IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received March 17, 2020, accepted March 30, 2020, date of publication April 10, 2020, date of current version April 29, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.2987097

An Efficient Public Key Cryptosystem Based on Dihedral Group and Quantum Spin States

HAFIZ MUHAMMAD WASEEM[1,2], ABDULLAH ALGHAFIS[3], AND MAJID KHAN[2,4]

[1]Department of Electrical Engineering, Institute of Space Technology, Islamabad 44000, Pakistan
[2]Cyber and Information Security Lab, Institute of Space Technology, Islamabad 44000, Pakistan
[3]King Abdulaziz City for Science and Technology, Riyadh 11442, Saudi Arabia
[4]Department of Applied Mathematics and Statistics, Institute of Space Technology, Islamabad 44000, Pakistan

Corresponding author: Majid Khan (mk.cfd1@gmail.com)

ABSTRACT The enciphering schemes based on medium transformations by following the strict guidelines are almost used everywhere. We have developed the structure to simulate the digital data with quantum spin states rather than following or creating the strict guidelines. We simulate the pixels of an image with the dihedral group and spin states for a defined phase to create confusion in it. The scope of this article is concerned in the development and deployment of public key cryptosystem, its performance and security analyses.

INDEX TERMS Digital data forensic analyses, Dihedral group encryption, image encryption, public key cryptography, quantum cryptography, quantum information theory, quantum spin states, rabin cryptosystem.

I. INTRODUCTION

The ability to process the digital contents competently and transfer securely is more dynamic, and has affected our veracity in the progressive growth of internet of things (IoTs). The computer or digital devices concerning crime, in which the computer can either be a tool, target or evidence, referred as cybercrime. As the information processing depends on information technology, the inhibition of activities and the control are dominant to the attainment of organization or individuals. To manage the computer frameworks from assaults or unauthorized access, cybersecurity bargain with the software or hardware equipment. The release of the intimate information, alteration or loss in digital contents may perhaps affected by the prohibited access [1]–[2]. Secure data transmission/reception across the communal complexes has incredible consequences and gradually imperative due to manipulation and larceny in digital contents. In everyday existence and at economic forums necessitating the digital contents security structure to enhance their privacy level and become completely predominant [3]–[4].

The advancement of quantum machines with the sufficient computational power could have distracted consequences for the advanced digital security. For instance, factorization and discrete log-based algorithms, such as RSA, DSA etc., which assumes to be secured can be illuminated effectually, if the universal quantum framework developed [5]–[8].

The technology dependent organizations and individuals give birth to rising wave of cybercrime. The consistent advancements in the frameworks are of high significance and the quantum expansions bring us near to such a variation, where we can explore the field lies at the intersection of quantum novelties and cybersecurity [9]–[12].

The digital contents privacy in quantum era reviews all the perspectives affecting the security of computation and communication by the development of quantum progressions [13]–[19].

This field can be comprehensively categorized into three classifications reliant on the access and design of quantum challenges. The first classification sustains the existing tasks remains protected, whereas the other two classifications emphasize the conceivable outcomes in quantum developments [20]–[24].

In the presented article, we have developed a public key digital contents confidentiality scheme which simulates the data/pixels of the content with the dihedral and spin states systems. Dihedral is the noncommutative cryptographic group, which is an attractive area to provide security to high-end applications. The working principle of this group is based on the random polynomials chosen by the communicating parties to secure key exchange, enciphering-deciphering, and authentication challenges. The order of this group is more challenging to length based assaults and brute-force

The associate editor coordinating the review of this manuscript and approving it for publication was Sedat Akleylek.

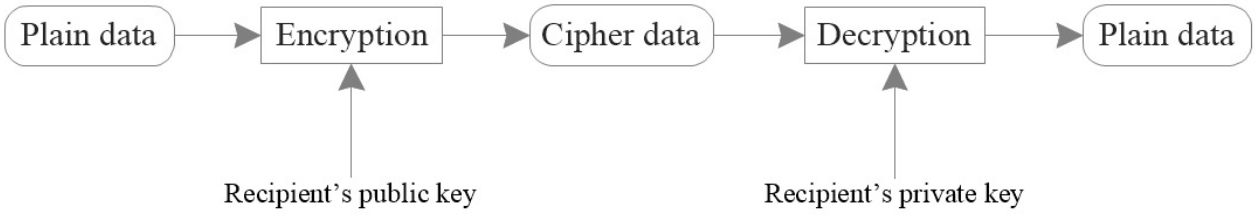

FIGURE 1. Rabin cryptosystem.

attacks [25]. The combination of spin states with the non-commutative cryptographic group provides legitimate security to high-end applications and also satisfy the quantum challenges.

This article is organized in 6 segments. The basic terminologies of public key protocol, dihedral group representation and quantum spin states sorted out in segment 2. The proposed security structure, algorithm and implementation on standard digital contents canvassed in segment 3, whereas the performance and security analyses evaluated in segment 4. Digital forensics analyses for the proposed structure presented in segment 5, and the concluding remarks with future projections canvassed in segment 6.

II. PRELIMINARIES

The basic terminologies and implementations of Rabin cryptosystem, Dihedral groups representations, and the entanglement of quantum spin states discussed in subsections. The proposed cryptosystem based on these terminologies (see Fig. 4), its implication on standard digital images and performance/ security investigations discussed in rest of the article.

A. RABIN CRYPTOSYSTEM

The insolvability based Rabin public key cryptosystem resolves the square root modulo problematic of composite integers. It can be deliberated as a variant of RSA cryptosystem and has computational advantage over the RSA by consuming the public exponent $e = 2$ [26]–[27]. Its decryption practice faintly faster than the RSA, as it requires computations of two modular exponentiations and the Chinese Remainder Theorem (CRT).

Description of Rabin criteria (see Fig. 1) in the proposed algorithm: Let Alice send the enciphered digital data to Bob at a phase 332°, Bob will share his public key with Alice after generating public and private keys. At this instant, Alice will encode the phase value at the public key of Bob and transmit over the public channel. To recover the phase value, Bob will utilize his private key and then apply the phase over the enciphered digital contents to decipher it.

B. DIHEDRAL GROUP

When an object remains unchanged under some transformations or functions, then it follows the rotational or reflexive symmetry [28]. Fig. 2 (a-d) follows the mirror symmetry due to its reflexive property, and if an object is rotated around its center at some angles (like 90° to 270°), then it will come back to its original position or shape [29]. The order of the symmetry is the total number of rotations or reflections of an object in which it comes back to its original shape [30]. The order of symmetry of the butter fly is 4 at an angle of 90° (see Fig. 2 (e-h)).

Dihedral group D_n is the subset of the symmetry group S_n. It is the regular polygon with n rotations and reflections and having $2n$ elements, while the symmetry group S_n have $n!$ elements [31]. Dihedral group in matrices form represented as:

$$r_k = \begin{pmatrix} cos(\frac{2\pi k}{n}) & -\sin(\frac{2\pi k}{n}) \\ \sin(\frac{2\pi k}{n}) & cos(\frac{2\pi k}{n}) \end{pmatrix},$$

$$s_k = \begin{pmatrix} cos(\frac{2\pi k}{n}) & \sin(\frac{2\pi k}{n}) \\ \sin(\frac{2\pi k}{n}) & -cos(\frac{2\pi k}{n}) \end{pmatrix},$$

where r_k is the counterclockwise rotation matrix through an angle of $2\pi/n$ and s_k is the reflection matrix across the line that makes an angle of π/n with the x-axis. Let us select the dihedral group D_4 which has 8 elements, 4 elements represents the rotation and the other 4 about the reflection of the square [32]. These elements are given as:

$$a = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}, \quad b = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix},$$
$$c = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}, \quad d = \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix},$$
$$e = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad f = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix},$$
$$g = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \quad h = \begin{bmatrix} 0 & -1 \\ -1 & 0 \end{bmatrix}.$$

The rotation about the angles of 0°, 90°, 180°, 270° denoted as a_0, a_1, a_2, a_3, and the reflection about the two perpendicular lines and diagonal segments of the square denoted as b_1, b_2, c_1, c_2. The Cayley table and general notation of the group D_4 gives as follows:

$$D_4 = < a, b : a^4 = b^2 = e, ab = ba^{-1} >$$
$$a_0 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}, \quad a_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix},$$

