IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received January 7, 2021, accepted January 24, 2021, date of publication January 27, 2021, date of current version February 4, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3054952

A Quantum Chaotic Image Cryptosystem and Its Application in IoT Secure Communication

HEPING WEN[1,2], CHONGFU ZHANG[1,2], (Senior Member, IEEE), PING CHEN[3], RUITING CHEN[1], JIAJUN XU[1], YUNLONG LIAO[1], ZHONGHAO LIANG[1], DANZE SHEN[1], LIMENGNAN ZHOU[1,2], AND JUXIN KE[4]

[1]School of Electronic Information, University of Electronic Science and Technology of China, Zhongshan Institute, Zhongshan 528402, China
[2]School of Information and Communication Engineering, University of Electronic Science and Technology of China, Chengdu 611731, China
[3]School of Automation, Guangdong University of Technology, Guangdong 510006, China
[4]The Center of Information and Technology, Dongguan Polytechnic, Dongguan 523808, China

Corresponding author: Chongfu Zhang (cfzhang@uestc.edu.cn)

This work was supported in part by the National Science Foundation of China under Grant 62071088, Grant 61901096, and Grant 61571092; in part by the Project for National Key Research and Development Program of China under Grant 2018YFB1801302; in part by the Project for Innovation Team of Guangdong University under Grant 2018KCXTD033; in part by the Project for Zhongshan Social Public Welfare Science and Technology under Grant 2019B2007; in part by the Zhongshan Innovative Research Team Program under Grant 180809162197886; in part by the Research Project for Talent of UESTC Zhongshan Institute under Grant 418YKQN07 and Grant 419YKQN23; and in part by the Natural Science Project for Young Innovative Talents by the Department of Education of Guangdong Province under Grant 2019KQNCX191.

ABSTRACT In the Internet of Things environment, the secure transmission of digital images has attracted much attention. To improve the confidentiality, we propose an image cryptosystem adopting a quantum chaotic map and the certain security-enhanced mechanisms. Firstly, we use the good random characteristics of quantum chaotic sequences to enhance security performance. Then, we introduce a plaintext correlation mechanism and a diffusion-permutation-diffusion structure in the cryptosystem. Finally, we verify the cryptosystem on a common secure communication platform. The theoretical and statistical analysis results demonstrate that the cryptosystem has excellent performance and can resist various cryptographic attacks. Moreover, feasibility and effectiveness of the image cryptosystem are verified on the Internet of Things secure communication experimental platform. It proves that the proposed image cryptosystem is a preferred and promising secure communication technology solution.

INDEX TERMS Secure communication, image encryption, Internet of Things, quantum chaos.

I. INTRODUCTION

With the vigorous development of emerging information technologies such as Big Data, Internet of Things (IoT), Artificial Intelligence, and 5G communication, the information security of multimedia, especially digital images, has attracted particular attention [1]–[3]. Digital images have some unique properties, such as strong correlation between adjacent pixels and high redundancy. In terms of real-time encryption, traditional cryptosystems such as DES, IDEA and AES face challenges [4]–[6]. Chaos owns the characteristics of high sensitivity to control parameters and initial values, ergodicity of modes, and dense periodic points. It has many similarities to the confusion and diffusion in Shannon's cryptographic theory [7]–[11]. Thus, image encryption technology based on chaos theory has attracted much attention [2], [3], [5], [12], [13]. Furthermore, the rapid development of Internet of Things applications makes its communication and transmission security issues more attractive [7], [14], [15]. Therefore, it is very necessary to implement effective security and confidentiality technology for the transmission in IoT [5], [16], [17].

For the image cryptosystems, the ''permutation-diffusion'' is widely used as the most basic algorithm structure [4], [5], [12], [13]. In 2014, [17] systematically designed a new method for constructing a robust 1D chaotic system, and proposed an image cipher based on the permutation-diffusion structure. The experimental results verified its excellent encryption performance. In 2018, [18] proposed an image cryptosystem using multiple chaotic systems and bit-plane decomposition, which uses bit-level permutation and diffusion encryption to enhance the confusion and diffusion

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

effects. However, due to lack of authoritative security standards for chaotic cryptographic algorithms, these chaotic image encryption algorithms have been pointed out that they cannot resist cryptographic attacks [4], [19], including ciphertext-only attacks, known-plaintext attacks, chosen-plaintext attacks and chosen-ciphertext attack. In 2019, [7] pointed out that [18] has security flaws. The algorithm can be cracked by merely low computational complexity and data complexity. Therefore, it is particularly critical to improve the security performance to resist cryptographic attacks, which is also one of the important factors that determines the technology from theoretical research to practical application [20].

In view of the cryptanalysis of digital image encryption algorithms in the world, the insecurity of current algorithm is mainly caused by two points [21], [22]. First, the security of the chaotic system used in encryption scheme is insufficient as studied in [23], [24]. It is reported that the dynamics of some chaotic systems for encryption are not complex enough, thus the risk of being estimated or identified increases [25]. Second, the encryption algorithm structure has security defects, which cannot resist cryptanalysis algorithm attacks [26]. For example, the chaotic key sequence generation process is independent of plaintext, which makes it easy to be attacked by plaintext attacks [4], [26]. The essential reason is that the encryption process is independent of plain images, so the cryptosystem exists equivalent keys [4], [7]. In addition, the computational complexity of the image cryptosystem and its hardware system technology implementation are less considered [23], [27]. The above factors are critical for promoting image encryption technology from theory to application, and it is worthy of in-depth study [20], [28].

This paper proposes a secure image cryptosystem using quantum chaos and verifies its feasibility on the IoT experimental platform. A quantum logistic chaotic map is selected to generate the *PRNS* (pseudo-random number sequence) for encryption. The *PRNS* has been verified to have better randomness, and is suitable for information security protection in cryptographic systems. To enhance the ability of encryption algorithms against cryptographic attacks, we propose an image cryptosystem of the structure ''diffusion-permutation-diffusion''. By means of permutation, the confusion and diffusion performance of encryption algorithm are enhanced, and the ability of cipher image to resist various noise attacks is improved. The diffusion method of ciphertext feedback can traverse the information of the plaintext and the key to be distributed to all the ciphertext pixels, so as to achieve a better encryption effect. Simulation results show that plaintext correlation to generate chaotic key sequences and ciphertext feedback diffusion encryption security mechanism can improve the security of the encryption scheme performance. Finally, we verify the proposed image cryptosystem on a general experimental platform of the Internet of Things. The experiments verified the feasibility of the encryption algorithm used in the Internet of Things environment. The contributions of this paper are mainly reflected in:

1. Improve the security of the image cryptosystem. Based on the latest cryptanalysis research results [29]–[35], we propose a security-enhanced version. Adopting the diffusion-permutation-diffusion structure and a plaintext-related mechanism to resist chosen-plaintext/ciphertext attacks.

2. Ensure the efficiency of the image cryptosystem. Compared with similar algorithms, only one quantum chaotic system is used and more streamlined operations are considered to bring lower computational complexity.

3. Realize the hardware technology implementation of the image cryptosystem. It should be admitted that hardware technology implementation is more difficult and requires more work. As far as we know, this is also relatively lacking in existing research [12], [24]. In fact, the realization of the hardware system is an extremely important part of the technology from theoretical research to practical application.

In summary, our proposed image cryptosystem has the advantages of high security, low computational complexity and technical realization. In addition, we provide the experimental results of security performance analysis and hardware technology implementation.

II. QUANTUM LOGISTIC CHAOTIC MAP

The quantum logistic map has more complex dynamics and quantum properties [6]. The coupling of the dissipative quantum system and the harmonic oscillator path will produce a quantum logistic map with quantum correction. Goggin et al, quantified the classic Logistic mapping through the recoil rotor model, and produced the corresponding iterative equations of the quantum logistic mapping as:

$$\begin{cases} x_{n+1} = r(x_n - |x_n|^2) - r y_n \\ y_{n+1} = -y_n e^{-2\beta} + e^{-\beta} r[(2 - x_n - x_n^*) y_n - x_n z_n^* - x_n^* z_n] \\ z_{n+1} = -z_n e^{-2\beta} + e^{-\beta} r[2(1 - x_n^*) z_n - 2 x_n y_n - x_n] \end{cases} \quad (1)$$

where $x =< a >$, $y =< \delta a^{\dagger} \delta a >$, $z =< \delta a \delta a >$, r is the control parameter, and β is the dissipation parameter. x_n^*, z_n^* are respectively the conjugate complex numbers of x_n, z_n. Normally, when x_n, z_n are both plurals, x_n^*, z_n^*, y_n are also complex numbers. When $x_n \in [0, 1]$, $y_n \in [0, 0.1]$, $z_n \in [0, 0.2]$, $\beta \in [6, +\infty]$, $r \in [0, 4]$, Eq. (1) is in a chaotic state. Reference [36] proved that when $r = 3.99$ and $\beta > 6$, the randomness of quantum chaotic mapping is better, and the generated chaotic sequence can pass the strict TESTU01 test [37]. The iterative timing diagram of the quantum chaos given in Eq. (1) is shown in Fig. 1.

