		0.76542	0.76541	0.61721	0.74728	Pass
Overlapping templates		0.82849	0.83898	0.84998	0.79979	Pass
No overlapping templates		0.99921	0.96826	0.88245	0.98799	Pass
Spectral DFT		0.88663	0.74465	0.53889	0.25756	Pass
Approximate entropy		0.61372	0.36176	0.21183	0.59989	Pass
Universal		0.99986	0.99565	0.99529	0.99442	Pass
Serial	*p values 1*	055143	0.21024	0.13028	0.42132	Pass
Serial	*p values 2*	0.88783	0.84662	0.66936	0.91392	Pass
Cumulative sum forward		0.64267	0.43476	0.33676	0.53526	Pass
Cumulative sum reverse		0.77512	0.53121	0.82928	0.87679	Pass
Random excursions	$X=-3$	0.98132	0.87795	0.86443	0.76251	Pass
	$X=-2$	0.97228	0.76016	0.14445	0.33270	Pass
	$X=-1$	0.96653	0.77265	0.66710	0.86291	Pass
	$X=1$	0.96116	0.96687	0.83132	0.90225	Pass
	$X=2$	0.21156	0.55121	0.42162	0.12781	Pass
	$X=3$	0.61×10^{-5}	0.05366	0.13356	0.02112	Pass
Random excursion variants	$X=-3$	0.46427	0.22749	0.32996	0.42354	Pass
	$X=-2$	0.41563	0.56673	0.61655	0.28373	Pass
	$X=-1$	0.41078	0.55002	0.41596	0.22186	Pass
	$X=1$	0.55617	0.65238	0.42909	0.64261	Pass
	$X=2$	0.66138	0.75692	0.35671	0.90213	Pass
	$X=3$	0.78322	0.56894	0.70716	0.09502	Pass

4.5 Difference analyses

The image quality evaluation based on pixel difference procedure executed here by calculating the mean absolute error, mean square error, and peak signal-to-noise ratio.

Mean absolute error (MAE) is the most common technique used to measure the accuracy for continues variables. It defines the average of absolute difference between plain and ciphered image. Higher the MAE esteem to enhance the security and it is defined as follows:

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

MSE and PSNR compare the image encryption quality. MSE indicates the collective squared error among the plain and ciphered images, while PSNR indicates the measure of peak error:

$$\mathrm{MSE}=\frac{1}{M\times N}\sum_{i=0}^{M-1}\sum_{j=0}^{N-1}\left(P_{i,j}-C_{i,j}\right)^2.$$

The encryption quality is acceptable by higher the MSE esteem and lower the PSNR or vice versa. The quality of ciphered images can be evaluated by utilizing the PSNR as follows:

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

where I_{MAX} is the greatest pixel approximation of image contents and the feasibility of anticipated scheme evaluated for MSE and PSNR presented in Table 7.

4.6 Differential assault analyses

To affirm the image encryption scheme against differential assault, we require the impact of changing a single pixel in plain image and overall encrypted image and execute the number of pixels change rate (NPCR) and unified average intensity (UACI). We assumed two encoded images, whose source image just differs by a single pixel. The NPCR and UACI for