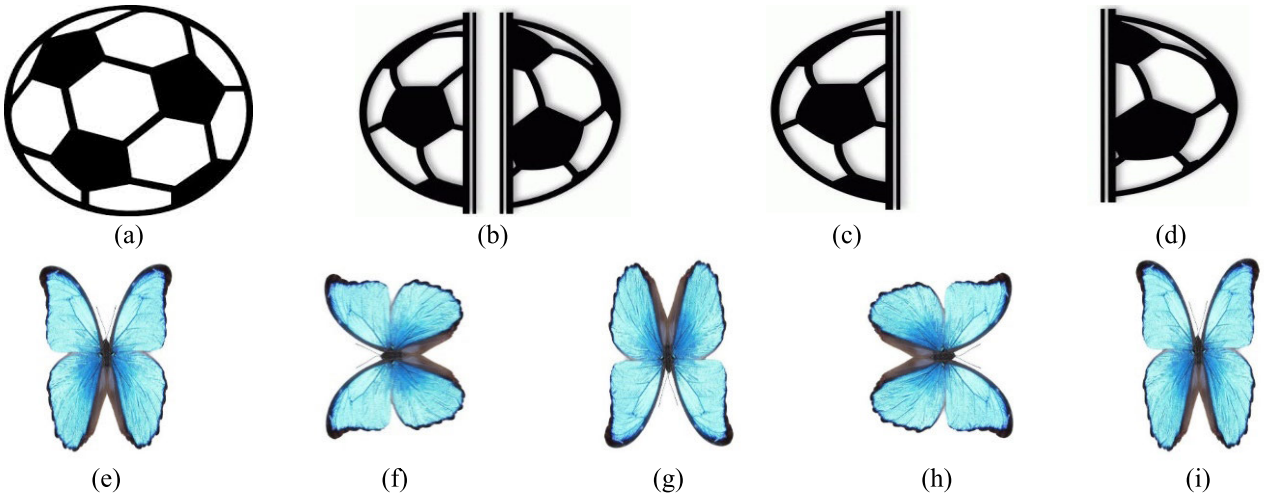

FIGURE 2. Demonstration of the reflection and rotational dihedral group symmetry. (a) original image, (b) Axis of symmetry for reflection, (c-d) Left and right halves of the reflection of symmetry. (e-h) Initial position and the rotations of 90° positions.

TABLE 1. Cayley table of D_4.

Table 1: Cayley table of D_4

	e	a	b	c	d	f	g	h
e	e	a	b	c	d	f	g	h
a	a	e	h	g	f	d	c	b
b	b	h	e	d	c	g	f	a
c	c	g	f	a	b	h	e	d
d	d	f	g	h	e	a	b	c
f	f	d	c	b	a	e	h	g
g	g	c	d	e	h	b	a	f
h	h	b	a	f	g	c	d	e

$$a_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}, \quad a_3 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix},$$
$$b_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}, \quad b_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix},$$
$$c_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}, \quad c_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix}.$$

C. QUANTUM SPIN SYSTEM

The Spin system specifies the rotation of particles around axes. The particles with half-integer spin follows the Fermi-Dirac measurement (Fermions) and Pauli's principle, whereas the whole integer spin follows the Bose-Einstein (Bosons) criteria to share the quantum states [33].

We have followed the half integer spin criteria in the anticipated mechanism, which have been formulated in view of quantum spin systems in literature [34]–[36]. The formulated spin system matrices for the rotation in x, y and z directions are:

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

where θ is the angle of rotational symmetry about x, y and z axes, and demonstrate the position at which the spin system act. Also, the phase of rotational symmetry satisfies the spin half algebra and Kramer's arbitrary spin system. Let entangle these 2×2 matrices by introducing an identity matrix to create a set E of 4×4 matrices, i.e., $E = \{E_k \in E_{4\times4}(I, R_x, R_y, R_z),\ k = 1, 2, \ldots, 24\}$. The spin states for the rotation about R_x, R_y, R_z and their entanglements specified in Fig. 3.

III. PROPOSED ALGORITHM

The spin system produces infinite states between -720^0 and 720^0 phases. The data, when followed by the defined entangled state or states produce ciphers of high randomness. The proposed enciphering-deciphering structure for the digital contents confidentiality demonstrated in Fig. 4.

Over the insecure line of communication, let us consider the establishment of secure channel between Alice and Bob. After the distribution of secrets using Rabin cryptosystem, first they apply the secret at Dihedral group matrices directly,

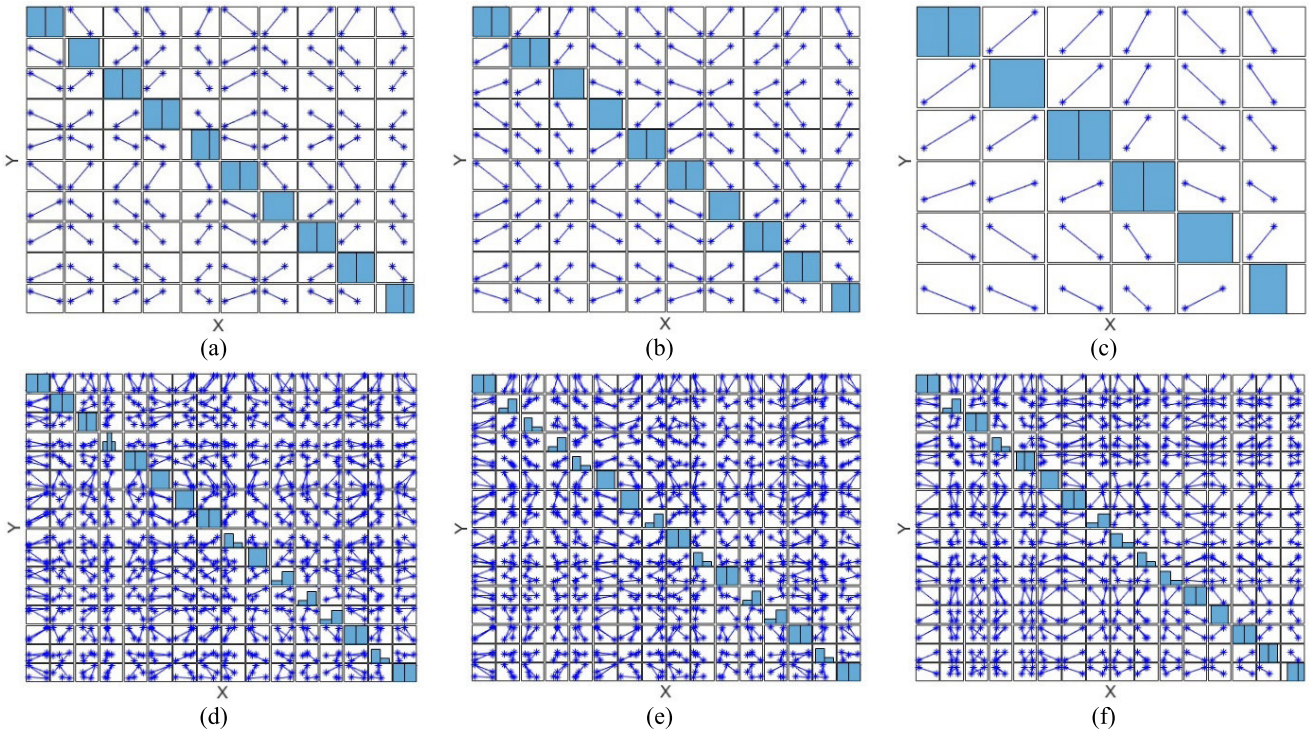

FIGURE 3. States of the spin system for 0° to 360 ° phase values with step-size 90. (a-c) R_x, R_y and R_z spin states, (d-e) Spin states entanglement at E_8, E_{14} and E_{24}.

then they evaluate the spin states by taking *mod* 720 of the shared secret, and finally they will choose the entangled state or states by taking *mod* 24 of the secrets. Now both Alice and Bob can transfer the data to each other securely over insecure line of communication by smearing the plain data with spin states at finite state automation.

A. EXPERIMENTATION OF ANTICIPATED STRUCTURE

The pixels of standard Pepper and House images operated with the combination of dihedral matrices and entangled state E_{20} (by taking *mod24* of 332) at phase 332° for the proposed structure followed in Fig. 5.

IV. PERFORMANCE ANALYSES AND SECURITY EVALUATIONS

To sustain the security assessments and performance analyses for the anticipated algorithm, we have performed the standard evaluations in the subsections of 4 on standard images of size 512×512 taken from SIPI (signal and image processing institute) image database [37]. These evaluations consist of uncertainty assessments, factual examinations and sensibility analyses for the enciphered information to perceive the affectability of the anticipated structure.