III. THE PROPOSED IMAGE CRYPTOSYSTEM

We propose a chaotic image cryptosystem based on the ''diffusion-permutation-diffusion'' structure. To improve the security, we adopt a plaintext correlation mechanism to generate chaos-based *PRNS* and the ciphertext feedback diffusion algorithm. The block diagrams of the encryption and

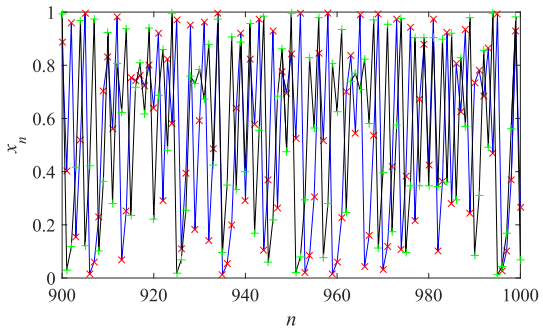


FIGURE 1. Iterative sequence diagram of quantum Logistic chaotic map.

decryption machines of the proposed cryptosystem are respectively shown in Fig. 2(a) and Fig. 2(b).

- *The secret key*

The secret key of the cryptosystem includes the 256-bit hash of the plain image and three initial values of the quantum chaos. The specific key space is $\{hash256, x(0), y(0), z(0)\}$, where $hash256$ is the 256-bit hash value, and $x(0)$, $y(0)$, $z(0)$ are the initial values of Eq. (1).

- *The encryption machine*

The specific steps of the encryption machine are described as follows:

Step 1: *Quantum chaotic encryption sequences*

To resist differential attacks, the hash value of plaintext is used to dynamically disturb the initial values of the quantum chaos. Thus, the corresponding key sequences of different plaintexts are not fixed. The method of dynamic disturbance is as follows:

$$\begin{cases} x'(0) = x(0) + \sum_{i=1}^{5} h_i \times 10^{-5} \\ \qquad + \dfrac{h_6 \oplus h_7 \oplus \cdots \oplus h_{10}}{10^8} \\ y'(0) = y(0) + \sum_{i=1}^{15} h_i \times 10^{-5} \\ \qquad + \dfrac{h_{16} \oplus h_{17} \oplus \cdots \oplus h_{20}}{10^8} \\ z'(0) = z(0) + \sum_{i=21}^{25} h_i \times 10^{-5} \\ \qquad + \dfrac{h_{26} \oplus h_{27} \oplus \cdots \oplus h_{32}}{10^8} \end{cases} \tag{2}$$

where $x'(0)$, $y'(0)$, $z'(0)$ are the updated initial values of the quantum chaos after the disturbance. Obviously, the updated initial values will change with the different plain images.

Next, the chaotic sequence is preprocessed. To avoid the harmful transient effect of chaotic mapping, the previous l=300 iterative sequences are usually discarded. The diffusion sequence generated by the quantum logistic chaotic map is

$$\begin{cases} kd_1 = mod(fix(x_i \times 10^8), 256) \\ kd_2 = mod(fix(z_i \times 10^{10}), 256) \end{cases} \tag{3}$$

where $i = 1, 2, \ldots, H \times W$ is used for forward and backward diffusion encryption respectively, and the sequence length is as long as the image size $H \times W$. Similarly, the permutation sequence is generated by

$$\begin{cases} [value_1, kp_1] = sort(y(1:H)) \\ [value_2, kp_2] = sort(y(H+1:H+W)) \\ [value_3, kp_3] = sort(y(H+W+1:H+9W)) \end{cases} \tag{4}$$

where y is the sequence of the quantum chaotic map after discarding l=300, and the total length is $H + 9W$. kp_1, kp_2, and kp_3 are the index sequences of pixel rows, pixel columns, and bit columns generated by the sort function. The lengths of the index sequences are H, W and $8W$, respectively, and $value_1$, $value_2$, and $value_3$ are sorted numerical sequences.

Step 2: *Forward diffusion*

Forward diffusion is to diffuse the input image information from the first pixel to the last pixel by means of ciphertext feedback. The first pixel encryption process is expressed as:

$$\begin{aligned} C_1(i) = mod(&mod(P(1) + kd_1(1), 256) \\ &\oplus kd_1(1) + C_0, 256) \end{aligned} \tag{5}$$

where P is a given plain image, C_1 is the image after forward diffusion; kd_1 is the first key sequence generated by quantum chaos, and C_0 is the initial key of forward diffusion, with a value of [0, 255]. The *i-th* pixel encryption process is expressed as:

$$\begin{aligned} C_1(i) = mod(&mod(P(i) + kd_1(i), 256) \\ &\oplus kd_1(i) + C_1(i-1), 256) \end{aligned} \tag{6}$$

where $i = 2, 3, \ldots, HW$, the encrypted pixel values of the diffused ciphertext C_1 are obtained by iteration in turn.

Step 3: *Pixel permutation*

The pixel position of the image C_1 after forward diffusion encryption is permuted, which is described as follows:

$$C_2(i, j) = swap(C_1(kp_1(i), kp_2(j)), C_1(i, j)) \tag{7}$$

where $i = 1, 2, \ldots, H, j = 1, 2, \ldots, W$, $swap(\cdot)$ is the exchange function of element values, and C_2 is the image after pixel-level permutation.

Step 4: *Bit permutation*

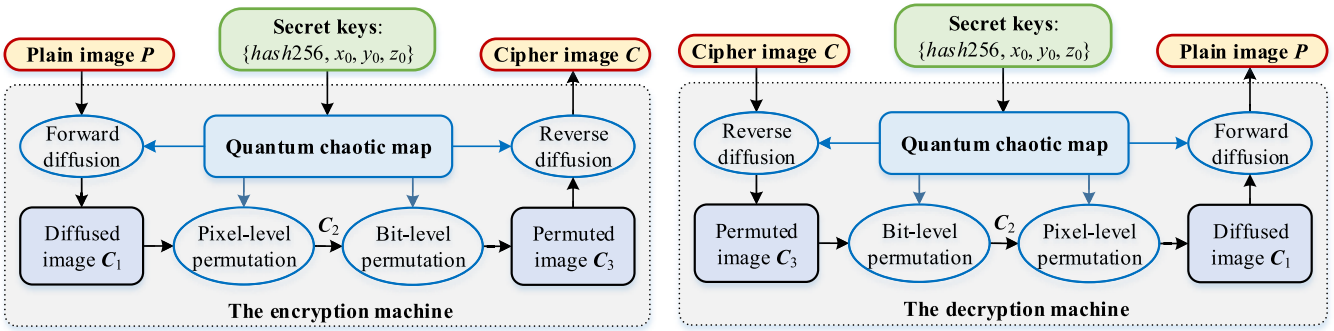
The image C_2 after pixel permutation is performed bit-level permutation, which is described as follows:

$$C_3(i, j) = swap(C_2(:, kp_3(k)), C_2(:, k)) \tag{8}$$

where $k = 1, 2, \ldots, 8W$. C_3 is the image after bit-level permutation. Note that in the second round of permutation, the bit-level image is expanded according to the row-invariant rule, so the permutation is only for the expanded column permutation.

Step 5: *Backward diffusion*

Different from forward diffusion, backward diffusion uses ciphertext feedback to diffuse the input image information from the last pixel to the first pixel. It further enhances the confusion and diffusion characteristics through forward and backward complement each other.



(a) The encryption process

(b) The decryption process

FIGURE 2. The block diagrams of the encryption and decryption machines.

