https://doi.org/10.1007/s11467-023-1293-3

RESEARCH ARTICLE

A probabilistic model of quantum states for classical data security

Muhammad Waseem Hafiz[1], Seong Oun Hwang[2,†]

[1] *Department of IT Convergence Engineering, Gachon University, Seongnam 13120, South Korea*
[2] *Department of Computer Engineering, Gachon University, Seongnam 13120, South Korea*
Corresponding author. E-mail:[†]*sohwang@gachon.ac.kr*

Received December 12, 2022; accepted April 6, 2023

1 Experimental results

The superposition of states for a qubit system on the Bloch sphere for diverse phase domains using IBM quantum composer, and fetch unique states for a classical system as shown in Figs. 1 and 2. Quantum mainframes can efficiently simulate these complex states to authenticate users and simulate data over classical, as well as quantum, computers.

1.1 Evaluation of quantum states

The demonstrated states in Figs. 1 and 2 were generated on 15 points [85.1176 90.2067 95.2958 100.3849 105.4740 110.5631 115.6522 120.7413 125.8304 130.9195 136.0086 141.0977 146.1868 151.2759 156.3650] and 25 points [-60 -54.9909 -49.9818 -44.9727 -39.9636 -34.9545 -29.9454 -24.9363 -19.9272 -14.9181 -9.9090 -4.8999 0.1092 5.1183 10.1274 15.1365 20.1456 25.1547 30.1638 35.1729 40.1820 45.1911 50.2002 55.2093 60.2184]. For a 15-point system, each point value indicates 60 distinct states to represent data. Similarly, for the 25-point system in Fig. 2, each point value indicates 100 distinct states to represent data.

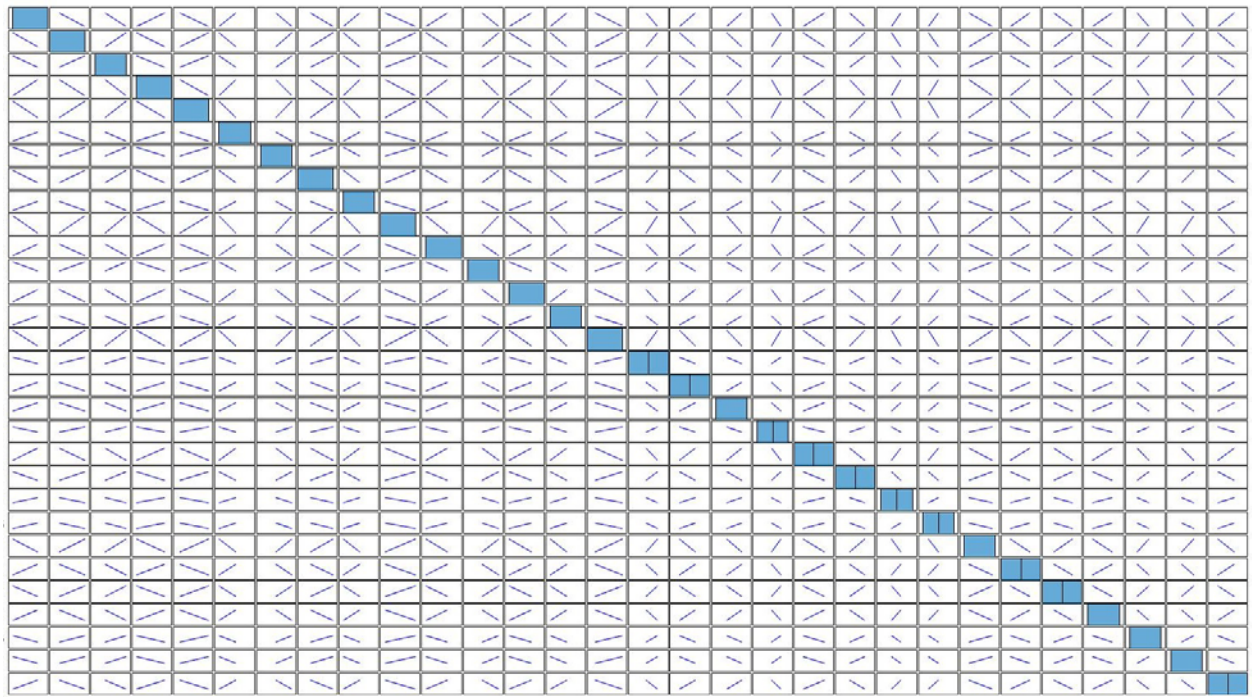


Fig. 1 Demonstration of a 15-point spin state system (domain of 85.1176 to 159.8238 with a step size of 5.0891) for a solo qubit.