A. UNCERTAINTY ANALYSES

To specify the randomness in the transmitted message, the average of information characterizes as entropy. To specify the arbitrary trials from set of dissimilar events $\{d_1, d_2, d_3, \ldots, d_n\}$ with associated likelihoods, the average consequences of the source referred as Shannon entropy [38]. It can be determined for the digital contents as:

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

where 2^N is the average information and d_i is the source image. The ideal Shannon entropy for perfectly indiscrimination in 8-bit digital contents is 8 [39]. The evaluations of entropies for the plain and enciphered layer wise digital contents, and their assessments with the most recent existing methodologies depicted in Table 2.

We have certified the outcomes in 8-bit digital enciphered contents for the anticipated algorithm of Fig. 4 exceptionally close to the ideal Shannon entropy, and have superior outcomes when associated with existing methodologies. The mechanism of the foreseen plan is sheltered upon entropy attacks, as the secretion of information is inappropriate.

B. HISTOGRAMS CONSISTENCY ANALYSES

To evaluate the algorithm of the anticipated plan, we have measured the consistency in enciphered contents histograms [41]–[43]. The processed plain and enciphered contents of Pepper and House images having 256 dark facet levels with distinctive constituent demonstrated in Fig. 6.

Fig. 6 demonstrate the consistency in enciphered contents which classifies the factual assaults hard, and the plain contents have sharp drops after sharp upsurges.

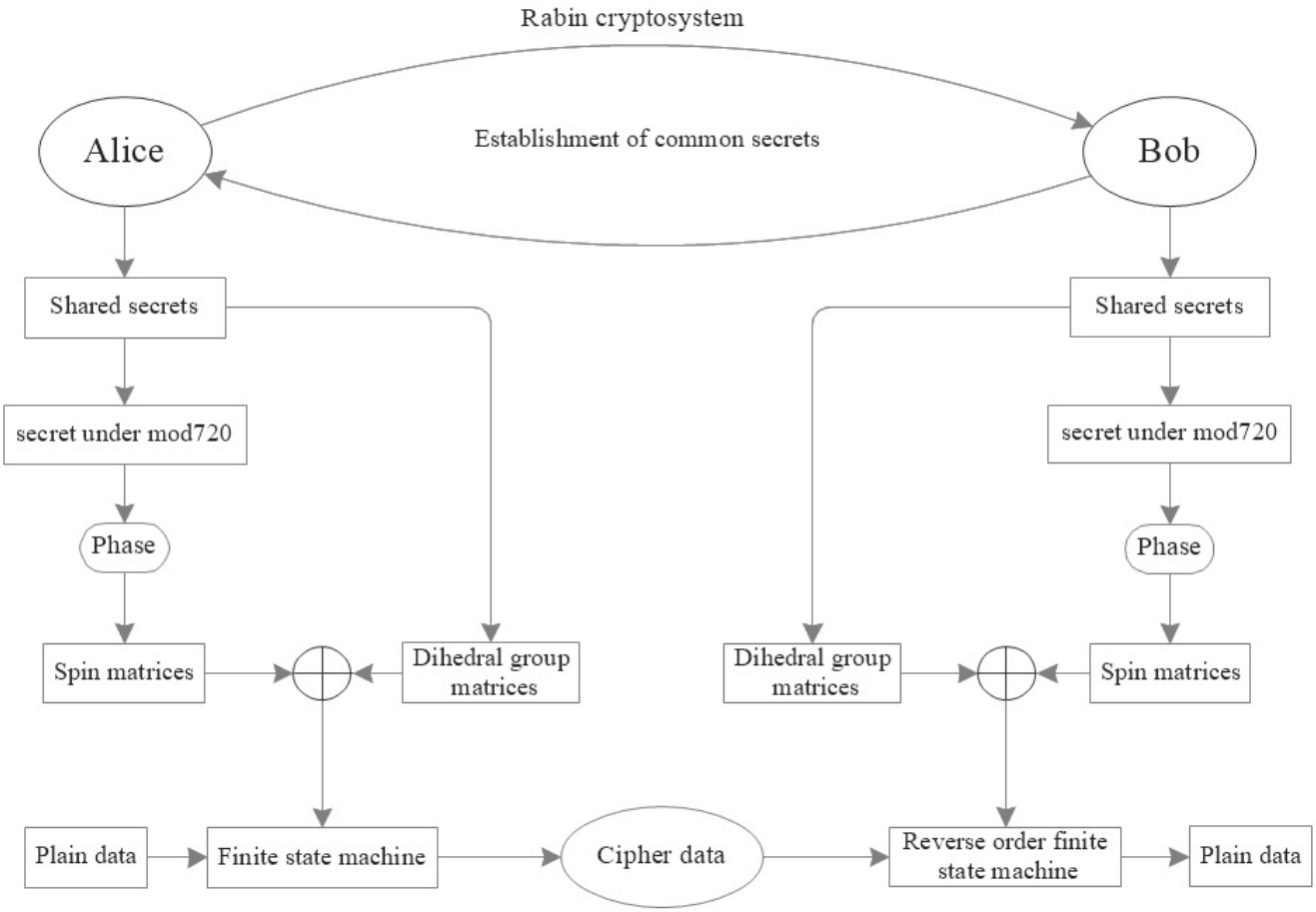

FIGURE 4. Proposed enciphering and deciphering structure.

TABLE 2. Analyses of information entropies for the plain and enciphered digital contents and their assessments with existing methodologies.

Image	Plain contents				Enciphered contents				Ref. [40]	Ref. [38]		
	Gray	Red	Green	Blue	Gray	Red	Green	Blue	Gray	Red	Green	Blue
Pepper	7.5889	7.3516	7.5812	7.1347	7.9986	7.9984	7.9983	7.9984	7.9974	7.9970	7.9971	7.9971
House	7.2386	7.4493	7.2632	7.4891	7.9985	7.9986	7.9982	7.9983	7.9973	7.9974	7.9971	7.9970
Lena	7.4451	7.2531	7.5940	6.9684	7.9987	7.9981	7.9983	7.9974	7.9979	7.9975	7.9970	7.9971
Baboon	7.3485	7.7444	7.4493	7.7513	7.9984	7.9986	7.9985	7.9982	7.9974	7.9967	7.9973	7.9973
Airplane	6.7056	6.7489	6.8106	6.2682	7.9986	7.9984	7.9987	7.9981	7.9972	7.9972	7.9968	7.9972
Splash	7.2579	7.0807	6.9771	6.2126	7.9985	7.9984	7.9982	7.9987	-	7.9973	7.9970	7.9972

C. PIXELS' CORRELATION ANALYSES

To observe the adjacent pairs of pixels associated in horizontal, vertical and diagonal orders, we have performed the correlation analyses. Let us pick the 10000 adjacent pixels' pairs from each content initially and endure the association among the adjacent pixels of plain and enciphered contents. In sense of assessable investigation, the enciphered information assistances the relation of pixels to improve the barrier [44]–[46]. We have computed the two-dimensional correlation coefficients for the numerous pairs of plain and enciphered contents with the following expression.

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

where M and N are the height and width of the contents, plain and enciphered contents signified as P and C, and the mean approximation of P and C are $\overline{P}$ and $\overline{C}$.