When $i=HW$,

$$C(i) = mod(mod(C_3(i) + kd_2(i), 256) \oplus kd_2(i) + C_{end}, 256) \quad (9)$$

Then, when $i=HW-1, \ldots, 2, 1$,

$$C(i) = mod(mod(C_3(i) + kd_2(i), 256) \oplus kd_2(i) + C(i+1), 256) \quad (10)$$

where C is the final ciphertext image, C_{end} is the backward diffusion initial value key, and kd_2 is the encryption sequence generated by quantum chaos.

- *The decryption machine*

The block diagram of the decryption machine is shown in Fig. 2(b). We should pay attention to two points. One is that the operation order of each module should be reversed. The backward diffusion, bit permutation, pixel permutation, and forward diffusion should be performed in sequence. The second is that the order of pixel iteration in diffusion is also reversed.

- *Its application in IoT*

This image cryptosystem can be applied in a general IoT secure communication scenario. A schematic diagram for IoT secure communication is illustrated in Fig. 3. Both the sending end and the receiving end are embedded terminals, which can store, display and transmit digital images. To enhance the confidentiality of information, we encrypt the digital image at the sending end so that the information transmitted over the network will not be stolen by hackers or attackers. When the legitimate user at the receiving end obtains the ciphertext image, the original plaintext information can be effectively restored by the correct key. Thus, our proposed image cryptosystem can be used in various IoT secure communication environments.

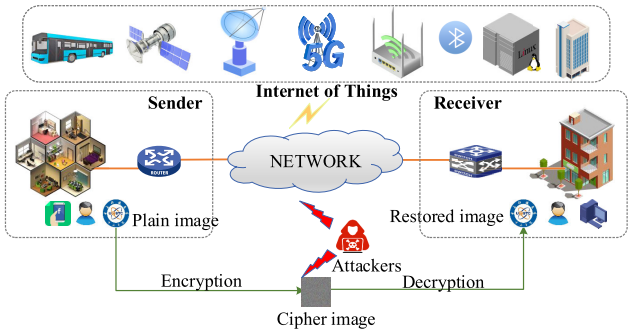


FIGURE 3. A diagram of the image cryptosystem used in IoT secure communication.

IV. EXPERIMENTAL VERIFICATION AND DISCUSSION

A. EXPERIMENT SETTINGS AND RESULTS

Firstly, we conduct simulation verification on the proposed image cryptosystem based on a PC (personal computer) with MATLAB r2018b. The running PC is installed with Windows 10 64-bit OS (operating system) with Intel i7-8565U CPU @ 1.80GHz 1.99GHz and 8GB memory. We select some standard images as the testing images for experiments, including MISC image database and other images. The parameters of the quantum chaotic map in the Eq. (1) are given, which r=3.99 and β=6. The experimental results before and after encryption are given in Figs. 4(a)-(f) respectively. Fig. 6 and Table 1 show the comparison result of the operating efficiency of this paper and several other similar references. It can be seen that our cryptosystem has lower computational complexity. Moreover, as the image size increases, our performance advantage becomes more prominent.

Moreover, to verify effectiveness and feasibility of the cryptosystem, we carry out experiments on the Internet of Things experimental platform based on ARM Embedded System. This digital image secure communication system based on the Internet of Things is mainly composed of two sets of ARM Embedded System development boards and an Ethernet wireless router TP-LINKTL-WR886N450M. The ARM development main board is NanoPC-T2, the chip is S5P4418 of cortex-A9 architecture, and the operating system is 64-bit Ubuntu16.04, which is equipped with a 10.5-inch LCD display. The wireless router is used for network communication at the sending end and the receiving end, and the address is obtained by DHCP, which are 192.168.1.100 and 192.168.1.101 respectively. The sending

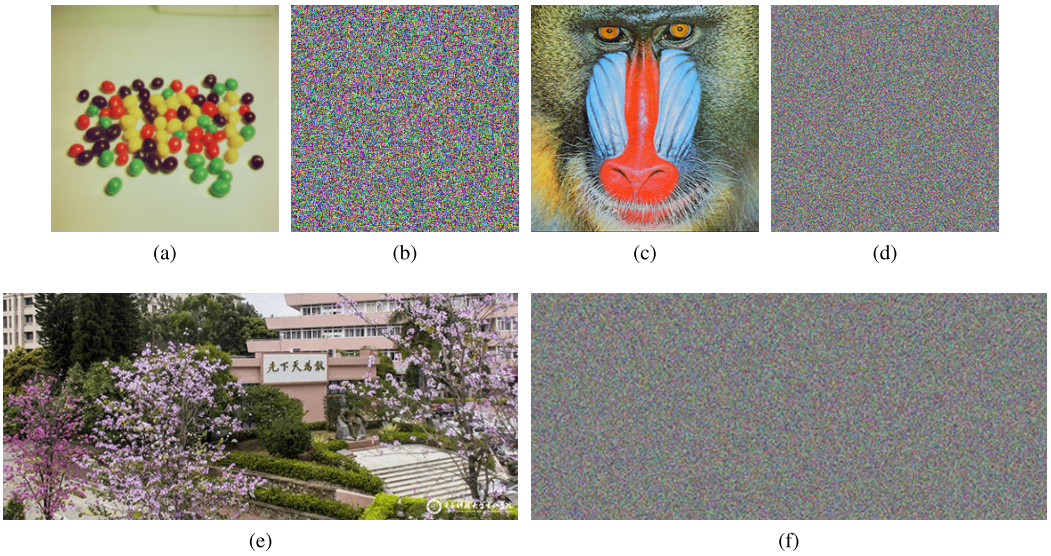


FIGURE 4. The experimental images before and after encryption: a) $1^{\#}$ plain image; b) $1^{\#}$ cipher image; c) $2^{\#}$ plain image; d) $2^{\#}$ cipher image; e) $3^{\#}$ plain image; f) $3^{\#}$ cipher image.

TABLE 1. Time complexity versus similar image cryptosystems.

Operations	This paper	Ref. [38]	Ref. [39]	Ref. [16]	Ref. [40]
add/sub	$4N+1$	$2N^2$	$10N+\frac{7}{2}N^2$	$44N$	$13N$
mul/div	$3N^2+3N+1$	N^2	$13N+\frac{7}{2}N^2$+1	$68N$	$10N$
mod	$2N+2$	N^2	$2N$	N	N
bitxor	$3N-1$	$2N$	$8N$	N	N
floor/fix/round/reashape	N	$6N^2+9N$	$12N$	$7N^2+4N$	$4N^2+13N$

end is responsible for the display, encryption and transmission of the plain images, while the receiving end stores, displays and decrypts the received cipher images. The experimental hardware platform and experimental results are shown in Figs. 5(a)-(e). As shown in Fig. 5, the encrypted images effectively hide the information of the original images, which improves the security of secure communication. In addition, the experimental environment is aimed at common IoT secure communication platforms, so it is more universal.

Although the experimental results of Fig. 4 and Fig. 5 are formally consistent, the latter is much more technically difficult. Our purpose is to illustrate the feasibility of the hardware system implementation of the proposed image cryptosystem. In fact, ARM embedded hardware implementation requires greater workload. And this part of the work has effectively verified its technical feasibility, so it can be regarded as a technical solution that is expected to be applied to the secure communication of the Internet of Things.

B. THEORETICAL AND STATISTICAL SECURITY ANALYSIS

1) HISTOGRAM

The histogram reflects the distribution characteristics of digital image pixel value. Figs. 7(a)-(h) shows the images before and after encryption using our proposed scheme and their corresponding histograms. It can be seen that the cryptographic image is noise-like and greatly hides the pixel value information of the image. Therefore, the scheme has a good encryption effect. This makes it difficult for attackers to obtain valid information through cipher images. Therefore, our proposed image encryption scheme can resist statistical analysis attacks.