Table 4 Correlation coefficients of plain and encrypted images at RGB scale

Image		Plain			Encrypted			Ref [48].		
		Horizontal	Vertical	Diagonal	Horizontal	Vertical	Diagonal	Horizontal	Vertical	Diagonal
Pepper	R	0.9662	0.9639	0.9368	−0.0046	−0.0019	0.0012	-	-	-
	G	0.9479	0.957	0.9132	−0.0021	0.0017	−0.0034	–	–	–
	B	0.9787	0.982	0.9646	0.0007	−0.0022	−0.0023	–	–	–
Airplane	R	0.9759	0.9729	0.9516	−0.0011	0.0003	−0.0062	–	–	–
	G	0.9757	0.9753	0.9546	0.0006	0.0005	−0.0014	–	–	–
	B	0.9699	0.9603	0.9396	0.0004	−0.0026	0.0015	–	–	–
Lena	R	0.9759	0.9878	0.9637	−0.0035	0.0002	−0.0021	0.0023	0.0005	0.0009
	G	0.9814	0.9833	0.9665	0.0004	0.0002	−0.0016	0.0003	0.0012	0.0007
	B	0.8534	0.7598	0.7300	0.0001	−0.0041	−0.0008	0.0006	0.0003	0.0007
Baboon	R	0.9625	0.9313	0.9166	0.0010	−0.0013	−0.0014	–	–	–
	G	0.9121	0.8530	0.8232	−0.0012	0.0002	0.0016	–	–	–
	B	0.9696	0.9558	0.9380	0.0008	−0.0013	−0.0035	–	–	–
House	R	0.9713	0.9756	0.9506	0.0011	0.0007	0.0008	–	–	–
	G	0.9581	0.9659	0.9282	0.0021	0.0012	0.0013	–	–	–
	B	0.9817	0.9827	0.9674	0.0009	−0.0015	−0.0055	–	–	–
Jelly bean	R	0.9772	0.9791	0.9592	−0.0013	−0.0018	−0.0031	–	–	–
	G	0.9815	0.9852	0.9694	−0.0017	0.0018	0.0009	–	–	–
	B	0.9916	0.9906	0.9843	0.0004	−0.0036	−0.0061	–	–	–
Sail boat	R	0.9791	0.9759	0.9610	0.0013	−0.0017	0.0007	–	–	–
	G	0.9850	0.9831	0.9711	0.0034	−0.0012	−0.0061	–	–	–
	B	0.9874	0.9880	0.9782	−0.0024	0.0023	0.0017	–	–	–
Splash	R	0.9943	0.9978	0.9926	0.0004	0.0022	0.0007	–	–	–
	G	0.9894	0.9937	0.9837	−0.0036	−0.0061	0.0014	–	–	–
	B	0.9891	0.9904	0.9809	−0.0021	0.0036	0.0022	–	–	–
Tree	R	0.9770	0.9596	0.9460	−0.0079	−0.0091	0.0047	–	–	–
	G	0.9800	0.9639	0.9522	−0.0072	−0.0041	−0.0018	–	–	–
	B	0.9830	0.9678	0.9583	−0.0088	0.0002	0.0005	–	–	–

Table 5 Correlation coefficients of plain and encrypted images at gray scale and comparison with the existing approaches

Image	Plain			Encrypted			Refs. [45, 46]		
	Horizontal	Vertical	Diagonal	Horizontal	Vertical	Diagonal	Horizontal	Vertical	Diagonal
Pepper	0.9814	0.9833	0.9665	−0.0055	0.0025	0.0011	0.0007	−0.0012	0.0001
Airplane	0.9662	0.9639	0.9368	−0.0046	−0.0019	0.0012	−0.0016	0.0008	0.0033
Lena	0.9737	0.9869	0.9610	−0.0045	−0.0070	0.0013	0.0009	0.0021	−0.0007
Baboon	0.8534	0.7598	0.7300	0.0015	−0.0021	−0.0018	0.0039	−0.0045	0.0039
House	0.9479	0.957	0.9132	−0.0028	0.0087	−0.0034	−0.0028	−0.0041	0.0045
Jelly beans	0.9787	0.982	0.9646	0.0017	−0.0023	−0.0023	−0.0033	0.0018	−0.0045
Sail boat	0.9737	0.9700	0.9569	0.0010	−0.0033	−0.0014	−0.0040	−0.0051	0.0001
Splash	0.9840	0.9915	0.9773	−0.0042	0.0012	0.0016	0.0017	−0.0041	0.0015
Tree	0.9669	0.9441	0.9294	0.0028	−0.0013	−0.0035	0.0019	−0.0021	0.0036

two encoded images $C_1(i,j)$ and $C_2(i,j)$ can be assessed by the following expressions:

$$\mathrm{NPCR} = \frac{1}{W \times H} \sum\nolimits_{i,j} x(i,j),$$

where

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

Table 6 Pixels' similarity analyses between original and encrypted standard images

Standard image	Proposed scheme			Ref [49].	Ref [6].
	SSIM	NCC	SC	SSIM	NCC
Pepper	0.0047	0.9959	0.9980	0.0067	0.9933
Airplane	0.0030	0.9956	0.9971	–	–
Lena	0.0010	0.9930	0.9981	0.0053	0.9920
Baboon	0.0016	0.9989	0.9983	0.0074	0.9927
House	0.0112	0.9938	0.9982	0.0115	–
Jelly beans	0.0154	0.9956	0.9919	–	–
Sail boat	0.0030	0.9974	0.9980	0.0010	0.9938
Splash	0.0114	0.9912	0.9911	–	–
Tree	0.0019	0.9968	0.9928	–	–

Table 7 Pixels' difference analyses between plain and ciphered images and assessment with the existing approaches