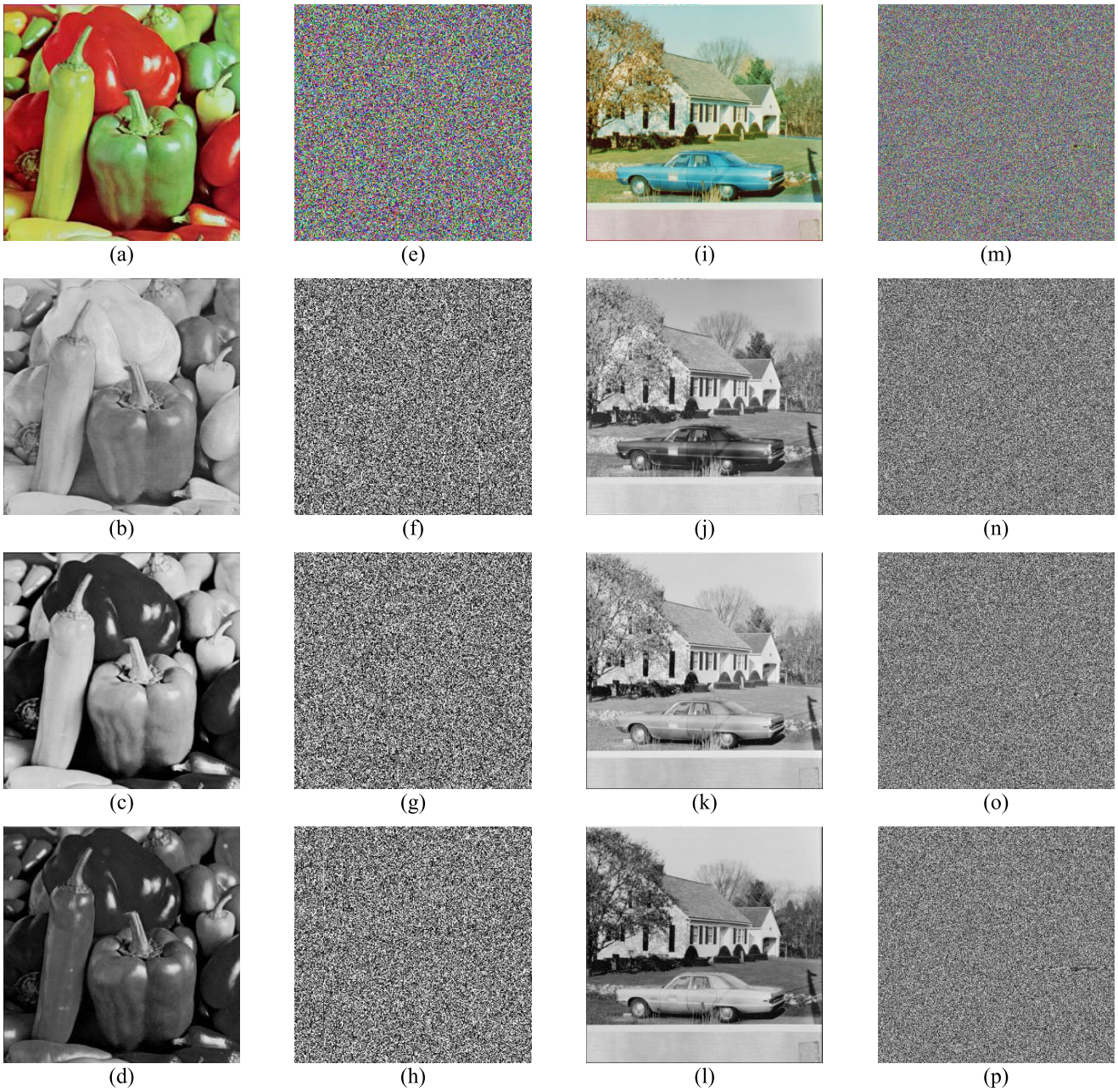

FIGURE 5. Plain and enciphered layer wise Pepper and House images contents. (a-d) Plain color pepper image and corresponding layer wise RGB contents, (e-h) Enciphered color pepper image and corresponding layer wise RGB contents, (i-l) Plain color House image and corresponding layer wise RGB contents, (m-p) Enciphered color House image and corresponding layer wise RGB contents.

The plain and enciphered contents correlation coefficients demonstration and assessments with the existing methodology followed in Table 3.

The enciphered contents correlation coefficients in Table 2 are exceptionally close to zero, which is the requisite for the competent enciphering plan and has inferior values on comparison with existing approach. The demonstration of horizontal, vertical and diagonal analyses on standard Pepper and House images in picture form (see Fig. 7) evaluated by the following expression:

$$r_{x,y} = \frac{\sigma_{x,y}}{\sqrt{\sigma_x^2 \sigma_y^2}}. \tag{3}$$

The adjacent pixels approximation signified by x and y, the variances signified by σ_x^2 and σ_y^2, and the covariance of x and y random variables is $\sigma_{x,y}$.

D. PIXELS' SIMILITUDE ANALYSES

The similitude analyses signified the structure resemblance between the plain and enciphered contents. We have evaluated the normalized cross-correlation (NCC), structural content (SC) and structure similarity index measure (SSIM) to observe the variation in structure between the plain and enciphered contents. The resemblance and traces of correlation measured by NCC, whereas SC regulates the noise level and sharpness, and SSIM relates the luminance, divergence

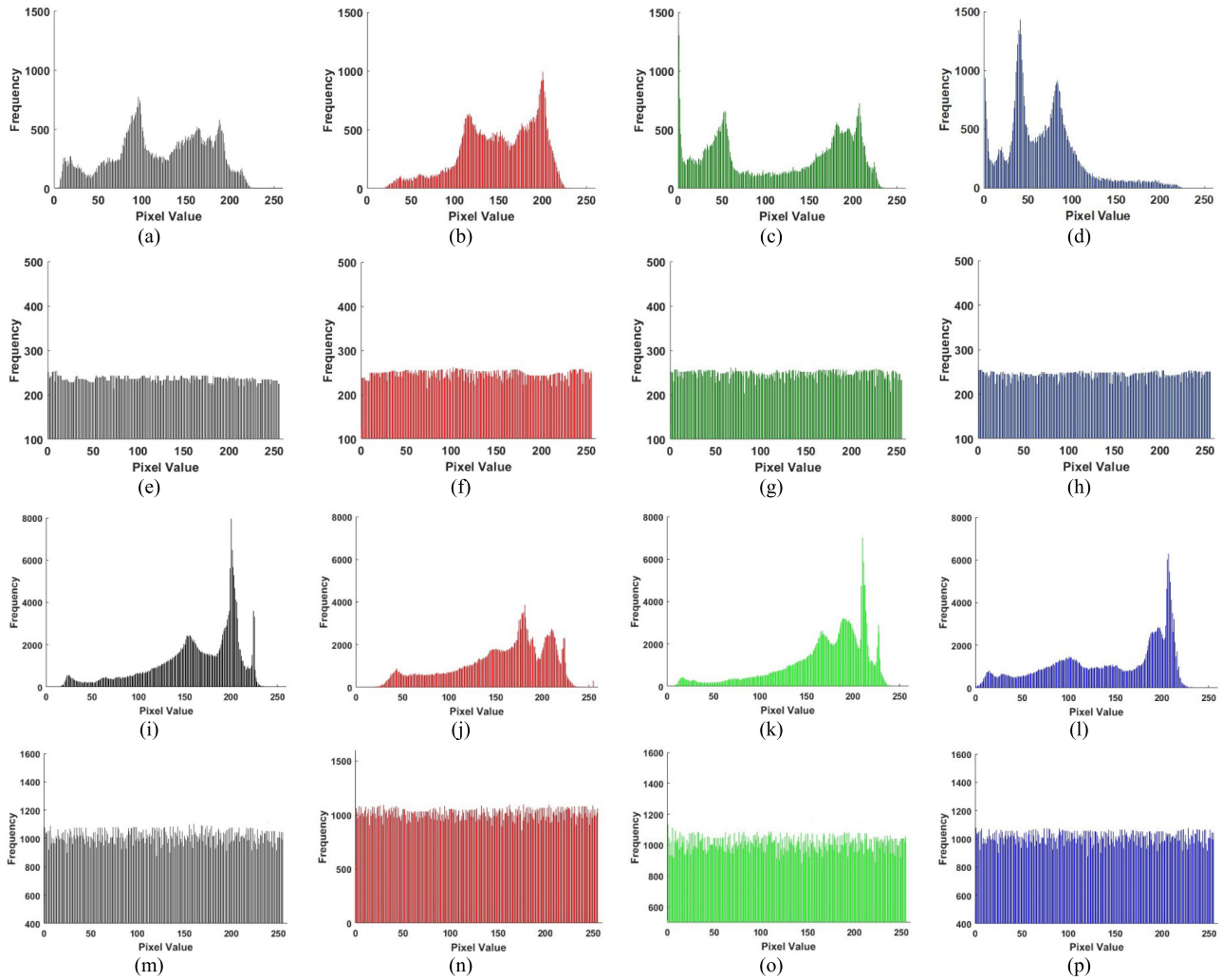

FIGURE 6. Histograms consistency analyses for the Plain and enciphered layer wise Pepper and House images contents. (a-d) Plain pepper image at gray scale and corresponding RGB contents, (e-h) Enciphered pepper image at gray scale and corresponding RGB contents, (i-l) Plain House image at gray scale and corresponding RGB contents, (m-p) Enciphered House image at gray scale and corresponding RGB contents.

TABLE 3. Pixels' correlation coefficients for the plain and enciphered contents, and their assessments with the most recent existing methodology.