2) ENCRYPTION QUALITY ANALYSIS

We adopt two indicators *PSNR* (Peak Signal to Noise Ratio) and *SSIM* (structural similarity index metric) to test and analyze the encryption quality, defined as [27], [41]:

$$PSNR = 10 \times \log_{10} \frac{255^2}{MSE}(dB) \tag{11}$$

$$MSE = \frac{1}{M \times N \times 3} \sum_{i=1}^{H} \sum_{j=1}^{W} \sum_{k=1}^{3} (P(i,j,k) - C(i,j,k))^2 \tag{12}$$

where H and W are the height and width of the color images P and C respectively. The larger the value of *PSNR*, the better the encryption quality. And *SSIM* is given

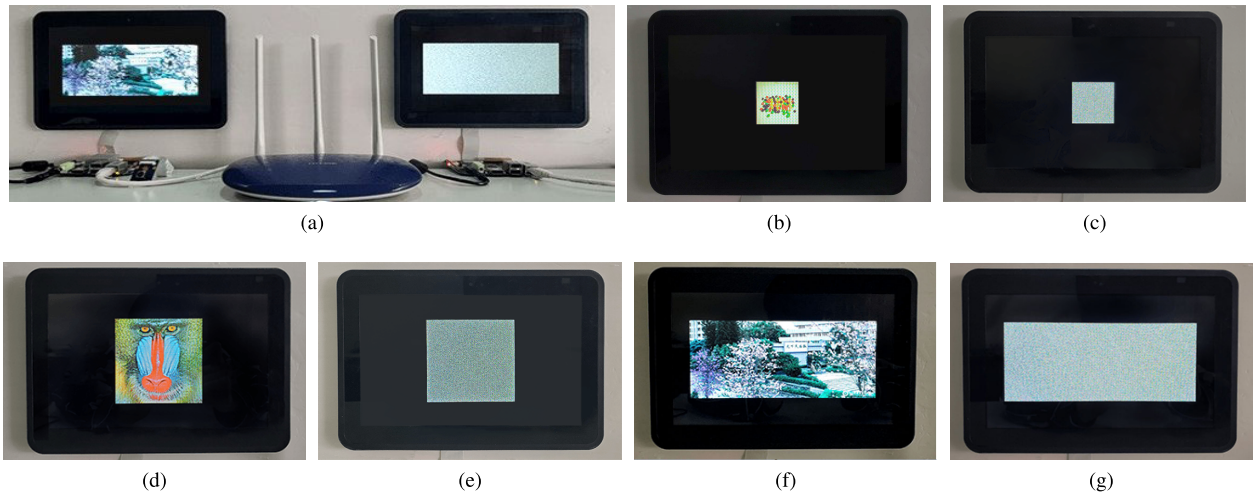


FIGURE 5. Experimental results in IoT secure communication platform: a) The overall physical diagram; b) 1# plain image; c) 1# cipher image; d) 2# plain image; e) 2# cipher image; f) 3# plain image; g) 3# cipher image.

TABLE 2. The PSNR of the cipher images with different cryptosystems.

Images	This paper	Ref. [44]	Ref. [39]	Ref. [16]	Ref. [45]	Ref. [38]
4.1.01.tiff	30.0113	30.0140	29.9726	29.9660	29.9737	29.9005
4.1.02.tiff	32.9091	32.8400	32.8847	32.7998	32.8399	32.8829
4.2.01.tiff	25.9461	25.9463	25.9466	25.9388	25.9415	25.9416
House.tiff	26.5273	26.5161	26.5159	26.5268	26.5264	26.5238
Fig. 4(e)	27.9873	27.9871	27.9769	27.9820	27.9950	27.9874

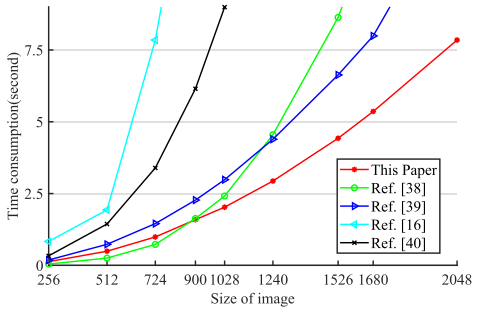


FIGURE 6. Running times.

by [42], [43]:

$$SSIM(P, C) = \frac{2\mu_P\mu_C + A_1}{\mu_P^2 + \mu_C^2 + A_1} \times \frac{2\sigma_P\sigma_C + A_2}{\sigma_P^2 + \sigma_C^2 + A_2} \times \frac{\sigma_{PC} + A_3}{\sigma_P\sigma_C + A_3} \quad (13)$$

where μ_P and μ_C are the average values of image P and C, σ_P, σ_C are their variances, σ_{PC} is the covariance between P and C; A_1, A_2, A_3 are constants, A_1=$(0.01L)^2$, A_2=$(0.03L)^2$, A_3=$\frac{A_2}{2}$, L=255. Tables 2 and 3 show the encryption quality of our proposed scheme has better cryptographic performance.

3) ADJACENT PIXEL CORRELATION

Strong correlation between adjacent pixels is a basic characteristic of natural images. And encryption improves security by breaking the correlation. The correlation coefficient r_{vw} is defined as [16]:

$$\begin{cases} r_{vw} = \dfrac{cov(v, w)}{\sqrt{D(v)}\sqrt{D(w)}} \\ cov(v, w) = \dfrac{1}{N}\sum_{i=1}^{N}(v_i - E(v))(w_i - E(w)) \\ D(v) = \dfrac{1}{N}\sum_{i=1}^{N}(v_i - E(v))^2 \\ E(v) = \dfrac{1}{N}\sum_{i=1}^{N} v_i \end{cases} \quad (14)$$

where $cov(v, w)$ is the covariance between the image v and w, and $E(v)$ and $D(v)$ are the expected and mean square error of image v, respectively. We test the correlation coefficients of some images in different directions. The experimental results are shown in Figs. 8(a)-(h). As can be seen, the plain images have strong correlation between adjacent pixels in different directions, while the correlation of the corresponding encrypted images is almost 0. Therefore, there is no correlation between all the pixel values of cipher-images.

TABLE 3. The SSIM versus similar cryptosystems.

Images	This paper	Ref. [38]	Ref. [39]	Ref. [16]	Ref. [45]	Ref. [38]
4.1.01.tiff	0.0232	0.0243	0.0236	0.0227	0.0236	0.0241
4.1.02.tiff	0.0171	0.0178	0.0188	0.0179	0.0168	0.0189
4.2.01.tiff	0.0301	0.0297	0.0301	0.0296	0.0296	0.0302
House.tiff	0.0286	0.0291	0.0294	0.0308	0.0289	0.0286
Fig. 4(e)	0.0235	0.0237	0.0224	0.0233	0.0235	0.0242

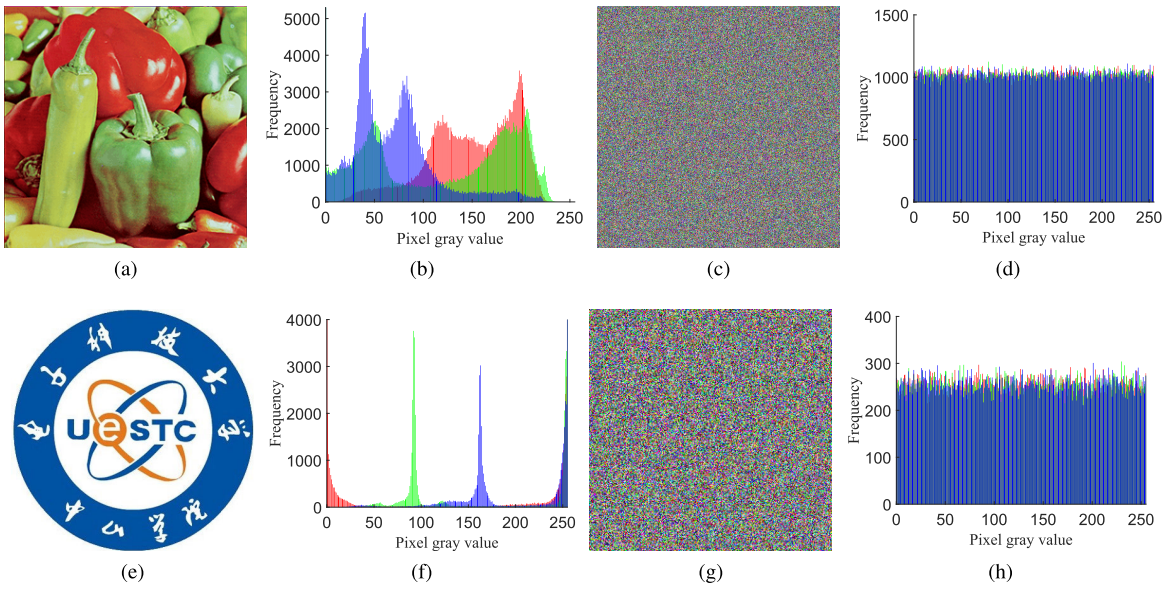


FIGURE 7. The histograms of images before and after encryption: a) $4^{\#}$ plain image; b) The histogram of a); c) $4^{\#}$ cipher image; d) The histogram of c); e) $5^{\#}$ plain image; f) The histogram of e); g) $5^{\#}$ cipher image; h) The histogram of g).

