Optica Applicata, Vol. LV, No. 4, 2025
DOI: 10.37190/oa/211317

A quantum image encryption-authentication method using quantum Haar wavelet transform and affine transform

PING-PING ZENG[1], JIA-WEN WU[2], MING-XUAN CHEN[3], MENG-MENG WANG[4,*]

[1] School of Information Engineering, Gandong University, Fuzhou 344000, Jiangxi, China

[2] Department of Electronic Information Engineering, Nanchang University, Nanchang 330031, China

[3] School of Electronic and Electrical Engineering, Shanghai University of Engineering Science, Shanghai 201620, China

[4] School of Information and Control Engineering, Qingdao University of Technology, Qingdao 266033, China

[*]Corresponding author: wangmengmeng@qut.edu.cn

The quantum image encryption and authentication algorithm are proposed based on quantum affine transformation and quantum Haar wavelet transform. This algorithm is divided into two main steps: encryption and embedding. During the encryption phase, affine transform and Hénon map are combined to carry out scrambling-diffusion processing on the plaintext image. In the phase of embedding, the color carrier image undergoes decomposition using the quantum Haar wavelet transform. Then the ciphertext image information and identity information are hidden into the wavelet domain of the color carrier image, and the final transmitted image has visual significance. The suggested algorithm significantly minimizes the risk of image data compromise during transmission and realizes the dual security of encryption and authentication. The security and the robustness of the algorithm are analyzed by using the evaluation indexes of image encryption and information hiding. The findings indicate that the introduced algorithm offers superior security compared to alternative methods, ensuring a more dependable and safeguarded transmission of image data.

Keywords: quantum image encryption preparation, quantum Haar wavelet transform, affine transform.

1. Introduction

Information security technology mainly includes two fields: data hiding and cryptography. Image encryption is the application of cryptographic technology in image information protection, which effectively protects image information by converting plaintext

images into meaningless ciphertext images [1-4]. Data hiding technology enables secret information to be embedded in electronic media like images, video, audio and text to protect copyright or conduct secret communications [5, 6]. Due to their sensitivity to initial conditions and parameters, as well as their ergodic behavior, chaotic systems possess inherent properties that make them highly suitable for strengthening image security [7-9].

Leveraging the distinctive properties of quantum state superposition and entanglement, quantum computers show strong parallel processing ability [10]. This enables quantum algorithms to significantly reduce the computational complexity when performing complex image operations, thus greatly improving the processing efficiency [11]. To enable the application of quantum technology, the color and positional information of images need to be encoded into qubits using a quantum representation model [12]. Since the emergence of the initial quantum image representation method known as the qubit lattice [13], numerous models have been developed. Models such as the flexible representation of quantum images (FRQI) [14], the novel enhanced quantum representation (NEQR) [15], and the general quantum image representation (GQIR) [16] are commonly used to represent grayscale images.

The process of quantum image encryption generally includes scrambling and diffusion steps. Matrix transformation-based methods are widely used in the scrambling process, aiming to disrupt the spatial correlation of pixel locations in the original image [17, 18]. ZHOU *et al*. raised a new algorithm that integrates image compression and encryption. The method leverages a quantum wavelet transform to achieve compression, followed by an XOR operation between the compressed image and a key image generated via a 3D hyperchaotic map to produce the final ciphertext [19]. MOU *et al*. devised an innovative hybrid color image encryption scheme that enhances key space size and ensures data integrity by integrating quantum random walk with the SHA-256 algorithm [20].

In the field of quantum information hiding, steganography is widely applied in sensitive domains like military and public security [21]. The continuous advancement in quantum image steganography has led to the emergence of numerous innovative algorithms [22-25]. WANG *et al*. designed a quantum color image steganography algorithm based on turtle shell and LSB modification, which significantly enhanced the concealment of the algorithm by introducing the human visual system (HVS) model [26]. The proposed quantum approach embeds information by integrating three frequency -domain techniques: DWT, DCT, and SVD [27]. Image watermarking can be divided into blind watermarking, semi-blind watermarking and non-blind watermarking according to different ways of extracting additional information [28]. In the frequency domain, the embedding process typically ensures the watermark's invisibility and robustness [29]. To enhance digital watermarking performance, ZHANG *et al*. proposed the algorithm based on frequency-domain attention guidance (FARW), resulting in improved visual fidelity and robustness [30].