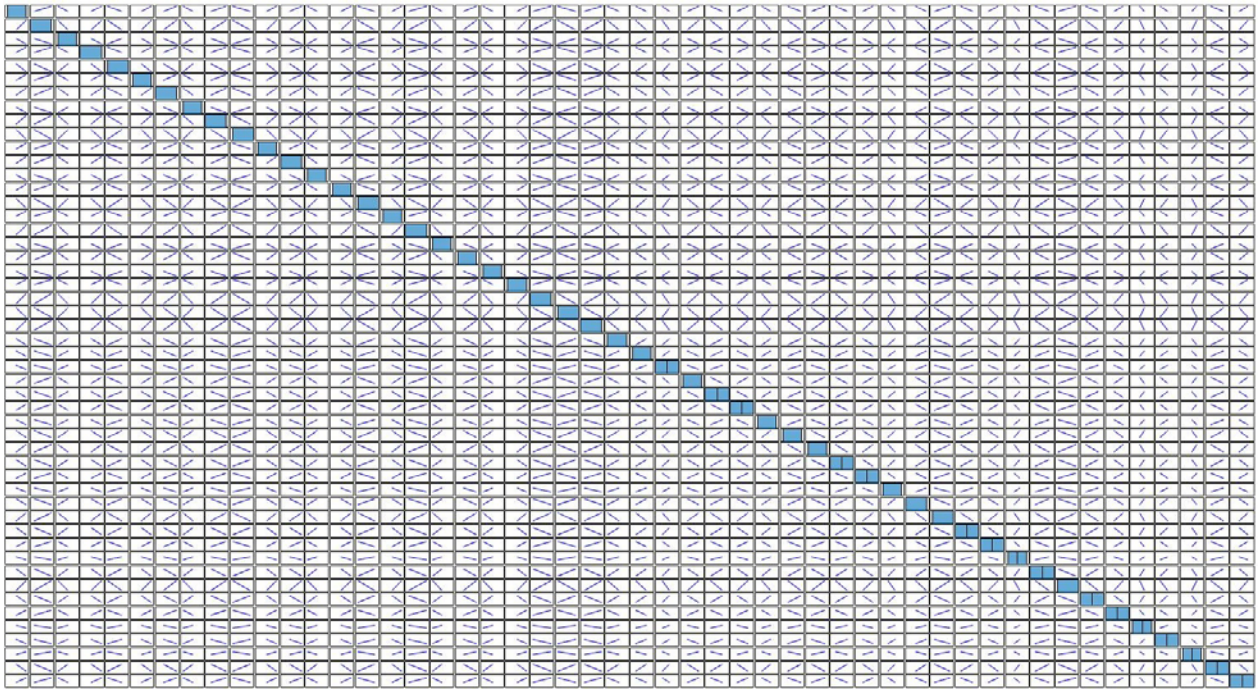


Fig. 2 Demonstration of a 25-point spin state system (domain of -60 to 60.8238 with a step size of 5.0091) for a solo qubit.

Each state has distinct symmetrical characteristics, and the information one can obtain via this method can be conceived as a hash function of q-states on classical systems. For a distinct copy of a state, one can assume that many copies are available and solve for all pure and mixed states of a single qubit [1-3]. To predict the basis of the states to retrieve the transmitted data, an observer in the channel needs to compute 1440^{60} combinations with a step size of 1 and

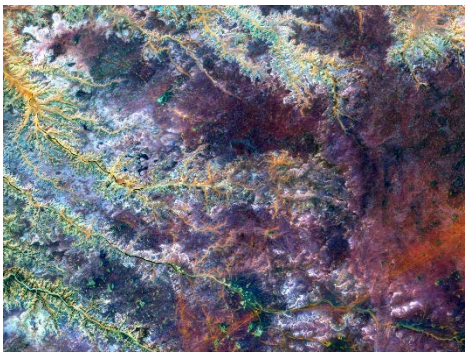
14400^{60} combinations with a step size of 0.1 to predict measurement for the correct basis. It is not realistic for an observer to measure the correct basis by evaluating the states for the domain $[-720 : x : 720]^n$ even with quantum resources for a smaller x and larger n.