Here, we select several typical digital images for experiments. Table 4 is the result of the correlation experiment of adjacent pixels. Thus, our proposed image cryptosystem is proved to be effective in terms of the correlation coefficient.

4) DIFFERENTIAL ANALYSIS

The sensitivity to secret key and plain image with an encryption system determines its ability to resist differential analysis. In image encryption algorithms, we adopt *NPCR* (Number of Pixels Change Rate) and *UACI* (Unified Average Changing Intensity) to determine the encryption performance. The calculation formula is [24]:

$$\begin{cases} NPCR = \dfrac{1}{H \times W} \displaystyle\sum_{i=1}^{H} \sum_{j=1}^{W} D_{ij} \times 100\% \\ UACI = \dfrac{1}{H \times W} \displaystyle\sum_{i=1}^{H} \sum_{j=1}^{W} \left(\dfrac{v(i,j) - v'(i,j)}{255} \right) \times 100\% \end{cases} \tag{15}$$

where $D_{ij} = \begin{cases} 1, v(i,j) \neq v'(i,j) \\ 0, v(i,j) = v'(i,j) \end{cases}$. v and v' are the cipher images before and after the plain image changed by one pixel.

Firstly, we evaluate the sensitivity of the key. In our encryption system, there are 3 keys (x_0, y_0, z_0) associated with the quantum chaotic map. Thus, a set of 200 keys is randomly selected from the key space, expressed as $key(i) = (x_0(i), y_0(i), z_0(i))$, where $i = 1, 2, 3, \ldots, 200$. We update a new key by adding 10^{-10} to the x_0 of the previous key to encrypt the same image. For example, the first time we choose $key(1) = (0.1, 0.02, 0.002)$, the second time we select $key(2) = (0.1 + 10^{-10}, 0.02, 0.002)$. Then, we calculate 200 pairs of *NPCR* and *UACI* according to the Eq. (15). The sensitivity of other keys y_0, z_0 is tested in the same way. The average values of 200 pairs of *NPCR* and *UACI* are shown in Table 5. We can see that these test values are very close to the theoretical values.

In order to visualize the key sensitivity, we choose exactly the same experimental parameters. Figs. 9(b) and (c) show the cipher images of Fig. 9(a) with $key(1)$ and $key(2)$, respectively. Fig. 9(d) is a different result of the two images between Figs. 9(b) and (c), and Fig. 9(e) is the corresponding histogram. We can conclude that even if the secret key changes slightly, the cipher -images will change dramatically. This verifies that the proposed image cryptosystem has an avalanche effect on plaintext and keys.

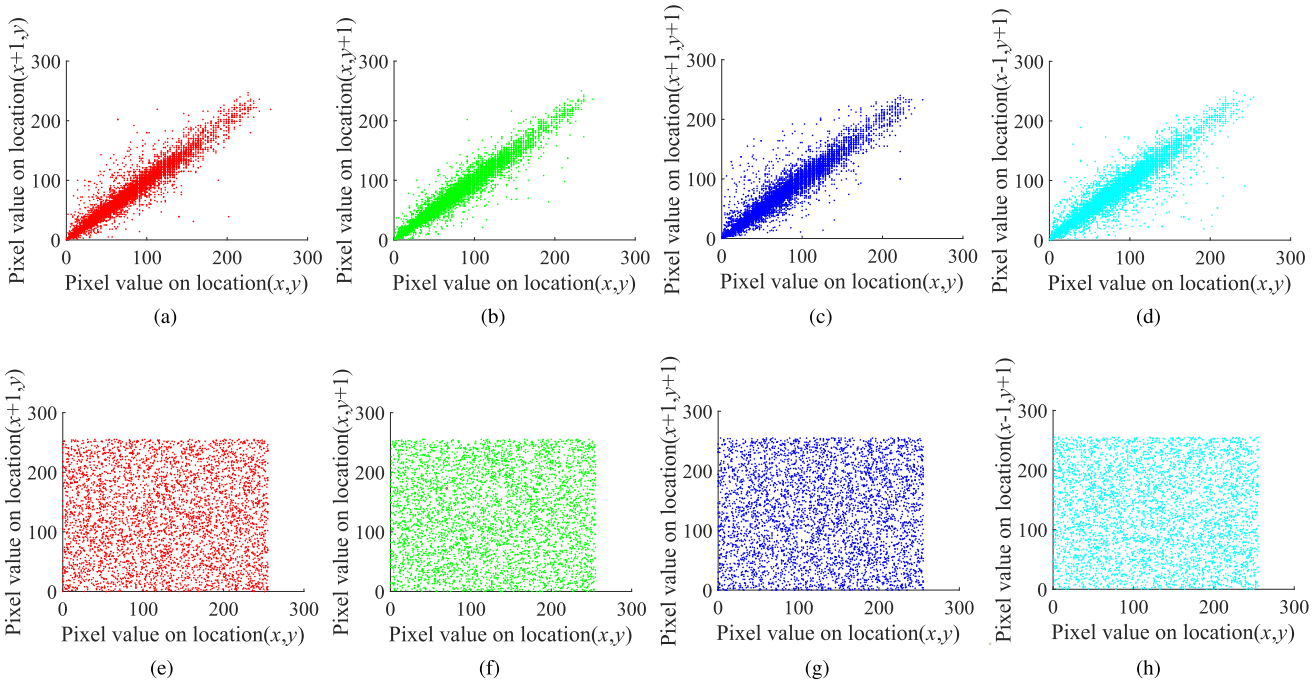


FIGURE 8. The correlation characteristic: a) Horizontal direction of plaintext; b) Vertical direction of plaintext; c) Positive diagonal direction of plaintext; d) Opposite angular direction of plaintext; e) Horizontal direction of ciphertext; f) Vertical direction of ciphertext; g) Positive diagonal direction of cihpertext; h) Opposite angular direction of ciphertext.

TABLE 4. Correlation coefficients in four directions before and after encryption.

Images		Plain-image				Cipher-image			
		V	H	D	A	V	H	D	A
4.1.01.tiff	R	0.9614	0.9745	0.9454	0.9386	0.0099	-0.0096	-0.0156	-0.0086
	G	0.9628	0.9722	0.9579	0.9479	-0.0132	-0.0133	-0.0445	-0.0208
	B	0.9492	0.9598	0.9377	0.9417	0.0221	0.0310	0.0047	0.0160
4.1.06.tiff	R	0.9330	0.9572	0.9217	0.9081	-0.0134	-0.0012	-0.0130	-0.0456
	G	0.9452	0.9680	0.9252	0.9172	0.0317	-0.0067	-0.0275	0.0245
	B	0.9358	0.9646	0.9164	0.9169	0.0035	0.0249	-0.0054	0.0009
4.2.03.tiff	R	0.8684	0.9278	0.8600	0.8438	-0.0420	-0.0015	-0.0104	-0.0013
	G	0.7502	0.8724	0.7301	0.7272	0.0221	-0.0086	0.0073	0.0046
	B	0.8733	0.9188	0.8553	0.8446	-0.0231	0.0171	-0.0294	0.0289
4.2.05.tiff	R	0.9577	0.9762	0.9270	0.9434	0.0080	-0.0199	0.0030	0.0279
	G	0.9675	0.9618	0.9304	0.9363	0.0025	-0.0323	-0.0051	-0.0051
	B	0.9328	0.9689	0.9203	0.8891	-0.0020	0.0408	-0.0001	0.0101
Fig. 4(e)	R	0.9150	0.9279	0.8739	0.8731	0.0772	0.0742	0.0737	0.0750
	G	0.9043	0.0933	0.8856	0.8841	0.0720	0.0905	0.0665	0.0707
	B	0.9817	0.9923	0.9810	0.9755	-0.0043	-0.0176	-0.0362	-0.0090

Similarly, we test the sensitivity of plain images. On the premise of the same key, we select and change only a certain pixel value of a plain image. For example, by changing the pixel values of the same position (30, 27) from 154 to 155, the overall effect is also shown in Fig. 9. Moreover, we calculate the values of 200 pairs of *NPCR* and *UACI*, the results are shown in Table 6. As can be shown, the values of *NPCR* and *UACI* in our cryptosystem are both close to their theoretical values. This shows that the cryptosystem is also sensitive to plain images.