Image	Proposed scheme			Ref. [50]	Ref. [51]	
	MAE	MSE	PSNR	MAE	MSE	PSNR
Pepper	85.48	8992.82	8.8917	75.64	8261	8.9603
Airplane	87.97	8853.77	8.8954	83.19	–	–
Lena	79.88	8765.76	8.9570	78.24	–	–
Baboon	81.53	8619.66	8.9865	71.38	7385	9.4474
House	89.23	8924.86	8.8919	–	7699	9.2667
Jelly beans	66.83	8566.12	8.8954	–	–	–
Sail boat	88.34	8142.86	9.1162	–	7701	9.2653
Splash	78.17	9106.73	8.1152	76.74	8731	8.7200
Tree	78.99	7436.10	9.4345	–	–	–

Table 8 NPCR analyses between plain and ciphered images

Image	NPCR				Ref. [52]	Ref. [46]		
	Gray	R	G	B	Gray	R	G	B
Pepper	99.92	99.72	99.82	99.61	99.15	99.60	99.63	99.58
Airplane	99.84	99.81	99.86	99.77	99.18	99.61	99.61	99.60
Lena	99.86	99.86	99.81	99.89	99.22	–	–	–
Baboon	99.88	99.85	99.72	99.87	99.12	99.63	99.59	99.62
House	99.79	99.65	99.68	99.86	98.87	99.63	99.59	99.60
Jelly beans	99.81	99.82	99.83	99.77	–	99.60	99.58	99.61
Sail boat	99.89	99.86	99.78	99.81	–	99.61	99.61	99.59
Splash	99.74	99.62	99.72	99.58	–	99.61	99.59	99.59
Tree	99.82	99.76	99.67	99.87	–	99.58	99.54	99.56

Table 9 UACI analyses between plain and ciphered images

Image	UACI				Ref. [52]	Ref. [46]		
	Gray	R	G	B	Gray	R	G	B
Pepper	33.58	36.39	33.14	35.26	33.14	33.42	33.49	33.41
Airplane	33.44	38.33	34.26	34.21	33.11	33.47	33.40	33.37
Lena	33.68	34.97	33.06	33.81	33.12	–	–	–
Baboon	33.64	35.48	33.06	34.81	33.11	33.48	33.54	33.53
House	33.25	32.37	33.21	32.41	32.16	33.52	33.53	33.48
Jelly beans	33.21	32.94	31.85	33.18	–	33.52	33.61	33.46
Sail boat	33.47	32.56	34.11	32.25	–	33.49	33.56	33.43
Splash	33.04	34.42	30.14	32.29	–	33.49	33.54	33.46
Tree	33.31	33.64	31.55	33.23	–	33.48	33.36	33.32

Table 10 Gray-level co- occurrence matrix analyses

Image	Proposed scheme			Ref [54]	Ref. [55]	Ref. [54]
	Homogeneity	Contrast	Energy	Homogeneity	Contrast	Energy
Pepper	0.9856	10.6103	0.0156	–	10.5432	–
Airplane	0.9893	10.6231	0.0156	0.464131	–	0.0282
Lena	0.9891	10.4963	0.0157	–	10.4511	–
Baboon	0.9890	10.5001	0.0155	–	10.4784	–
House	0.9791	10.4421	0.0158	–	–	–
Jelly beans	0.9796	10.5101	0.0157	–	–	–
Sail boat	0.9894	10.5136	0.0157	–	10.4423	–
Splash	0.9795	10.5006	0.0159	–	–	–
Tree	0.9895	10.5001	0.0156	–	–	–

Table 11 Encryption execution time in seconds

Image	Proposed scheme	Ref. [55]	Ref. [23]
Pepper	1.41	2.76	3.68
Airplane	1.29	–	–
Lena	1.32	2.25	3.23
Baboon	1.36	2.55	3.53
House	1.22	–	–
Jelly beans	1.19	–	–
Sail boat	1.39	2.66	3.55
Splash	1.10	–	–
Tree	1.26	–	–

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

To examine the sensitivity of plain image, we have to encrypt it first and then change one pixel randomly in the plain image. The experimental results of these assessments are provided in Tables 8 and 9.

NPCR esteems using proposed technique are persistently correspondent to the perfect estimation of 1 and the assessment of differential assault analyses of anticipated process with modern approaches is also discussed in Tables 8 and 9.