Image	Plain contents			Enciphered contents			Ref. [38]		
	Horizontal	Vertical	Diagonal	Horizontal	Vertical	Diagonal	Horizontal	Vertical	Diagonal
Pepper	0.9767	0.9765	0.9644	-0.0042	0.0023	0.0052	-0.0352	0.0075	0.0448
House	0.9488	0.9562	0.9128	-0.0033	0.0018	0.0043	0.0378	-0.0016	-0.0147
Lena	0.9776	0.9848	0.9589	0.0046	-0.0028	-0.0021	-0.0265	0.0167	-0.0135
Baboon	0.8538	0.7613	0.7315	0.0017	0.0049	-0.0017	-0.0624	-0.0392	0.0375
Airplane	0.9644	0.9643	0.9359	0.0023	-0.0051	0.0044	0.0250	-0.0650	0.0149
Splash	0.9833	0.9921	0.9769	-0.0024	0.0031	0.0026	-0.0231	0.0124	-0.0249

and assembly between the plain and enciphered contents. The similitude analyses evaluated here by the following expressions:

$$NCC = \sum_{i=0}^{M-1}\sum_{j=0}^{N-1} \frac{P_{i,j} \times C_{i,j}}{\sum_{i=0}^{M-1}\sum_{j=0}^{N-1} P_{i,j}^2}, \tag{4}$$

$$S\,C = \sum_{i=0}^{M-1}\sum_{j=0}^{N-1} \frac{P_{i,j}^2}{\sum_{i=0}^{M-1}\sum_{j=0}^{N-1} C_{i,j}^2}, \tag{5}$$

$$SSIM = \frac{(2\mu_p\,\mu_c + C_1)(2\sigma_{pc} + C_2)}{(\mu_p^2 + \mu_c^2 + C_1)(\sigma_p^2 + \sigma_c^2 + C_2)}, \tag{6}$$

where $P_{i,j}$ and $C_{i,j}$ are the plain and enciphered contents, the mean values are μ_p and μ_c, and the standard deviation is $\sigma_{p\,c}$.

The NCC, SC and SSIM esteems are fairly close to unity, if there is any structure similarity or correlation traces between the plain and enciphered contents [44]. Higher the SC estimation derives the eminence of image.

The similitude analyses and their assessments with existing approaches conceded in Table 4 for the plain-enciphered contents.

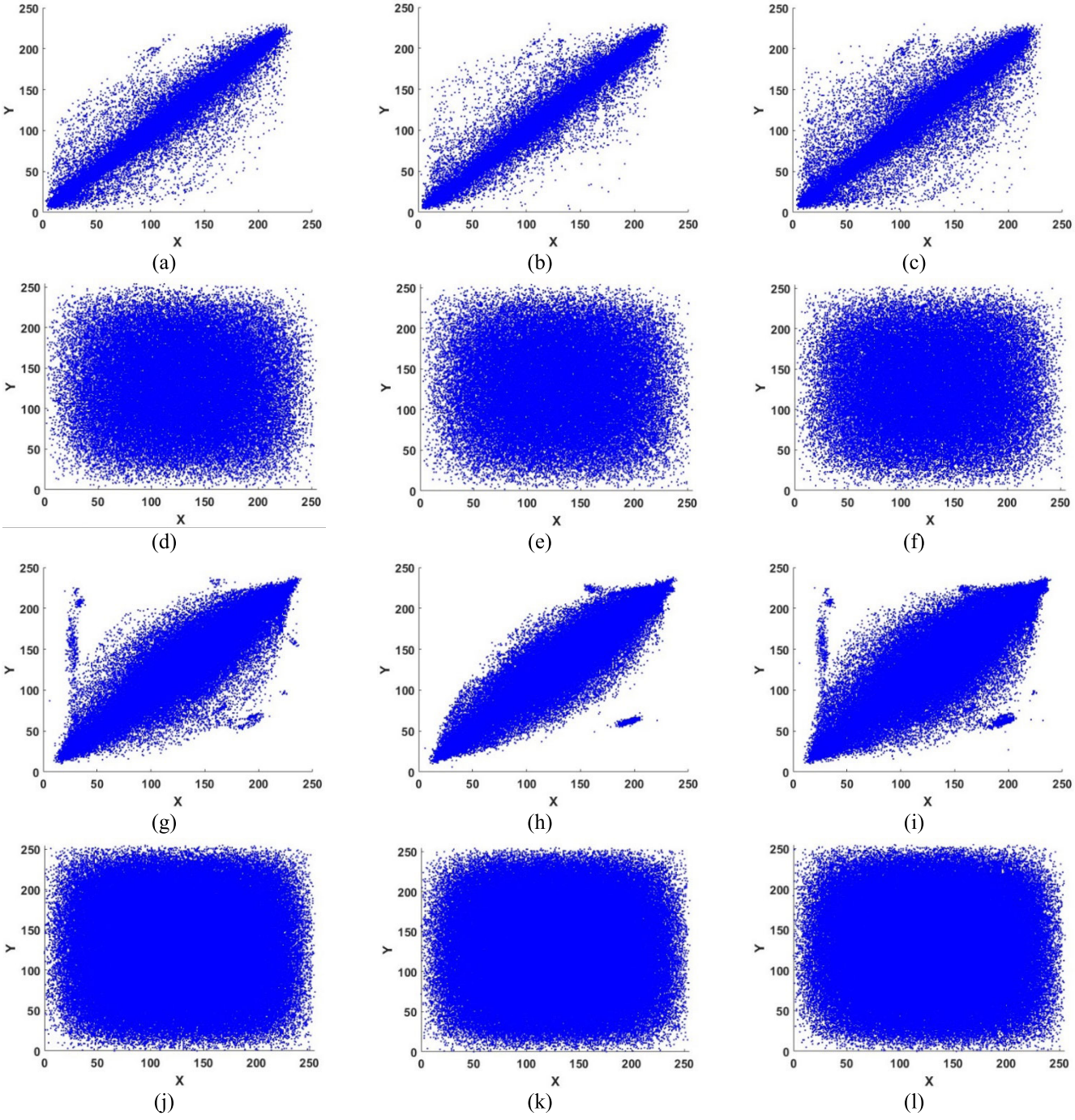

FIGURE 7. Plain and enciphered Pepper and House images correlation analyses for the pixels' pairs in horizontal, vertical and diagonal orders. (a-c) Plain Pepper image analyses, (d-f) Enciphered Pepper image analyses, (g-i) Plain House image analyses, (j-l) Enciphered House image analyses.

In the light of Table 4, NCC, SC and SSIM esteems are fairly close to zero, which represents the structure dissimilarity and correlation invalidation between the plain and enciphered contents.

E. PIXELS' INCONSISTENCY ANALYSES

We have analyzed the divergence of image pixels' by estimating the mean absolute error (MAE), mean square error (MSE) and peak signal to noise ratio (PSNR) [45]. The precision of continuous variables for the disparity in enciphered contents regarding the plain image estimated here by MAE. The enciphered contents eminence can be specified by MSE and PSNR, whereas the average absolute difference between the plain and enciphered contents estimated here by MAE. The aggregate square error between the plain and enciphered content estimated by MSE, and the peal error by PSNR. The following expressions are examined here to estimate the inconsistency between the plain and enciphered

TABLE 4. Pixels' similitude analyses for plain-encoded contents, and their assessments with existing methodologies.

Image	Similitude analyses			Ref. [47]			Ref. [48]		
	NCC	SC	SSIM	NCC	SC	SSIM	NCC	SC	SSIM
Pepper	0.0039	0.0024	0.00768	0.0041	0.0020	0.0047	0.0927	0.0049	0.00113
House	0.0053	0.0025	0.00476	0.0062	0.0018	0.0112	0.0751	0.0055	0.00247
Lena	0.0041	0.0022	0.00641	0.0044	0.0029	0.0030	0.0637	0.0047	0.00152
Baboon	0.0049	0.0017	0.00363	0.0070	0.0019	0.0010	0.0914	0.0076	0.00161
Airplane	0.0022	0.0021	0.00486	0.0011	0.0017	0.0016	0.0818	0.0058	0.00108
Splash	0.0036	0.0027	0.00318	0.0088	0.0089	0.0114	0.0834	0.0063	0.00291

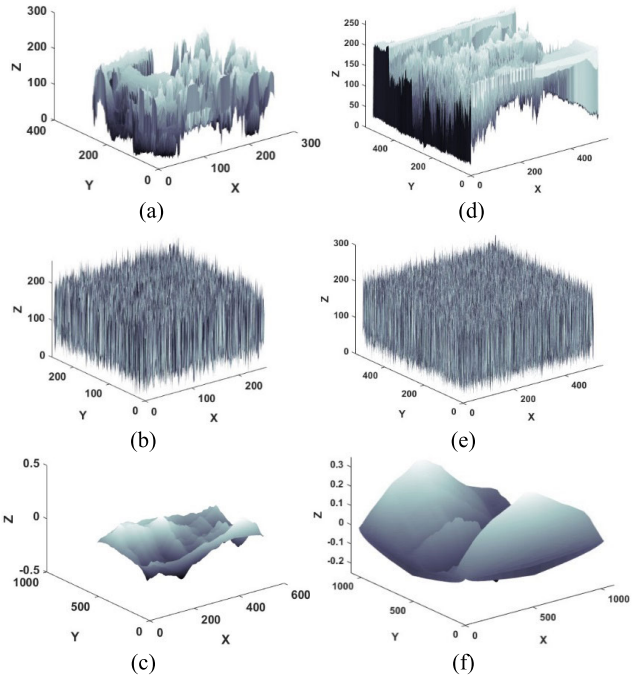

FIGURE 8. Surface plots of NCC for Pepper and House images. (a-c) Plots for plain, enciphered and plain-enciphered cross correlated Pepper image, (a-c) Plots for plain, enciphered and plain-enciphered cross correlated House image.

data.