5) INFORMATION ENTROPY

Generally, information entropy is used as a measure of image uncertainty. For an encryption system, the greater the entropy of the cipher image is, the better the encryption performance is. The formula of information entropy with 8-bit grayscale

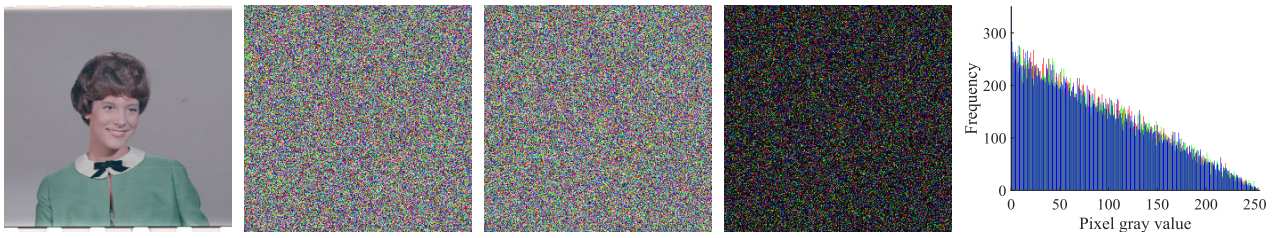


FIGURE 9. The differential cipher image and its histogram: a) $6^{\#}$ plain image; b) $6^{\#}$ ciphertext with *key*(1); c) $6^{\#}$ ciphertext with *key*(2); d) Difference of b) and c); e) Histogram of d).

TABLE 5. Average value of 200 pairs of NPCR and UACI for testing key sensitivity.

Images	NPCR(99.6094%)			UACI(33.4635%)		
	R	G	B	R	G	B
4.1.01.tiff	99.6122	99.6131	99.6106	33.4389	33.5038	33.5120
4.1.06.tiff	99.6102	99.6110	99.6070	33.4108	33.4747	33.4650
4.2.03.tiff	99.6110	99.6094	99.6090	33.4603	33.4525	33.4525
4.2.05.tiff	99.6101	99.6095	99.6103	33.4664	33.4650	33.4851
Fig. 4(e)	99.6104	99.6170	99.6085	33.4640	33.5086	33.4615

TABLE 6. The average values of 200 pairs of NPCR and UACI for testing the sensitivity of the flat image.

Images	NPCR(99.6094%)			UACI(33.4635%)		
	R	G	B	R	G	B
4.1.01.tiff	99.6070	99.6120	99.6084	33.4395	33.5031	33.5017
4.1.06.tiff	99.6098	99.6113	99.6084	33.4191	33.4841	33.4751
4.2.03.tiff	99.6092	99.6102	99.6102	33.4681	33.4528	33.4507
4.2.05.tiff	99.6090	99.6102	99.6093	33.4641	33.4580	33.4833
Fig. 4(e)	99.6085	99.6082	99.6092	33.4811	33.4621	33.4584

image is given as:

$$H = -\sum_{i=1}^{256} p(i) log_2 p(i) \tag{16}$$

where $p(i)$ stands for the probability of the pixel value i. The experimental results of our proposed cryptosystem are shown in Table 7. The information entropy of the encrypted images by our proposed cryptosystem is close to the theoretical value of 8, which has a certain improvement compared with the similar references.

6) SECURITY ANALYSIS BASED ON CRYPTOGRAPHIC ATTACKS

For the cryptanalysis of the image cryptosystems, chosen-plaintext attacks and chosen-ciphertext attacks are the most powerful attack methods [4], [21], [22], [26]. The main idea is to select some special attack images, such as all black and all white, and then use algebra analysis to achieve the equivalent key of the original cryptosystem. For example, in [4], [7], we use the digital image group as shown in Figs. 10(a)-(c) and Figs. 10(e)-(g) to crack the target algorithms. Using similar attack methods, we conduct security checks on our proposed

TABLE 7. The results of information entropy test and comparison results.

Images	Plain-image			Cipher-image		
	R	G	B	R	G	B
4.1.01.tiff	6.8981	6.4457	6.3807	7.9974	7.9971	7.9978
4.1.06.tiff	7.5371	7.4136	6.9207	7.9971	7.9970	7.9971
4.2.01.tiff	7.7624	7.4744	7.7522	7.9993	7.9994	7.9994
4.2.05.tiff	6.6639	6.7990	6.2138	7.9993	7.9993	7.9993
Fig. 4(e)	7.0776	7.1500	6.7164	7.7304	7.7532	7.7184
4.1.01.tiff by Ref. [18]	6.8981	6.4457	6.3807	7.9972	7.9975	7.9971
4.1.01.tiff by Ref. [44]	6.8981	6.4457	6.3807	7.9968	7.9966	7.9969
4.1.01.tiff by Ref. [39]	6.8981	6.4457	6.3807	7.9970	7.9975	7.9970
4.1.01.tiff by Ref. [16]	6.8981	6.4457	6.3807	7.9973	7.9972	7.9972
4.1.01.tiff by Ref. [45]	6.8981	6.4457	6.3807	7.9972	7.9976	7.9974
4.1.01.tiff by Ref. [38]	6.8981	6.4457	6.3807	7.9975	7.9974	7.9975

image cryptosystem. Taking chosen-plaintext attack as an example, we select Figs. 10(a)-(c) as plaintext attack images respectively, and the corresponding intermediate and final cipher images are shown in Figs. 10(i)-(k). It can be seen from Fig. 10(l), their histogram characteristics are all in a noise-like state, which is significantly different from Fig. 10(d) and Fig. 10(h). So it is difficult for an attacker to conduct penetration attacks in this way. Similarly, the chosen-ciphertext attack is also difficult to work. The most essential reason is adopting the diffusion-permutation-diffusion structure and a plaintext-related mechanism, which can effectively improve the security performance.

7) COMPREHENSIVE DISCUSSION

In our proposed image cryptosystem, the key space of our cryptosystem involves three initial values of the quantum chaos and the *hash*256 of plain images, which can be expressed as $key(\cdot) = (hash256, x_0, y_0, z_0)$. Assuming that the precision of the three initial values x_0,y_0,z_0 is 10^{15}, the total key space is $10^{15\times3}+2^{256}$. In terms of the secret-key space, it is sufficient to withstand brute force attacks under the existing computing environment. Judging from the statistical information such as histogram, *PSNR*, *SSIM* and information entropy of the encrypted image, it can effectively resist ciphertext-only attacks and statistical analysis attacks. From the perspective of differential analysis, the encryption system proposed in this paper is both sensitive to secret keys and plaintexts, so it can resist plaintext attacks. In addition,