This judgement illustrate that projected technique has extreme degree impatient to a trivial alteration in plain image, irrespective of two enciphered plain images which have 1− bit alteration, the two images are fairly dissimilar from each other. Hence, the anticipated strategy has greater ability to hostile the differential assaults.

4.7 Gray-level co− occurrence matrix analyses

To analyze the visual strength of proposed algorithm, gray-level co− occurrence matrix (GLCM) analyses exemplify homogeneity, contrast, and energy [53]. The homogeneity analysis for an image can be calculated using the following expression:

$$\text{Homogeneity} = \sum_{i,j} \frac{\rho(i,j)}{1 + |i - j|}.$$

Homogeneity investigation accomplishes the closeness of distribution in GLCM to GLCM diagonally. Its range lies between 0 and 1, where 0 validates no variation and 1 validate large number of variation in image pixels.

The contrast analysis allows the observer to identify the object in the texture of an image and defined as follows:

$$\text{Contrast} = \sum_{i,j} |i - j|^2 \rho(i,j).$$

The rage of contrast lies between 0 and (size(image) − 1)^2. The constant image has 0 contrast and greater the contrast value illustrates the large number of variations in the image's pixels.

The energy exploration proceeds the sum of squared elements in GLCM and it is expressed as follows:

$$\text{Contrast} = \sum_{i,j} \rho(i,j)^2.$$

Its range lies between 0 and 1 and the constant image has 1 energy. Table 10 exhibits the GLCM analyses for enciphered images.

The corresponding homogeneity values for enciphered images are very close to 1 and contrast values are sufficiently large, which demonstrates the large number of variations in image pixels. The energy values for enciphered images approach 0, which proves that the image is not constant.

4.8 Time sensitivity analyses

The anticipated scheme in this article is very much effective than already existing techniques, because it uses minimum resources and least computation cost. To analyze the computational complication, we compare time complexity with the existing techniques in Table 11. The table demonstrates the time taken during encryption of plain images. Decryption time is almost equal to encryption time. The projected technique in Table 11 has less computational complexity than already existing approaches.

5 Conclusion

We have designed a new scheme based on quantum spinning to provide the security to digital contents. We consumed the half-spin phenomenon to add the confusion and diffusion abilities in our proposed structure. Cracking of keys and messages is not possible without knowledge of phase and entangled matrices. Due to half spinning, there are infinite points which lie between −720° and 720°, while possible combinations of spin matrices are 4!. By utilizing the statistical analyses, our proposed technique is appropriate for real-time applications due to small processing time and superior performance than the existing schemes.

Acknowledgements Both authors Dr. Majid Khan and Hafiz Muhammad Waseem are greatly thankful to Vice Chancellor Dr. Syed Wilayat Hussain and Dean Dr. Iqbal Rasool Memon, Institute of Space Technology, Islamabad Pakistan, for providing the decent environment for research and development.