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

$$MSE = \frac{\sum_{i=1}^{M} \sum_{j=1}^{N} (P_{ij} - C_{ij})^2}{M \times N}, \tag{8}$$

$$\text{PSNR} = 20 \log_{10} \left[\frac{I_{MAX}}{\sqrt{MSE}} \right], \tag{9}$$

The pixels' position for the plain and enciphered contents at i^{th} row and j^{th} column specified by $P_{i,j}$ and $C_{i,j}$, and the extreme pixel position specified by I_{MAX}.

The quality of enciphered contents can be enhanced by superior the MSE esteems and inferior the PSNR estimations, or vice-versa [49]. The evaluation of the proposed structure for inconsistency analyses followed in Table 5.

F. VISUAL STRENGTH ANALYSES

The visual strength analyses measure the image chromatic quality with respect to gray level co-occurrence matrix (GLCM). We have perceived the visual quality of images by observing the homogeneity, energy and contrast analyses of GLCM. The acquaintance of distribution in GLCM to GLCM diagonally performed by homogeneity, the aggregate of squared components of the content measured by energy, and the object in image's texture recognized by contrast [50]. The evaluation of GLCM analyses analyzed here with the following expressions.

$$Homogeneity = \sum_{i,j} \frac{\rho(i,j)}{1 + |i-j|}, \tag{10}$$

$$Energy = \sum_{i,j} \rho(i,j)^2, \tag{11}$$

$$Contrast = \sum_{i,j} |i-j|^2 \rho(i,j), \tag{12}$$

The row and column position of pixels are i and j, homogeneity and energy of the image lies in the range of 0 and 1, and the range of contrast between 0 and $(size\,(image) - 1)^2$. The contrast esteem must be superior for the great number of variations in the image's pixels, whereas the consistent image has 1 energy and 0 contrast value. Table 6 exhibits the analyses of GLCM for the projected enciphering plan and their assessments with most recent existing methodologies.

V. DIGITAL DATA FORENSIC ANALYSES

Digital data forensic specifically investigate the structure of enciphering/deciphering by specifying a documented chain of evidence to inspect what happened to digital data or medium. There are many tools available to investigate the systems/structures resistivity in sense of their encoded or damaged information [51]–[52]. We have performed the noise and differential assaults at the anticipated structure to affirm their resistivity.

A. NOISE ASSAULTS ANALYSE

It is possible in the digital communication either the channel or information affected by noises during the transmission or reception [53]. We investigate the effect of Gaussian noise having normalized power 0.000001 and 0.000005 in the

TABLE 5. Plain-enciphered pixels' inconsistency analyses and their assessments with existing approaches.

Image	Pixels' inconsistency analyses			Ref. [47]			Ref. [48]		
	MAE	MSE	PSNR	MAE	MSE	PSNR	MAE	MSE	PSNR
Pepper	81.12	8722.22	8.9293	87.97	8853.77	8.8954	82.14	8626.15	8.9328
House	80.76	8837.81	8.9016	89.23	8924.86	8.8919	83.88	8798.91	9.1565
Lena	82.11	8788.32	8.9197	85.48	8992.82	8.8917	75.91	8588.39	8.9152
Baboon	79.99	8901.17	8.8923	79.88	8765.76	8.9570	81.28	8942.21	8.7982
Airplane	84.05	8828.38	8.9081	81.53	8619.66	8.9865	79.88	8812.58	8.8667
Splash	82.81	8916.72	8.8605	78.17	9106.73	8.1152	83.59	8859.43	8.4251

TABLE 6. Visual strength analyses of enciphered contents for the proposed structure and their assessments with most existing approaches.

Image	GLCM analyses			Ref. [47]			Ref. [45]		
	Homogeneity	Energy	Contrast	Homogeneity	Energy	Contrast	Homogeneity	Energy	Contrast
Pepper	0.9897	0.0142	10.8126	0.9893	0.0156	10.6231	0.9791	0.0156	10.5103
House	0.9871	0.0133	11.0198	0.9791	0.0158	10.4421	0.9791	0.0158	10.4421
Lena	0.9868	0.0139	10.5621	0.9856	0.0156	10.6103	0.9791	0.0157	10.5463
Baboon	0.9902	0.0158	10.4812	0.9891	0.0157	10.4963	0.9790	0.0155	10.5001
Airplane	0.9881	0.0149	10.3751	0.9890	0.0155	10.5001	0.9793	0.0156	10.6231
Splash	0.9863	0.0153	10.7809	0.9795	0.0159	10.5006	0.9795	0.0159	10.5006

TABLE 7. Plain-enciphered pixels' inconsistency analyses by introducing Gaussian noise and their assessments with the most recent existing approach.

Image	Inconsistency analyses		Noise intensity				Ref. [48]			
			0.000001		0.000005		0.000001		0.000005	
	MSE	PSNR	MSE	PSNR	MSE	PSNR	MSE	PSNR	MSE	PSNR
Pepper	8722.22	8.9293	8702.71	8.9374	8632.24	8.9811	8602.64	8.9982	8541.54	9.1219
House	8837.81	8.9016	8813.83	8.9064	8758.82	8.9752	8759.41	9.2542	8662.79	9.3911
Lena	8788.32	8.9197	8756.19	8.9212	8702.16	8.9804	8543.24	8.9912	8487.69	9.1194
Baboon	8901.17	8.8923	8872.73	8.8978	8814.93	8.9658	8898.37	8.8127	8807.83	8.9489
Airplane	8828.38	8.9081	8802.62	8.9104	8742.42	8.9673	8785.17	8.8984	8716.12	8.9853

encoded information to determine the strength of the anticipated structure. The consequences of the introduced noise in the encoded information and assessments with the existing methodology exhibited in Table 7.

The PSNR estimation has very minute variation when the Gaussian noise strength varies from 0.000001 to 0.000005, and has superior results over existing approach, which affirms the improbable strength of anticipated structure against Gaussian noise assaults.

B. DIFFERENTIAL ASSAULTS ANALYSES

The strength of the projected structure by variation of a plain image solitary pixel modifies the encoded information allied with a probability of half-pixel variation demonstrated by differential assault analysis. The number of pixels changing rate (NPCR) bound together to find the unified average change intensity (UACI) for a precise objective to assess the consequence of miniature variation in the plain content on its encoded one [54]–[57]. The NPCR and UACI for the two enciphered contents, in which one of them is vacillated by a single pixel estimated by the following expressions:

$$NPCR = \frac{\sum_{i=0}^{W-1}\sum_{j=0}^{H-1} K(i,j)}{W \times H} \times 100\%, \tag{13}$$

$$UACI = \frac{1}{W \times H}\left(\sum_{i=0}^{W-1}\sum_{j=0}^{H-1}\frac{|C_1(i,j) - C_2(i,j)|}{255}\right) \times 100\%, \tag{14}$$

The width and height of the digital content represented by W and H, and K is the two dimensional set similar to the enciphered image size. If $C_1(i,j) = C_2(i,j)$, then $K(i,j) = 1$; otherwise $K(i,j) = 0$.

The consequences of the NPCR and UACI for the enciphered contents and their assessments with the most recent existing methodologies exhibited in Table 8-9.

In the light of Tables 8-9, the NPCR and UACI consequences have superior capacity to hostile attacks as NPCR esteems are fairly close to the perfect estimation of 1 and the proposed strategy has superior outcomes and great degree

TABLE 8. NPCR consequences for the encoded contents, and their assessments with existing approaches.