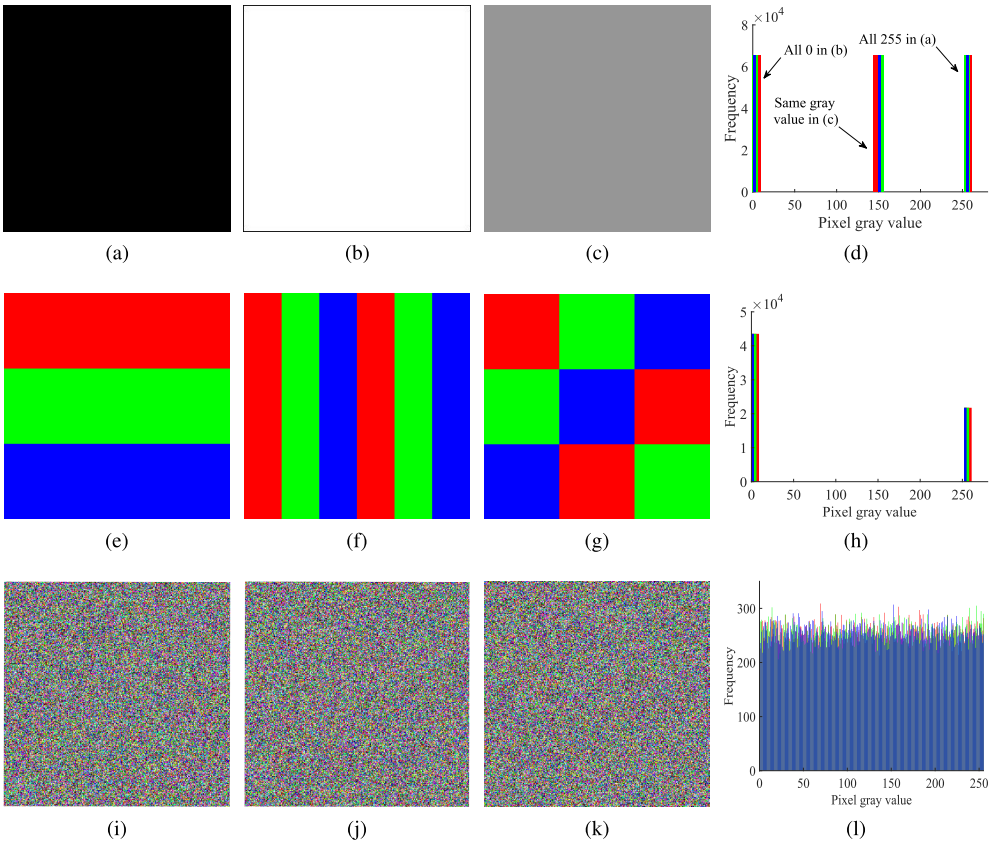


FIGURE 10. Special chosen plain images and their attacking results: a) All black; b) All white; c) All gray; d) Histogram of a)-c); e) $1^{\#}$ attack image; f) $2^{\#}$ attack image; g) $3^{\#}$ attack image; h) Histogram of e)-g); i) The corresponding C_1; j) The corresponding C_3; k) The corresponding C; l) Histogram of i)-k).

the algorithm uses a plaintext association mechanism and a diffusion-permutation-diffusion structure, so it can resist chosen plaintext and ciphertext attacks.

Regarding key management, we introduce a plaintext association mechanism to dynamically update the PRNSs to enhance security. This idea is based on our latest cryptanalysis research [4]. In fact, many insecure algorithms have common features that independent of plain images [7], [21], [26]. However, security and convenience are a pair of contradictions. Frankly speaking, this mechanism will increase key management overhead. Considering high security, it is undeniable that this is also a meaningful technical route. Moreover, throughout international research, this mechanism is accepted and recognized by peer experts [27], [33], [34]. In certain scenarios with higher security levels, such as military security and confidential communications, this is a feasible and preferred technical solution. Of course, the key management work will be more complicated. It is necessary to store and distribute a dynamic password in advance.

V. CONCLUSION

To improve the security of digital image encryption algorithms and provide high-quality technical solutions for secure communications in the Internet of Things, we have proposed a quantum chaotic image cryptosystem. The proposed image cryptosystem uses a diffusion-permutation-diffusion structure and introduces a plaintext association mechanism to enhance the security. Theoretical security analysis and experimental results both demonstrate the excellent performance of our proposed cryptosystem. It is both sensitive to plain images and secret keys, and has robust ability to resist differential attacks as well as other various common attacks. Moreover, we conducted experiments on the IoT secure communication platform, and the results verified the feasibility and effectiveness of the proposed scheme. The main contribution of this paper is to provide a security-enhanced image cryptosystem with low computational complexity. Further we systematically present its performance analysis and successfully realize the hardware implementation in IoT experimental platform. On the other hand, this paper still lacks consideration in terms of key management, and will continue to be improved in future research.

REFERENCES

[1] H. Wen, S. Yu, and J. Lü, "Encryption algorithm based on Hadoop and non-degenerate high-dimensional discrete hyperchaotic system," *Acta Phys. Sinica*, vol. 66, no. 23, 2017, Art. no. 230503.

[2] T. Wu, C. Zhang, C. Chen, H. Hou, H. Wei, S. Hu, and K. Qiu, "Security enhancement for OFDM-PON using Brownian motion and chaos in cell," *Opt. Exp.*, vol. 26, no. 18, pp. 22857–22865, Sep. 2018.