1.2 Pixel correlation analysis

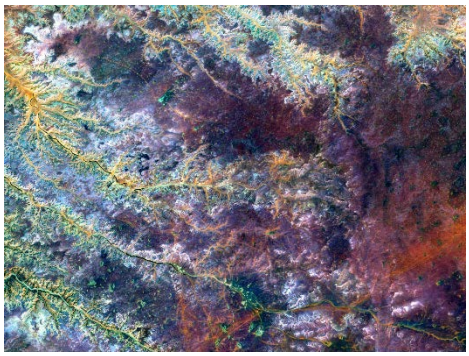
Correlation analysis signifies the strength of association between dependent variables [4-5]. We chose 10 000 combinations of neighboring pixel pairs from the original and recovered data to investigate their relationships. We utilized the following equation to analyze pairings in horizontal, vertical, and diagonal directions:

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

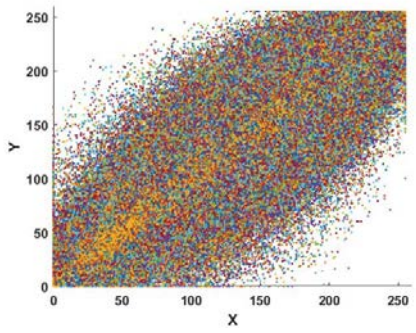
where x and y are the adjacent grayscale pixel values, σ_x^2 and σ_y^2 are the variances, and $\sigma_{x,y}$ is the covariance of random variables x and y.



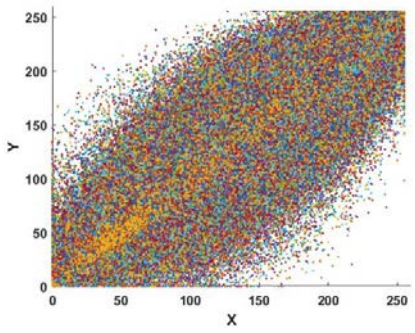
(a)



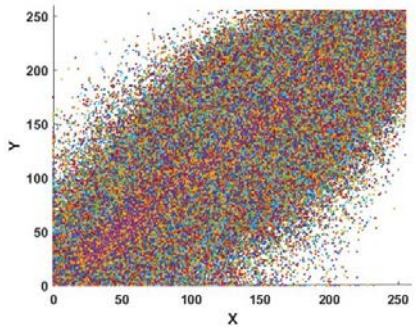
(e)



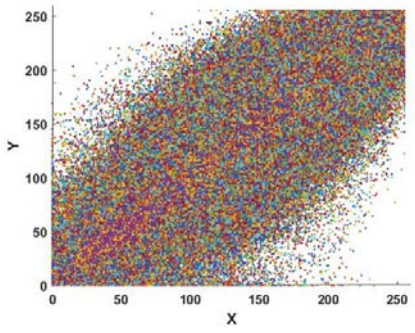
(b)



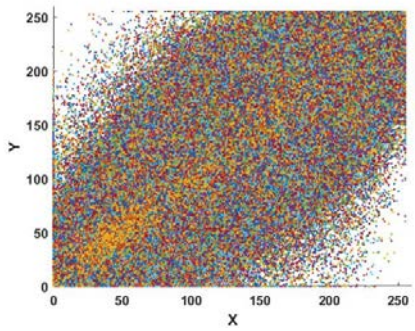
(f)



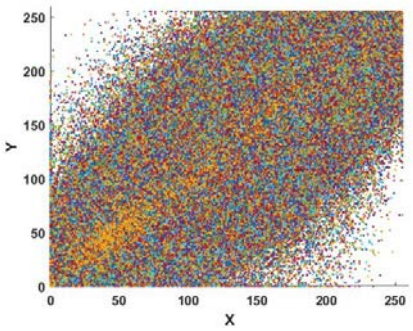
(c)



(g)

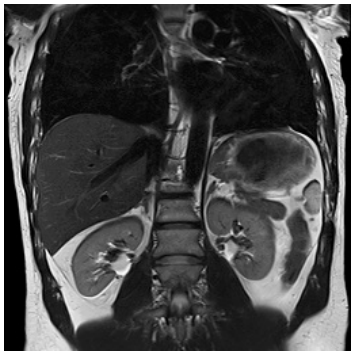


(d)