Image	NPCR consequences				Ref. [47]				Ref. [48]			
	Gray	Red	Green	Blue	Gray	Red	Green	Blue	Gray	Red	Green	Blue
Pepper	99.87	99.84	99.85	99.81	99.84	99.81	99.86	99.77	99.89	99.82	99.85	99.79
House	99.85	99.81	99.82	99.87	99.79	99.65	99.68	99.86	99.86	99.73	99.74	99.85
Lena	99.89	99.83	99.84	99.79	99.92	99.72	99.82	99.61	99.91	99.81	99.87	99.73
Baboon	99.86	99.84	99.86	99.81	99.86	99.86	99.81	99.89	99.88	99.82	99.84	99.84
Airplane	99.87	99.86	99.81	99.84	99.88	99.85	99.72	99.87	99.95	99.86	99.79	99.85
Splash	99.85	99.81	99.82	99.78	99.74	99.62	99.72	99.58	99.85	99.71	99.79	99.72

TABLE 9. UACI consequences for the encoded contents, and their assessments with existing approaches.

Image	UACI consequences				Ref. [47]				Ref. [48]			
	Gray	Red	Green	Blue	Gray	Red	Green	Blue	Gray	Red	Green	Blue
Pepper	33.34	36.72	34.97	33.82	33.44	38.33	34.26	34.21	33.38	34.12	32.96	33.68
House	33.32	35.61	34.14	33.94	33.25	32.37	33.21	32.41	33.31	34.72	33.54	33.24
Lena	33.36	34.83	33.83	34.89	33.58	36.39	33.14	35.26	33.41	33.86	33.61	33.21
Baboon	33.35	33.92	35.16	34.64	33.68	34.97	33.06	33.81	33.36	33.53	33.19	33.69
Airplane	33.34	36.42	34.66	35.08	33.64	35.48	33.06	34.81	33.34	33.48	33.29	34.41
Splash	33.39	35.18	33.48	33.58	33.04	34.42	30.14	32.29	33.27	34.12	32.12	33.16

touchy to a miniature change in the plain content over existing methodology [58]–[59].

VI. CONCLUDING REMARKS AND FUTURE PROJECTIONS

The upcoming frameworks will comprise of quantum and the association of traditional and quantum gadgets, and we will deal with these challengers when it marks our society. The proposed structure is appropriate for the traditional and quantum gadgets associations, and real time enciphering solicitations due to small execution time and capable of attacks hostility. The implication of the projected structure of Fig. 4 can be enhanced to a variety of digital mediums, such as audio/video calls, satellite imaginaries, etc.

CONFLICT OF INTEREST

We haven't any conflict of interest to declare concerning the publication of this article.

REFERENCES

[1] A. Belovs, G. Brassard, P. Hoyer, M. Kaplan, S. Laplante, and L. Salvail, "Provably secure key establishment against quantum adversaries," 2017, *arXiv:1704.08182*. [Online]. Available: http://arxiv.org/abs/1704.08182
[2] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," *Theor. Comput. Sci.*, vol. 560, pp. 7–11, Dec. 2014.
[3] A. Ekert and R. Renner, "The ultimate physical limits of privacy," *Nature*, vol. 507, no. 7493, pp. 443–447, Mar. 2014.
[4] Y. Lindell, "How to simulate it-a tutorial on the simulation proof technique," in *Tutorials on the Foundations of Cryptography*. Cham, Switzerland: Springer, 2017, pp. 277–346.
[5] J.-C. Faug'ere, K. Horan, D. Kahrobaei, M. Kaplan, E. Kashefi, and L. Perret, "Fast quantum algorithm for solving multivariate quadratic equations," 2017, *arXiv:1712.07211*. [Online]. Available: http://arxiv.org/abs/1712.07211
[6] A. Gheorghiu, T. Kapourniotis, and E. Kashefi, "Verification of quantum computation: An overview of existing approaches," *Theory Comput. Syst.*, vol. 63, no. 4, pp. 715–808, May 2019.
[7] S.-K. Liao *et al.*, "Satellite-relayed intercontinental quantum network," *Phys. Rev. Lett.*, vol. 120, no. 3, Jan. 2018, Art. no. 030501.
[8] N. Yu, C.-Y. Lai, and L. Zhou, "Protocols for packet quantum network intercommunication," 2019, *arXiv:1903.10685*. [Online]. Available: http://arxiv.org/abs/1903.10685
[9] H. Buhrman, N. Chandran, S. Fehr, R. Gelles, V. Goyal, R. Ostrovsky, and C. Schaffner, "Position-based quantum cryptography: Impossibility and constructions," *SIAM J. Comput.*, vol. 43, no. 1, pp. 150–178, Jan. 2014.
[10] D. Unruh, "Quantum proofs of knowledge," in *Proc. Annu. Int. Conf. Theory Appl. Cryptograph. Techn.* Berlin, Germany: Springer, 2012, pp. 135–152.
[11] D. Boneh, D. Öagdelen. M. Fischlin, A. Lehmann, C. Schaffner, and M. Zhandry, "Random oracles in a quantum worldv," in *Proc. Int. Conf. Theory Appl. Cryptol. Inf. Secur.* Berlin, Germany: Springer, 2011, pp. 41–69,
[12] Z. Ji, H. Zhang, and P. Fan, "Two-party quantum private comparison protocol with maximally entangled seven-qubit state," *Modern Phys. Lett. A*, vol. 34, no. 28, Sep. 2019, Art. no. 1950229.
[13] U. Mahadev, "Classical homomorphic encryption for quantum circuits," in *Proc. IEEE 59th Annu. Symp. Found. Comput. Sci. (FOCS)*, Oct. 2018, pp. 332–338.
[14] B. W. Reichardt, F. Unger, and U. Vazirani, "Classical command of quantum systems," *Nature*, vol. 496, no. 7446, pp. 456–460, Apr. 2013.
[15] D. Boneh and M. Zhandry, "Secure signatures and chosen ciphertext security in a quantum computing world," in *Proc. Annu. Cryptol. Conf.* Berlin, Germany: Springer, 2013, pp. 361–379.
[16] T. Gagliardoni, A. Hälsing, and C. Schaffner, "Semantic security and indistinguishability in the quantum world," in *Proc. Annu. Int. Cryptol. Conf.* Berlin, Germany: Springer, 2016, pp. 60–89.
[17] M. Kaplan, G. Leurent, A. Leverrier, and M. Naya-Plasencia, "Breaking symmetric cryptosystems using quantum period finding," in *Proc. Annu. Int. Cryptol. Conf.* Berlin, Germany: Springer, 2016, pp. 207–237.
[18] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, "Hacking commercial quantum cryptography systems by tailored bright illumination," *Nature Photon.*, vol. 4, no. 10, pp. 686–689, Oct. 2010.
[19] F. Xu, J. M. Arrazola, K. Wei, W. Wang, P. Palacios-Avila, C. Feng, S. Sajeed, N. Lätkenhaus, and H.-K. Lo, "Experimental quantum fingerprinting with weak coherent pulses," *Nature Commun.*, vol. 6, no. 1, p. 8735, Dec. 2015.
[20] A. Cojocaru, L. Colisson, E. Kashefi, and P. Wallden, "On the possibility of classical client blind quantum computing," 2018, *arXiv:1802.08759*. [Online]. Available: http://arxiv.org/abs/1802.08759
[21] J. F. Fitzsimons, "Private quantum computation: An introduction to blind quantum computing and related protocols," *NPJ Quantum Inf.*, vol. 3, no. 1, p. 23, Dec. 2017.