Existing image encryption and watermarking methods often face trade-offs between security [31], visual quality, and robustness, motivating the development of a dual-pur-

pose algorithm that combines encryption and authentication efficiently. In certain scenarios, such as military communications or the transmission of trade secrets, it is essential not only to secure the image but also to trace its source and protect its copyright. In this paper, we explore the effective combination of quantum image encryption technology and quantum information hiding technology, to achieve multiple and all-round protection of image information.

2. Fundamental knowledge

2.1. Generalized quantum image representation model

In the generalized quantum image representation (GQIR) model [13], as shown in Fig. 1, the generalized quantum image is expressed as

$$|I\rangle = \frac{1}{\sqrt{2}^{H+W}} \sum_{Y=0}^{H-1} \sum_{X=0}^{W-1} \bigotimes_{i=0}^{q-1} |C_{YX}^{i}\rangle |YX\rangle \tag{1}$$

$$|YX\rangle = |Y\rangle|X\rangle = |y_0\, y_1 \ldots y_{h-1}\rangle\, |x_0\, x_1 \ldots x_{\omega-1}\rangle, \quad y_i, x_i \in \{0, 1\} \tag{2}$$

$$|C_{YX}\rangle = |C_{YX}^{0}\, C_{YX}^{1} \ldots C_{YX}^{q-1}\rangle, \quad C_{YX}^{i} \in \{0, 1\} \tag{3}$$

2.2. Quantum Haar wavelet transform

By using DWT, the plaintext image is split into four frequency sub-bands, each containing different types of information. The QHWT decomposition process of the image is illustrated in Fig. 2. Figure 3 presents its corresponding quantum circuit.

	00	01	10	11
0	0	128	255	
1	64	32	16	

$$|I\rangle = \frac{1}{\sqrt{2}^{3}}\big(|00000000\rangle \otimes |000\rangle + |10000000\rangle \otimes |001\rangle + |11111111\rangle \otimes |010\rangle + |01000000\rangle \otimes |100\rangle + |00100000\rangle \otimes |101\rangle + |00010000\rangle \otimes |110\rangle\big)$$

Fig. 1. GQIR representation of 2×3 image.

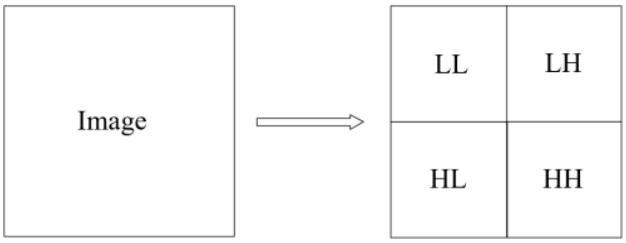

Fig. 2. QHWT decomposition process of the image.

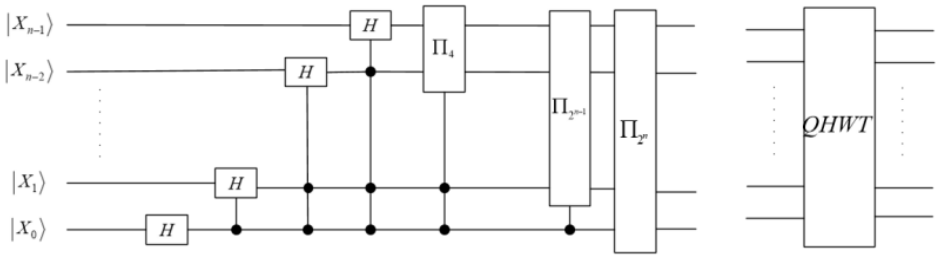

Fig. 3. Quantum circuit of QHWT.