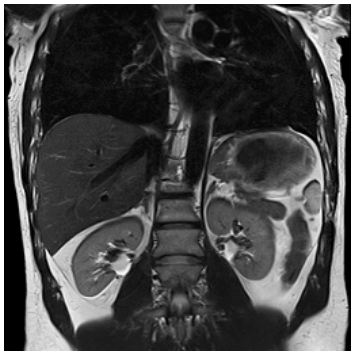


(h)

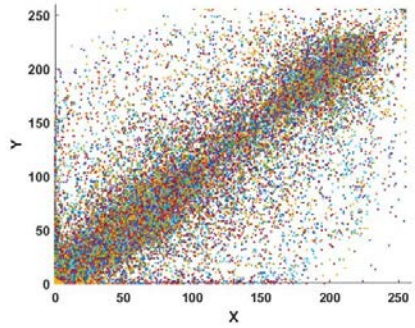
Fig. 3 Pixel correlation analysis of original and recovered multispectral images: (a-d) the original image and correlation analysis in the horizontal, vertical, and diagonal directions, and (e-h) the recovered image and its correlation analysis in the horizontal, vertical, and diagonal directions.



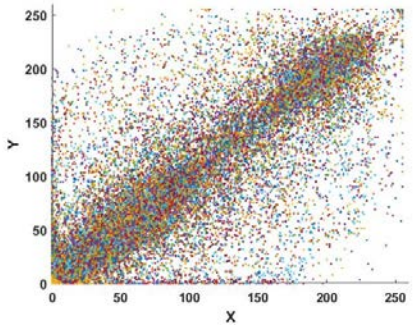
(a)



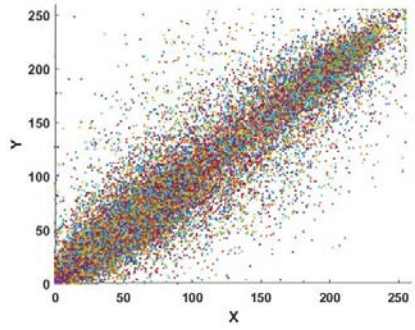
(e)



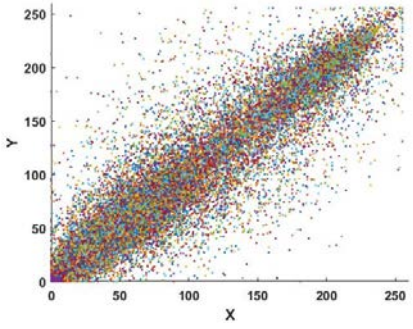
(b)



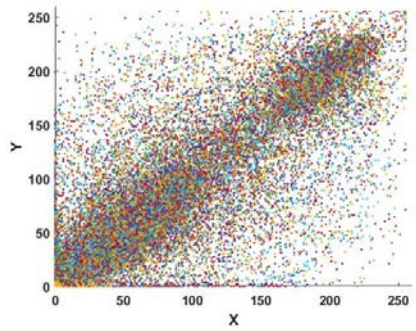
(f)



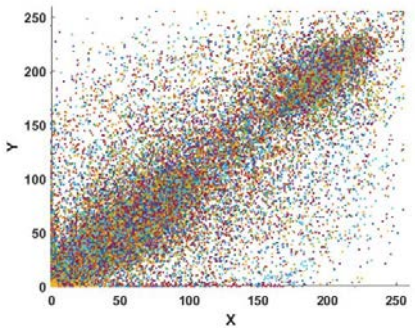
(c)



(g)



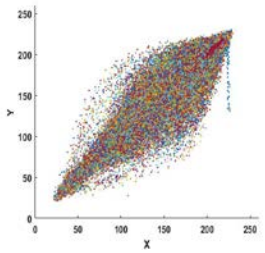
(d)



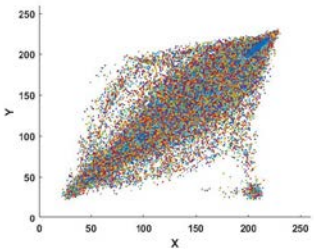
(h)

Fig. 4 Pixel correlation analysis for original and recovered abdominal MRI images: (a-d) the original image and correlation analysis in the horizontal, vertical, and diagonal directions, and (e-h) the recovered image and correlation analysis in the horizontal, vertical, and diagonal directions.