References

1. C.E. Shannon, Communication theory of secrecy systems. Bell Syst. Tech. J. **28**(4), 656–715 (1949)
2. A. Uhl, A. Pommer, 2004. Image and video encryption: from digital rights management to secured personal communication (Vol. 15). Springer, Heidelberg
3. B. Murugan, A.G. Nanjappa Gounder, S. Manohar, A hybrid image encryption algorithm using chaos and Conway's game− of− life cellular automata. Secur. Commun. Netw. **9**(7), 634–651 (2016)
4. S. Li, G. Chen, A. Cheung, B. Bhargava, K.T. Lo, On the design of perceptual MPEG− video encryption algorithms. IEEE Trans. Circ. Syst. Video Technol. **17**(2), 214–223 (2007)
5. F. Pareschi, R. Rovatti, G. Setti, On statistical tests for randomness included in the NIST SP800− 22 test suite and based on the binomial distribution. IEEE Trans. Inf. Forensics Secur. **7**(2), 491–505 (2012)
6. B. Yang, X. Liao. A new color image encryption scheme based on logistic map over the finite field Z_N. Multimed. Tools Appl. **77**(16), 21803–21821 (2018)
7. R. Enayatifar, A.H. Abdullah, I.F. Isnin, A. Altameem, M. Lee, Image encryption using a synchronous permutation− diffusion technique. Opt. Lasers Eng. **90**, 146–154 (2017)
8. R. Hamza, F. Titouna, A novel sensitive image encryption algorithm based on the Zaslavsky chaotic map. Inform. Secur. J. A Glob. Perspect. **25**(4–6), 162–179 (2016)
9. X.J. Tong, M. Zhang, Z. Wang, J. Ma, A joint color image encryption and compression scheme based on hyper− chaotic system. Nonlinear Dyn. **84**(4), 2333–2356 (2016)
10. Y. Zhang, D. Xiao, Self− adaptive permutation and combined global diffusion for chaotic color image encryption. AEU Int. J. Electron. Commun. **68**(4), 361–368 (2014)
11. X. Wang, L. Teng, X. Qin, A novel colour image encryption algorithm based on chaos. Sig. Process. **92**(4), 1101–1108 (2012)
12. L. Zhang, X. Liao, X. Wang, An image encryption approach based on chaotic maps. Chaos, Solitons Fractals **24**(3), 759–765 (2005)
13. Q. Zhou, K.W. Wong, X. Liao, T. Xiang, Y. Hu, Parallel image encryption algorithm based on discretized chaotic map. Chaos, Solitons Fractals **38**(4), 1081–1092 (2008)
14. H. Gao, Y. Zhang, S. Liang, D. Li, A new chaotic algorithm for image encryption. Chaos, Solitons Fractals **29**(2), 393–399 (2006)
15. Y. Mao, G. Chen, S. Lian, A novel fast image encryption scheme based on 3D chaotic baker maps. Int. J. Bifurc. Chaos **14**(10), 3613–3624 (2004)
16. S. Etemadi Borujeni, M. Eshghi, 2009. Chaotic image encryption design using Tompkins–Paige algorithm. Math. Probl. Eng. 2009
17. G. Zhang, Q. Liu, A novel image encryption method based on total shuffling scheme. Opt. Commun. **284**(12), 2775–2780 (2011)
18. A.A. Abushgra, K.M. Elleithy, A shared secret key initiated By EPR authentication and Qubit transmission channels. IEEE Access **5**, 17753–17763 (2017)
19. R.L. Rivest, A. Shamir, L. Adleman, A method for obtaining digital signatures and public− key cryptosystems. Commun. ACM **21**(2), 120–126 (1978)
20. W. Diffie, M. Hellman, New directions in cryptography. IEEE Trans. Inf. Theory **22**(6), 644–654 (1976)
21. M.R. Albrecht, K.G. Paterson, G.J. Watson Plaintext recovery attacks against SSH. in 30th IEEE Symposium on Security and Privacy, 2009. (IEEE, 2009), pp. 16–26
22. T. ElGamal, A public key cryptosystem and a signature scheme based on discrete logarithms. IEEE Trans. Inf. Theory **31**(4), 469–472 (1985)
23. F. Ahmed, A. Anees, V.U. Abbas, M.Y. Siyal, A noisy channel tolerant image encryption scheme. Wirel. Personal Commun **77**(4), 2771–2791 (2014)
24. J. Morris, Implications of quantum information processing on military operations. Cyber Def. Rev. **2**(3) (2015)
25. J. Preskill, Introduction to quantum information (part 1). Institute for Quantum Computing—CSSQI 2012 (2012), Online Lecture, http://iqim.caltech.edu/2012/11/27/john-preskill-introduction-to-quantum-information-part-1-cssqi-2012/
26. C. H. Bennett, G. Brassard, Quantum cryptography: public key distribution and coin tossing, Theor. Comput. Sci. **560**, 7–11 (2014)
27. R.J. Hughes, W.T. Buttler, P.G. Kwiat, S.K. Lamoreaux, G.G. Luther, G.L. Morgan, J.E. Nordholt, C.G. Peterson, Quantum cryptography for secure free− space communications. in Free− Space Laser Communication Technologies XI, vol. 3615 (International Society for Optics and Photonics, 1999), pp. 98–104
28. C.H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, W.K. Wootters, Teleporting an unknown quantum state via dual classical and Einstein–Podolsky–Rosen channels. Phys. Rev. Lett. **70**(13), 1895 (1993)
29. H.K. Lo, X. Ma, K. Chen, Decoy state quantum key distribution. Phys. Rev. Lett. **94**(23), 230504 (2005)
30. M. Khan, H.M. Waseem, A novel image encryption scheme based on quantum dynamical spinning and rotations. PloS One **13**(11), .e0206460 (2018)
31. S.E. Venegas− Andraca, S. Bose, Quantum computation and image processing: new trends in artificial intelligence. in IJCAI (2003) p. 1563
32. S.E. Venegas− Andraca, S. Bose, Storing, processing, and retrieving an image using quantum mechanics. In: Quantum