[22] Y. Sun, Y. Chen, H. Ahmad, and Z. Wei, "An asymmetric controlled bidirectional quantum state transmission protocol," *Comput., Mater. Continua*, vol. 59, no. 1, pp. 215–227, 2019.
[23] M. Xiao and D.-F. Zhang, "Practical quantum private Query with classical participants," *Chin. Phys. Lett.*, vol. 36, no. 3, Mar. 2019, Art. no. 030301.
[24] F. Gao, S. Qin, W. Huang, and Q. Wen, "Quantum private Query: A new kind of practical quantum cryptographic protocol," *Sci. China Phys., Mech. Astron.*, vol. 62, no. 7, p. 70301, Jul. 2019.
[25] G. Kumar and H. Saini, "Novel noncommutative cryptography scheme using extra special group," *Secur. Commun. Netw.*, vol. 2017, pp. 1–21, Feb. 2017.
[26] Z. Mahad, M. A. Asbullah, and M. R. K. Ariffin, "Efficient methods to overcome Rabin cryptosystem decryption failure," *Malaysian J. Math. Sci.*, vol. 11, pp. 9–20, 2017.
[27] A. K. Lenstra and E. R. Verheul, "Selecting cryptographic key sizes," *J. Cryptol.*, vol. 14, no. 4, pp. 255–293, 2001.
[28] M. I. G. Vasco, and R. Steinwandt, *Group Theoretic Cryptography*. Boca Raton, FL, USA: CRC Press, 2015.
[29] M. Uno and M. Kano, "Visual cryptography schemes with dihedral group access structure for many images," in *Proc. Int. Conf. Inf. Secur. Pract. Exper.* Berlin, Germany: Springer, 2007, pp. 344–359.
[30] P. Potočnik, "Smallest tetravalent half-arc-transitive graphs with the vertex-stabiliser isomorphic to the dihedral group of order," *J. Combinat. Theory A*, vol. 145, pp. 172–183, Dec. 2017.
[31] S. Lombardo and A. V. Mikhailov, "Reductions of integrable equations: Dihedral group," *J. Phys. A, Math. Gen.*, vol. 37, no. 31, pp. 7727–7742, Aug. 2004.
[32] G. Kuperberg, "A subexponential-time quantum algorithm for the dihedral hidden subgroup problem," *SIAM J. Comput.*, vol. 35, no. 1, pp. 170–188, Jan. 2005.
[33] M. Altunbulak and A. Klyachko, "The pauli principle revisited," *Commun. Math. Phys.*, vol. 282, no. 2, pp. 287–322, Sep. 2008.
[34] N. Wheeler, *Spin Matrices for Arbitrary Spin*. Portland, Oregon: Reed College Physics Department, 2000.
[35] H. M. Waseem and M. Khan, "Information confidentiality using quantum spinning, rotation and finite state machine," *Int. J. Theor. Phys.*, vol. 57, no. 11, pp. 3584–3594, Nov. 2018.
[36] J. Branson, "Quantum physics, derive the expression for rotation operator," Tech. Rep., Apr. 2013. [Online]. Available: https://quantum mechanics.ucsd.edu/ph130a/130_notes/node1.html
[37] A. G. Weber, "The USC-SIPI image database version," USC-SIPI, Los Angeles, CA, USA, Tech. Rep. 315, 1997, pp. 1–24.
[38] I. Younas and M. Khan, "A new efficient digital image encryption based on inverse left almost semi group and lorenz chaotic system," *Entropy*, vol. 20, no. 12, p. 913, 2018.
[39] M. Khan and N. Munir, "A novel image encryption technique based on generalized advanced encryption standard based on field of any characteristic," *Wireless Pers. Commun.*, vol. 109, no. 2, pp. 849–867, Nov. 2019.
[40] M. Khan and T. Shah, "An efficient chaotic image encryption scheme," *Neural Comput. Appl.*, vol. 26, no. 5, pp. 1137–1148, Jul. 2015.
[41] M. Khan and H. M. Waseem, "A novel image encryption scheme based on quantum dynamical spinning and rotations," *PLoS ONE*, vol. 13, no. 11, 0, Art. no. e0206460.
[42] K. M. Ali and M. Khan, "Application based construction and optimization of substitution boxes over 2D mixed chaotic maps," *Int. J. Theor. Phys.*, vol. 58, no. 9, pp. 3091–3117, Sep. 2019.
[43] K. M. Ali, and M. Khan, "A new construction of confusion component of block ciphers," *Multimedia Tools Appl.*, vol. 78, no. 22, pp. 32585–32604, 2019.
[44] M. Khan and H. M. Waseem, "A novel digital contents privacy scheme based on Kramer's arbitrary spin," *Int. J. Theor. Phys.*, vol. 58, no. 8, pp. 2720–2743, Aug. 2019.
[45] S. I. Batool and H. M. Waseem, "A novel image encryption scheme based on arnold scrambling and lucas series," *Multimedia Tools Appl.*, vol. 78, no. 19, pp. 27611–27637, Oct. 2019.
[46] N. Munir and M. Khan, "A generalization of algebraic expression for nonlinear component of symmetric key algorithms of any characteristic p," in *Proc. Int. Conf. Appl. Eng. Math. (ICAEM)*, Sep. 2018, pp. 48–52.
[47] H. M. Waseem and M. Khan, "A new approach to digital content privacy using quantum spin and finite-state machine," *Appl. Phys. B, Lasers Opt.*, vol. 125, no. 2, p. 27, Feb. 2019.
[48] A. Alghafis, H. M. Waseem, M. Khan, and S. S. Jamal, "A hybrid cryptosystem for digital contents confidentiality based on rotation of quantum spin states," *Phys. A, Stat. Mech. Appl.*, Dec. 2019, Art. no. 123908.
[49] H. M. Waseem, M. Khan, and T. Shah, "Image privacy scheme using quantum spinning and rotation," *J. Electron. Imag.*, vol. 27, no. 06, p. 1, Dec. 2018.
[50] M. Khan, T. Shah, and S. I. Batool, "Texture analysis of chaotic coupled map lattices based image encryption algorithm," *3D Res.*, vol. 5, no. 3, p. 19, Sep. 2014.
[51] J. Ahmad and S. O. Hwang, "A secure image encryption scheme based on chaotic maps and affine transformation," *Multimedia Tools Appl.*, vol. 75, no. 21, pp. 13951–13976, Nov. 2016.
[52] U. Arshad, S. I. Batool, and M. Amin, "A novel image encryption scheme based on Walsh compressed quantum spinning chaotic lorenz system," *Int. J. Theor. Phys.*, vol. 58, no. 10, pp. 3565–3588, Oct. 2019.
[53] S. I. Batool, M. Amin, and H. M. Waseem, "Public key digital contents confidentiality scheme based on quantum spin and finite state automation," *Phys. A, Stat. Mech. Appl.*, vol. 537, Jan. 2020, Art. no. 122677.
[54] C. Blondeau, G. Leander, and K. Nyberg, "Differential-linear cryptanalysis revisited," *J. Cryptol.*, vol. 30, no. 3, pp. 859–888, Jul. 2017.
[55] M. Khan and F. Masood, "A novel chaotic image encryption technique based on multiple discrete dynamical maps," *Multimedia Tools Appl.*, vol. 78, no. 18, pp. 26203–26222, Sep. 2019.
[56] M. Khan and T. Shah, "A construction of novel chaos base nonlinear component of block cipher," *Nonlinear Dyn.*, vol. 76, no. 1, pp. 377–382, Apr. 2014.
[57] M. Khan, T. Shah, and S. I. Batool, "A new implementation of chaotic S-boxes in CAPTCHA," *Signal, Image Video Process.*, vol. 10, no. 2, pp. 293–300, Feb. 2016.
[58] M. Khan and Z. Asghar, "A novel construction of substitution box for image encryption applications with gingerbreadman chaotic map and s8 permutation," *Neural Comput. Appl.*, vol. 29, no. 4, pp. 993–999, Feb. 2018.
[59] U. Arshad, M. Khan, S. Shaukat, M. Amin, and T. Shah, "An efficient image privacy scheme based on nonlinear chaotic system and linear canonical transformation," *Phys. A, Stat. Mech. Appl.*, vol. 546, May 2020, Art. no. 123458.

HAFIZ MUHAMMAD WASEEM received the B.S. degree in electronics engineering from the COMSATS Institute of Information Technology, Abbottabad, Pakistan, in 2014, and the M.S. degree in electrical engineering from the Institute of Space Technology (IST), Islamabad, Pakistan, in 2019. He is currently working as a Research Assistant at IST. His research interests include quantum information theory, information security, and cryptography, development of quantum cryptosystems, artificial intelligence, and cybersecurity.

ABDULLAH ALGHAFIS received the B.Sc. degree in electrical engineering from Pensilvania, USA, in 2009, the M.B.A. degree from Alabama, USA, in 2011, and the M.Sc. and Ph.D. degrees in electrical engineering from the University of Cape Town, in 2015 and 2018, respectively. He is currently a Researcher and the Director of the Command and Control Department, Information Technology Research Institute (CITRI), King Abdulaziz City for Science and Technology (KACST), Riyadh, Saudi Arabia. He has more than eight years of experience in industry and academia in Saudi Arabia and South Africa relating to telecommunications, software development, and management. His research results have been published in leading journals and conferences. His research interests include secure communication systems and radar systems.

MAJID KHAN received the M.S. and Ph.D. degrees in mathematics from Quaid-e-Azam University, Islamabad, in 2008 and 2015, respectively. He is currently an Assistant Professor with the Department of Applied Mathematics and Statistics, Institute of Space and Technology, Islamabad, Pakistan. His area of specialization is cryptography. He is also working in chaotic cryptography, quantum cryptography, and artificial intelligence based-encryption mechanisms.