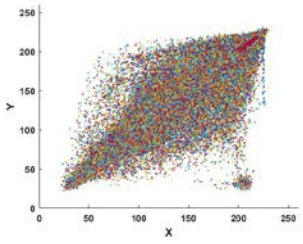
(a)



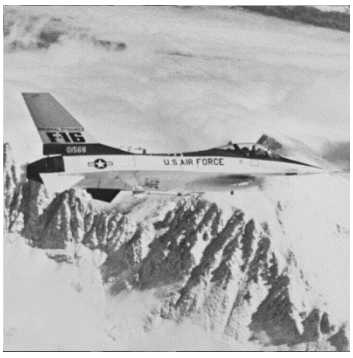
(b)



(c)



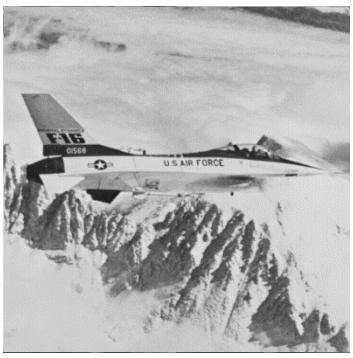
(d)



(e)

(f)

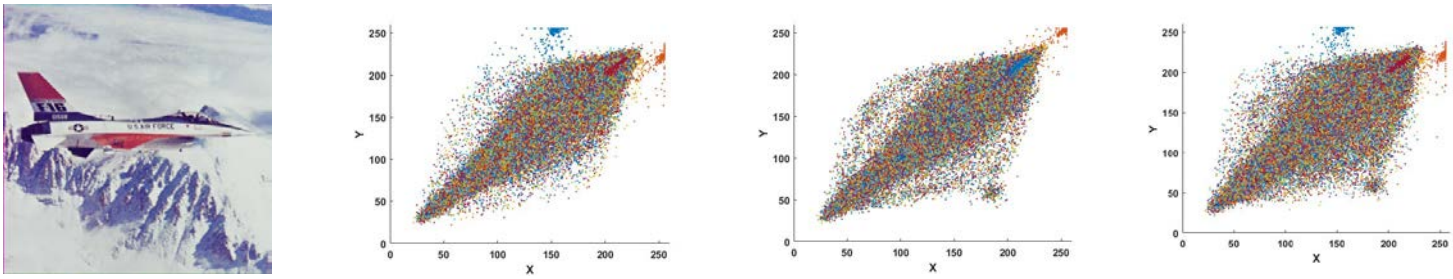
(g)



(h)

(i)

(j)



(k) (l) (m) (n)

Fig. 5 Pixel correlation analysis of the original and recovered RGB image titled Airplane: (a-d) the original image and correlation analysis in the horizontal, vertical, and diagonal directions, (e-g) layer-wise transmitted RGB contents, (h-j) the recovered RGB contents, and (k-n) the concatenated image from the recovered RGB contents and correlation analysis in the horizontal, vertical, and diagonal directions.

The data in Figs. 3-5 recovered from the states seem quite similar to the original transmitted contents. We computed two-dimensional correlation coefficients using the following expression to estimate the dissimilarity between the original and recovered contents by evaluating the correlation error [6]:

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

where P and R signify the plain and recovered contents, respectively, with mean approximations of $\overline{P}$ and $\overline{R}$, while M and N represent the content height and width. The assessment of correlation coefficients for the original and the recovered data, as well as the dissimilarity between the contents, is shown in Table 1.

Table 1 Pixel correlation coefficient analysis for the original and the recovered images.