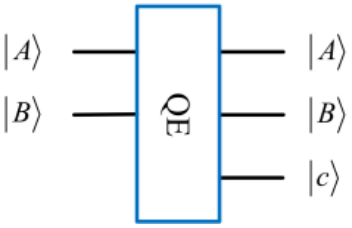

Fig. 4. Quantum equality module.

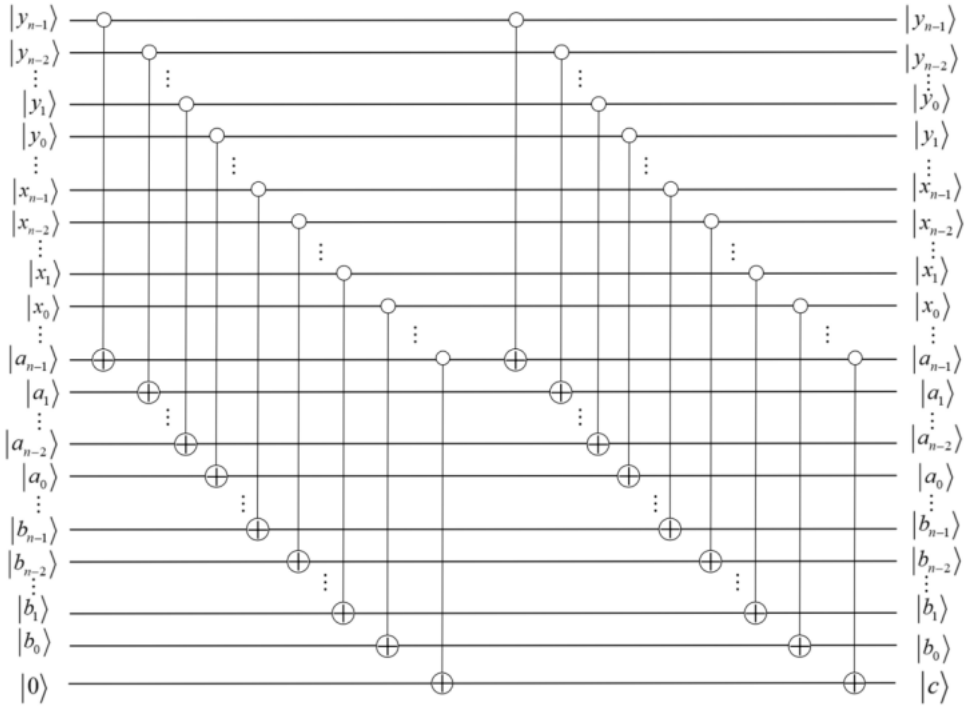

Fig. 5. Quantum circuit of QE.

2.3. Generalized affine transform

For a square image measuring $2^n \times 2^n$, the 2D affine transformation can be expressed as

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} 1 & a \\ b & ab+1 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} + \begin{pmatrix} c \\ d \end{pmatrix} (\mathrm{mod} 2^n) \tag{4}$$

where $ab + 1, c, d$ are positive integers less than 2^n. The affine transformation is Arnold transform with the parameters such that $c = d = 0$.

2.4. Quantum equality

With the quantum equal (QE) module, we can ascertain whether the two quantum sequences inputs $|A\rangle$ and $|B\rangle$ are identical or not. As shown in Fig. 4, the output qubit $|c\rangle$ denotes the result of the comparison, if $|c\rangle = |1\rangle$, then $|A\rangle = |B\rangle$; otherwise, $|A\rangle \neq |B\rangle$. The quantum circuit is depicted in Fig. 5.

3. Quantum image encryption and authentication algorithm

The process of encrypting and embedding within the algorithm is as follows.

Step 1. The grayscale image of size $M \times N$ is selected as the original image to be encrypted. The GQIR quantum expression form of the base image is

$$|I\rangle = \frac{1}{\sqrt{2}^{h+W}} \sum_{Y=0}^{M-1} \sum_{X=0}^{N-1} \bigotimes_{i=0}^{q-1} |C_{YX}^i\rangle |YX\rangle \tag{5}$$

suppose $M \leq N$, the pixel value set $|C_{YX}^i\rangle$ is a plaintext image, $|YX\rangle$ is the corresponding position information, $\omega = [\log_2 M]$ and $h = [\log_2 N]$.