Information and Computation, vol. 5105. (International Society for Optics and Photonics, 2003), pp. 137–148

33. M. Lanzagorta, J. Uhlmann, Quantum algorithmic methods for computational geometry. Math. Struct. Comput. Sci. **20**(6), 1117–1125 (2010)
34. C.A. Trugenberger, Probabilistic quantum memories. Phys. Rev. Lett. **87**(6), 067901 (2001)
35. C.A. Trugenberger, Phase transitions in quantum pattern recognition. Phys. Rev. Lett. **89**(27), 277903 (2002)
36. C.A. Trugenberger, Quantum pattern recognition. Quantum Inf. Process. **1**(6), 471–493 (2002)
37. G. Abal, R. Donangelo, H. Fort, Conditional strategies in iterated quantum games. Physica A **387**(21), 5326–5332 (2008)
38. P.W. Shor, Algorithms for quantum computation: discrete logarithms and factoring. in 35th Annual Symposium on Foundations of Computer Science, 1994 Proceedings. (IEEE, 1994), pp. 124–134
39. N. Zhou, Y. Liu, G. Zeng, J. Xiong, F. Zhu, Novel qubit block encryption algorithm with hybrid keys. Physica A **375**(2), 693–698 (2007)
40. Y.G. Yang, J. Xia, X. Jia, H. Zhang, Novel image encryption/decryption based on quantum Fourier transform and double phase encoding. Quantum Inf. Process. **12**(11), 3477–3493 (2013)
41. J. Branson, Quantum Physics 130. UCSD (2002) https://quantummechanics.ucsd.edu/ph130a/130_notes/node275.html
42. T. Guhr, A. Müller–Groeling, H.A. Weidenmüller, Random-matrix theories in quantum physics: common concepts. Phy. Reports **299**, 189–425 (1998)
43. H.M. Waseem, M. Khan, Information confidentiality using quantum spinning, rotation and finite state machine. Int. J. Theor. Phys. **57**(11), 3584–3594 (2018)
44. H.M. Waseem, M. Khan, T. Shah, Image privacy scheme using quantum spinning and rotation. J. Electron. Imaging **27**(6), 063022 (2018)
45. M. Khan, T. Shah, An efficient chaotic image encryption scheme. Neural Comput. Appl. **26**(5), 1137–1148 (2015)
46. B. Stoyanov, K. Kordov, Image encryption using Chebyshev map and rotation equation. Entropy **17**(4), 2117–2139 (2015)
47. M. Khan, A novel image encryption scheme based on multiple chaotic S− boxes. Nonlinear Dyn. **82**(1–2), 527–533 (2015)
48. S.M. Seyedzadeh, B. Norouzi, M.R. Mosavi, S. Mirzakuchaki, A novel color image encryption algorithm based on spatial permutation and quantum chaotic map. Nonlinear Dyn. **81**(1–2), 511–529 (2015)
49. H. Varshney, H. Gupta, M. Kushwaha, Image encryption using chaotic logistic map. Int. J. Electr. Electron. Comput. Sci. Eng. **4**, 40–45 (2017)
50. B. Norouzi, S.M. Seyedzadeh, S. Mirzakuchaki, M.R. Mosavi, A novel image encryption based on row− column, masking and main diffusion processes with hyper chaos. Multimed. Tools Appl. **74**(3), 781–811 (2015)
51. B. Norouzi, S. Mirzakuchaki, S.M. Seyedzadeh, M.R. Mosavi, A simple, sensitive and secure image encryption algorithm based on hyper− chaotic system with only one round diffusion process. Multimed. Tools Appl. **71**(3), 1469–1497 (2014)
52. R.E. Boriga, A.C. Dăscălescu, A.V. Diaconu, A new fast image encryption scheme based on 2D chaotic maps. IAENG Int. J. Comput. Sci. **41**(4), 249–258 (2014)
53. I. Hussain, A. Anees, M. Aslam, R. Ahmed, N. Siddiqui, A noise resistant symmetric key cryptosystem based on S 8 S− boxes and chaotic maps. Eur. Phys. J. Plus **133**, 1–23 (2018)
54. M. Khan, T. Shah, A novel image encryption technique based on Hénon chaotic map and S 8 symmetric group. Neural Comput. Appl. **25**(7–8), 1717–1722 (2014)
55. J. Ahmad, S.O. Hwang, A secure image encryption scheme based on chaotic maps and affine transformation. Multimed. Tools Appl. **75**(21), 13951–13976 (2016)