Image	Direction	Original image	Recovered image	Correlation error
Multispectral	Horizontal	0.9279	0.9268	0.0011
	Vertical	0.9197	0.9180	0.0017
	Diagonal	0.8733	0.8697	0.0036
Abdominal MRI	Horizontal	0.8980	0.8980	0
	Vertical	0.9604	0.9603	0.0001
	Diagonal	0.8805	0.8805	0
Airplane	Horizontal	0.9726	0.9652	0.0074
	Vertical	0.9610	0.9568	0.0042
	Diagonal	0.9343	0.9325	0.0018

The correlation coefficients for the original and recovered images listed in Table 1 are highly comparable, and the discrepancy between the transmitted and received contents is negligible, demonstrating the feasibility and effectiveness of the recovery procedure. Analyses to compare the divergence and luminance (SSIM), the quality of the image concerning noise and sharpness (SC), and the divergence of recovered contents from the original (NAE) [7] were carried out and are presented in Table 2 using the following expressions:

$$SSIM = \frac{(2\mu_p \mu_r + R_1)(2\sigma_{pr} + R_2)}{(\mu_p^2 + \mu_r^2 + R_1)(\sigma_p^2 + \sigma_r^2 + R_2)},$$

$$SC = \sum_{k=0}^{M-1}\sum_{l=0}^{N-1} \frac{P^2_{k,l}}{\sum_{k=0}^{M-1}\sum_{l=0}^{N-1} R^2_{k,l}},$$

$$NAE = \sum_{i=0}^{M-1}\sum_{j=0}^{N-1} \frac{\left|P_{i,j} - R_{i,j}\right|}{\sum_{i=0}^{M-1}\sum_{j=0}^{N-1}\left|P_{i,j}\right|},$$

where $P_{k,l}$ and $R_{k,l}$ represent the original and recovered contents in the k^{th} row and l^{th} column, μ_p and μ_r represent mean values, and σ_{pr} is the standard deviation. A higher estimation of SSIM (i.e. 1) infers a strong resemblance between the original and recovered images.

Table 2 Similarity analyses between the original and recovered images.

Image	NAE	SSIM	SC
Multispectral	0.0008	0.990190	0.9999
Abdominal MRI	0.0011	0.999525	0.9999
Airplane	0.0064	0.945067	0.9999

The NAE between the original and the recovered images is almost negligible, whereas the luminance, divergence, and assembly of the recovered contents had more than 99% similarity in the multispectral and abdominal MRI images, and more than 94% similarity in the RGB contents of the image titled Airplane. The structural details of recovered images were more than 99% similar to the original contents in terms of sharpness and noise. These analyses validate the efficacy of the proposed methodology with trivial loss in the recovery of data from the q-states.

We performed the experiments in an ideal scenario, with no channel loss or disturbance in states, to transform classical data into q-states for transmission and recovery from free states. In comparison, we observed a minute loss in the recovered data.

2 Conclusion

In this paper, we demonstrated the arbitrated quantum signature and unclonable spin states, in both theory and experimentation, for secure transmission and reception of classical data. The experiment is comprehended without assumptions of computational hardness and entanglement exertion, and the findings verified that quantum physics countenances improved security tradeoffs for certain computing tasks in classical communications. We observed that the outcomes produced by the proposed methodology are in good accord with the readily available technology, and we believe that the provided work insinuates the rich domain of quantum practices to enhance the security of classical computations. Future advancements would allow for quantum state verification and non-separable measurement on the client side, which might be the intention of, and an improvement to, the anticipated model.

References

1. Wu KD, Theurer T, Xiang GY, Li CF, Guo GC, Plenio MB, Streltsov A. Quantum coherence and state conversion: theory and experiment. npj Quantum Information. 2020, 6(1): 1
2. Shi HL, Wang XH, Liu SY, Yang WL, Yang ZY, Fan H. Coherence transformations in single qubit systems. Scientific reports. 2017, 7(1): 1
3. Wei Y, Wang S, Zhu Y, Li T. Sender-controlled measurement-device-independent multiparty quantum communication. Frontiers of Physics. 2022, 17(2): 1-9
4. Li J, Chen L, Cai W, Xiao J, Zhu J, Hu Y, Wen K. Holographic encryption algorithm based on bit-plane decomposition and hyperchaotic Lorenz system. Optics & Laser Technology. 2022,152: 108127
5. Khan M, Waseem HM. A novel image encryption scheme based on quantum dynamical spinning and rotations. PloS one. 2018, 13(11): e0206460
6. Huang ZW, Zhou NR. Image encryption scheme based on discrete cosine Stockwell transform and DNA-level modulus diffusion. Optics & Laser Technology. 2022, 149: 107879
7. Batool SI, Waseem HM. A novel image encryption scheme based on Arnold scrambling and Lucas series. Multimedia tools and applications. 2019, 78(19): 27611