Step 2. A_i is the generalized affine scrambling operator, after applying k times affine permutation on the base image $|I\rangle$, gaining the quantum image $|I_1\rangle$.

$$\begin{aligned} |I_1\rangle = A_i|I\rangle &= \frac{1}{2^{h+\omega}} \sum_{Y=0}^{2^h-1} \sum_{X=0}^{2^\omega-1} \bigotimes_{j=0}^{7} |C_{YX}^j\rangle A_i |YX\rangle \\ &= \frac{1}{2^{h+\omega}} \sum_{Y'=0}^{2^h-1} \sum_{X'=0}^{2^\omega-1} \bigotimes_{j=0}^{7} |C_{YX}^j\rangle A_i |Y'X'\rangle \end{aligned} \tag{6}$$

Step 3. I^* is a pseudo-random sequence generated by the Logistic map, and the items are sorted from lowest to highest to form the sequence D, and an index sequence D_1, quantum image $|I_2\rangle$ is obtained after scrambling.

Step 4. The 3-D Hénon system is iterated $2^\omega \times 2^h$ times to produce chaotic sequences. Element values should be limited to the gray value range of the image, and the

key should be stored in the form of a quantum image. $|E\rangle$ is obtained after applying XOR operation.

$$|K\rangle = \frac{1}{2^n}\sum_{Y'=0}^{2^h-1}\sum_{X'=0}^{2^\omega-1}|Z_{Y'X'}\rangle|Y'X'\rangle \tag{7}$$

$$|E\rangle = |I_2\rangle \oplus |K\rangle = \frac{1}{2^{h+\omega}}\sum_{Y'=0}^{2^\omega-1}\sum_{X'=0}^{2^h-1}|I_{2\,Y'X'} \oplus K_{Y'X'}\rangle|Y'X'\rangle \tag{8}$$

Step 5. The text information mainly includes names "Name" and "ID". $|0\rangle$ and $|1\rangle$ are used to distinguish them, respectively. The ASCII code $|W\rangle$ corresponding to each character in the text information is converted into an 8-bit binary sequence.

Step 6. Taking into account the properties of human visual perception, channel G or B are chosen to embed the watermark. The color image of size $L\times L$ ($L \geq 2N$) is chosen as the carrier, and its G and B channels are decomposed by the quantum Haar wavelet transform. Row and column decomposition is achieved by performing H_{r} and H_{c} operations on the horizontal direction respectively.

$$H_{2^n} = H_{\mathrm{r}}H_{\mathrm{c}} = (I_2^{\otimes q} \otimes I_2^{\otimes n} \otimes H_{2^n})(I_2^{\otimes q} \otimes H_{2^n} \otimes I_2^{\otimes n}) \tag{9}$$

Step 7. Combined with the chaotic sequence, coefficient r is randomly selected in $\mathrm{LL_b}$. In the gray value qubit of the selected pixel, the XOR of the lower two bits is compared with the embedded bit through QE. If $|c\rangle = |1\rangle$, it remains unchanged, and if $|c\rangle = 0$, the lower qubits are modified to embed the text information. The remaining intermediate frequency subbands are used to embed the secret image. The inverse QHWT is utilized, and by merging the three channels, the watermarked quantum image denoted as $|WE\rangle$ is acquired.

The decryption and extraction process of the algorithm is in the following.

Step 1. By applying QHWT operation on the G and B channel of the double-watermarked quantum image, the subbands $\mathrm{LL'_b}$, $\mathrm{LH'_b}$, $\mathrm{HL'_b}$, $\mathrm{HH'_b}$ and $\mathrm{LL'_g}$, $\mathrm{LH'_g}$, $\mathrm{HL'_g}$, $\mathrm{HH'_g}$ are obtained. The binary sequence is extracted correlation coefficient from the subband $\mathrm{LL_b}$. The information is converted into ASCII code for identity authentication, the secret image is extracted from the rest of the subbands, and the inverse QHWT is applied to obtain the ciphertext image $|E\rangle$.