[3] T. Wu, C. Zhang, H. Wei, and K. Qiu, "Papr and security in OFDM-PON via optimum block dividing with dynamic key and 2D-LASM," *Opt. Exp.*, vol. 27, no. 20, pp. 27946–27961, 2019.
[4] H. Wen, S. Yu, and J. Lü, "Breaking an image encryption algorithm based on DNA encoding and spatiotemporal chaos," *Entropy*, vol. 21, no. 3, p. 246, Mar. 2019.
[5] T. Wu, C. Zhang, H. Huang, Z. Zhang, H. Wei, H. Wen, and K. Qiu, "Security improvement for OFDM-PON via dna extension code and chaotic systems," *IEEE Access*, vol. 8, pp. 124452–124460, 2020.
[6] C. Zhang, Y. Yan, T. Wu, X. Zhang, G. Wen, and K. Qiu, "Phase masking and time-frequency chaotic encryption for DFMA-PON," *IEEE Photon. J.*, vol. 10, no. 4, Jul. 2018, Art. no. 7203009.
[7] H. Wen and S. Yu, "Cryptanalysis of an image encryption cryptosystem based on binary bit planes extraction and multiple chaotic maps," *Eur. Phys. J. Plus*, vol. 134, no. 7, p. 337, Jul. 2019.
[8] J. Fridrich, "Symmetric ciphers based on two-dimensional chaotic maps," *Int. J. Bifurcation Chaos*, vol. 8, no. 6, pp. 1259–1284, Jun. 1998, doi: 10.1142/S021812749800098X.
[9] D. D. Wheeler, "Problems with chaotic cryptosystems," *Cryptologia*, vol. 13, no. 3, pp. 243–250, Jul. 1989, doi: 10.1080/0161-118991863934.
[10] E. N. Lorenz, "Deterministic nonperiodic flow," *J. Atmos. Sci.*, vol. 20, no. 2, pp. 130–141, Mar. 1963.
[11] T.-Y. Li and J. A. Yorke, "Period three implies chaos," *Amer. Math. Monthly*, vol. 82, no. 10, pp. 985–992, Dec. 1975, doi: 10.1080/00029890.1975.11994008.
[12] C. Zhang, W. Zhang, C. Chen, X. He, and K. Qiu, "Physical-enhanced secure strategy for OFDMA-PON using chaos and deoxyribonucleic acid encoding," *J. Lightw. Technol.*, vol. 36, no. 9, pp. 1706–1712, May 1, 2018.
[13] H. Wei, C. Zhang, T. Wu, H. Huang, and K. Qiu, "Chaotic multilevel separated encryption for security enhancement of OFDM-PON," *IEEE Access*, vol. 7, pp. 124452–124460, 2019.
[14] W. Cao, Y. Mao, and Y. Zhou, "Designing a 2D infinite collapse map for image encryption," *Signal Process.*, vol. 171, Jun. 2020, Art. no. 107457.
[15] Z. M. Z. Muhammad and F. Ozkaynak, "Security problems of chaotic image encryption algorithms based on cryptanalysis driven design technique," *IEEE Access*, vol. 7, pp. 99945–99953, 2019.
[16] C. Pak, K. An, P. Jang, J. Kim, and S. Kim, "A novel bit-level color image encryption using improved 1D chaotic map," *Multimedia Tools Appl.*, vol. 78, no. 9, pp. 12027–12042, May 2019.
[17] Y. Zhou, L. Bao, and C. L. P. Chen, "A new 1D chaotic system for image encryption," *Signal Process.*, vol. 97, pp. 172–182, Apr. 2014.
[18] A. Shafique and J. Shahid, "Novel image encryption cryptosystem based on binary bit planes extraction and multiple chaotic maps," *Eur. Phys. J. Plus*, vol. 133, no. 8, p. 331, Aug. 2018.
[19] C. Song and Y. Qiao, "A novel image encryption algorithm based on DNA encoding and spatiotemporal chaos," *Entropy*, vol. 17, no. 12, pp. 6954–6968, Oct. 2015.
[20] H. Diab and A. M. El-semary, "Cryptanalysis and improvement of the image cryptosystem reusing permutation matrix dynamically," *Signal Process.*, vol. 148, pp. 172–192, Jul. 2018.
[21] C. Li, D. Lin, J. Lu, and F. Hao, "Cryptanalyzing an image encryption algorithm based on autoblocking and electrocardiography," *IEEE MultiMediaMag.*, vol. 25, no. 4, pp. 46–56, Oct. 2018.
[22] C. Li, D. Lin, and J. Lu, "Cryptanalyzing an image-scrambling encryption algorithm of pixel bits," *IEEE MultimediaMag.*, vol. 24, no. 3, pp. 64–71, Aug. 2017.
[23] Z. Hua, Y. Zhang, and Y. Zhou, "Two-dimensional modular chaotification system for improving chaos complexity," *IEEE Trans. Signal Process.*, vol. 68, pp. 1937–1949, 2020.
[24] Z. Hua, Y. Zhou, and H. Huang, "Cosine-transform-based chaotic system for image encryption," *Inf. Sci.*, vol. 480, pp. 403–419, Apr. 2019.
[25] C. Li, B. Feng, S. Li, J. Kurths, and G. Chen, "Dynamic analysis of digital chaotic maps via state-mapping networks," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 66, no. 6, pp. 2322–2335, Jun. 2019.
[26] M. Li, D. Lu, W. Wen, H. Ren, and Y. Zhang, "Cryptanalyzing a color image encryption scheme based on hybrid hyper-chaotic system and cellular automata," *IEEE Access*, vol. 6, pp. 47102–47111, 2018.
[27] X. Chai, Z. Gan, K. Yuan, Y. Chen, and X. Liu, "A novel image encryption scheme based on DNA sequence operations and chaotic systems," *Neural Comput. Appl.*, vol. 31, no. 1, pp. 219–237, Jan. 2019.
[28] Q. Yin and C. Wang, "A new chaotic image encryption scheme using breadth-first search and dynamic diffusion," *Int. J. Bifurcation Chaos*, vol. 28, no. 4, Apr. 2018, Art. no. 1850047.
[29] H. Liu, A. Kadir, and C. Xu, "Cryptanalysis and constructing S-box based on chaotic map and backtracking," *Appl. Math. Comput.*, vol. 376, Jul. 2020, Art. no. 125153. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0096300320301223
[30] H. Liu, Y. Xu, and C. Ma, "Chaos-based image hybrid encryption algorithm using key stretching and hash feedback," *Optik*, vol. 216, Aug. 2020, Art. no. 164925. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0030402620307610
[31] Q. Xu, K. Sun, C. Cao, and C. Zhu, "A fast image encryption algorithm based on compressive sensing and hyperchaotic map," *Opt. Lasers Eng.*, vol. 121, pp. 203–214, Oct. 2019. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0143816618315707
[32] C. Chen, K. Sun, and S. He, "An improved image encryption algorithm with finite computing precision," *Signal Process.*, vol. 168, Mar. 2020, Art. no. 107340. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0165168419303937
[33] Q. Xu, K. Sun, S. He, and C. Zhu, "An effective image encryption algorithm based on compressive sensing and 2D-SLIM," *Opt. Lasers Eng.*, vol. 134, Nov. 2020, Art. no. 106178. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0143816620301676
[34] X. Wang and N. Guan, "Chaotic image encryption algorithm based on block theory and reversible mixed cellular automata," *Opt. Laser Technol.*, vol. 132, Dec. 2020, Art. no. 106501. [Online]. Available: http://www.sciencedirect.com/science/article/pii/
[35] Y. Ma, C. Li, and B. Ou, "Cryptanalysis of an image block encryption algorithm based on chaotic maps," *J. Inf. Secur. Appl.*, vol. 54, Oct. 2020, Art. no. 102566. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S2214212620301629
[36] A. Akhshani, A. Akhavan, S.-C. Lim, and Z. Hassan, "An image encryption scheme based on quantum logistic map," *Commun. Nonlinear Sci. Numer. Simul.*, vol. 17, no. 12, pp. 4653–4661, Dec. 2012.
[37] M. E. Goggin, B. Sundaram, and P. W. Milonni, "Quantum logistic map," *Phys. Rev. A, Gen. Phys.*, vol. 41, no. 10, p. 5705, 1990.
[38] X. Huang, T. Sun, Y. Li, and J. Liang, "A color image encryption algorithm based on a fractional-order hyperchaotic system," *Entropy*, vol. 17, no. 1, pp. 28–38, Dec. 2014.
[39] L. Xu, Z. Li, J. Li, and W. Hua, "A novel bit-level image encryption algorithm based on chaotic maps," *Opt. Lasers Eng.*, vol. 78, pp. 17–25, Mar. 2016.
[40] A. Shafique and J. Shahid, "Novel image encryption cryptosystem based on binary bit planes extraction and multiple chaotic maps," *Eur. Phys. J. Plus*, vol. 133, no. 8, p. 331, Aug. 2018.
[41] X. Chai, J. Bi, Z. Gan, X. Liu, Y. Zhang, and Y. Chen, "Color image compression and encryption scheme based on compressive sensing and double random encryption strategy," *Signal Process.*, vol. 176, Nov. 2020, Art. no. 107684.
[42] X. Chai, H. Wu, Z. Gan, D. Han, Y. Zhang, and Y. Chen, "An efficient approach for encrypting double color images into a visually meaningful cipher image using 2D compressive sensing," *Inf. Sci.*, to be published, doi: 10.1016/j.ins.2020.10.007.
[43] X. Chai, H. Wu, Z. Gan, Y. Zhang, and Y. Chen, "Hiding cipher-images generated by 2-D compressive sensing with a multi-embedding strategy," *Signal Process.*, vol. 171, Jun. 2020, Art. no. 107525.
[44] Q. Yin and C. Wang, "A new chaotic image encryption scheme using breadth-first search and dynamic diffusion," *Int. J. Bifurcation Chaos*, vol. 28, no. 04, Apr. 2018, Art. no. 1850047.
[45] M. Essaid, I. Akharraz, A. Saaidi, and E. A. Mouhib, "Image encryption scheme based on a new secure variant of hill cipher and 1D chaotic maps," *J. Inf. Secur. Appl.*, vol. 47, pp. 173–187, Aug. 2019.

HEPING WEN received the Ph.D. degree from the Guangdong University of Technology, Guangzhou, China, in 2019. He is currently a Senior Engineer with the School of Electronic and Information Engineering, Zhongshan Institute, University of Electronic Science and Technology of China. He is also a Postdoctoral Researcher with the University of Electronic Science and Technology of China. His research interests include chaos-based secure communication and image encryption.

CHONGFU ZHANG (Senior Member, IEEE) received the Ph.D. degree from the University of Electronic Science and Technology of China, Chengdu, China, in 2009. From 2013 to 2014, he was a Visiting Scholar with the OCLAB, University of Southern California. He is currently a Full Professor with UESTC. He has authored/coauthored over 100 articles and holds 40 patents. His research interests include broadband access networks, microwave photonics, communication security, and optical signal processing. He is also a member of the OSA. Along with his colleagues, he has received six awards of science and technology.

PING CHEN received the M.S. and Ph.D. degrees from the Guangdong University of Technology, Guangzhou, China, in 2010 and 2019, respectively. He is currently a Lecturer with the Guangdong University of Technology. His research interests include chaos-based secure communication and video encrypiton.

RUITING CHEN is currently pursuing the bachelor's degree with the School of Electronic and Information, Zhongshan Institute, University of Electronic Science and Technology of China, Zhongshan, China. His current research interests include image encryption and information security.

JIAJUN XU is currently pursuing the bachelor's degree with the School of Electronic and Information, Zhongshan Institute, University of Electronic Science and Technology of China, Zhongshan, China. His current research interests include image encryption and information security.

YUNLONG LIAO is currently pursuing the bachelor's degree with the School of Electronic and Information, Zhongshan Institute, University of Electronic Science and Technology of China, Zhongshan, China. His current research interests include image encryption and information security.

ZHONGHAO LIANG is currently pursuing the bachelor's degree with the School of Electronic and Information, Zhongshan Institute, University of Electronic Science and Technology of China, Zhongshan, China. His current research interests include image encryption and information security.

DANZE SHEN is currently pursuing the bachelor's degree with the School of Electronic and Information, Zhongshan Institute, University of Electronic Science and Technology of China, Zhongshan, China. His current research interests include image encryption and information security.

LIMENGNAN ZHOU received the B.S. and Ph.D. degrees in information and communication engineering from Southwest Jiaotong University, Chengdu, China, in 2012 and 2017, respectively. Since 2017, she has been with the School of Electronic and Information Engineering, University of Electronic Science and Technology of China, Zhongshan Institute, Zhongshan, China, where she is currently a Teacher. Her research interest includes sequence design and its applications.

JUXIN KE received the M.S. degree from the Guangdong University of Technology, Guangzhou, China, in 2009, respectively. He is currently an Engineer with the Dongguan Polytechnic College. His research interests include security of network and big data, and next generation communication.