Step 2. The chaotic sequence is iteratively generated by the 3D Hénon hyperchaotic system, and the quantum image $|Q\rangle$ is obtained by applying XOR between the artificially constructed quantum key image $|K\rangle$ and the quantum ciphertext image $|E\rangle$.

Step 3. Image $|P\rangle$ can be obtained by scrambling quantum image $|Q\rangle$ with index sequence D_1, and the base image $|I\rangle$ can be obtained by inverting the inverse scrambling operation on $|P\rangle$.

4. Simulation outcomes and performance analysis

This study utilizes four grayscale images sized 100×200 and another four sized 128×256 as original images. The *Baboon* and *Sailboat* images serve as color carriers.

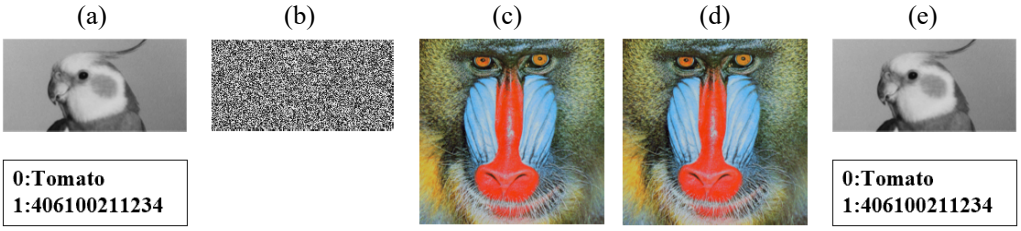

Fig. 6. (a) Original images and text information, *Coco*. (b) Ciphertext images, *Coco*. (c) Carrier images, *Baboon*. (d) Visually meaningful images, *Baboon*. (e) Extract and decrypt images, *Coco*.

All experiments are conducted in MATLAB. The chaotic system's control parameters are configured as $a = 1.99$, $b = 0.001$, $\mu = 1.14$, and set $x_0 = 1.4$, $y_0 = 0.101$, $z_0 = 0.1$. Other parameters are $a = 2$, $b = c = d = 1$, $k = 43$. Test image *Coco* is shown in Fig. 6(a). Figure 6(b) shows the encrypted image, and the visually meaningful image embedded with text and secret image is shown in Fig. 6(d). With the correct key, decrypt the image and text information as shown in Fig. 6(e). To provide an additional insight into the algorithm's characteristics, the key characteristics of the proposed scheme and other typical schemes are summarized in Table 1. The images used in this paper are partly from "CVG-UGR" image database.

T a b l e 1. Comparison of scheme characteristics.

	Scheme			
	Ref. [32]	Ref. [33]	Ref. [34]	Proposed scheme
Text information	+	–	+	+
Transmitted image	Noise-like	Visual meaning	Visual meaning	Visual meaning
Robustness	+	+	–	+
Quantum algorithms	–	+	–	+

4.1. Statistic analysis

Attackers often rely on histogram analysis to examine pixel value distributions in images and extract sensitive information. However, when the histogram of an encrypted image is uniformly distributed or shows substantial deviation from that of the original image, it becomes difficult for adversaries to infer any meaningful content.

The histogram variations of the plaintext images and the ciphertext images are presented in Fig. 7. Figures 7(a)–(d) are the histogram of the base image, Figs. 7(e)–(h) are the histogram of the corresponding ciphertext images.

In statistical analysis attacks, the assessment of pixel correlation among neighbors serves as a crucial analytical instrument. Taking *Coco* as an example, Fig. 8 shows the pixel distribution of the original image and the encrypted image in three different directions, respectively. The correlation coefficients of adjacent pixels for eight plaintext and ciphertext images are listed in Table 2. This demonstrates that the plaintext image

exhibits strong correlations in different directions, while the ciphertext image shows significantly reduced correlation, with pixel values becoming uniformly distributed. Therefore, the algorithm demonstrates strong resistance to statistical analysis attacks.

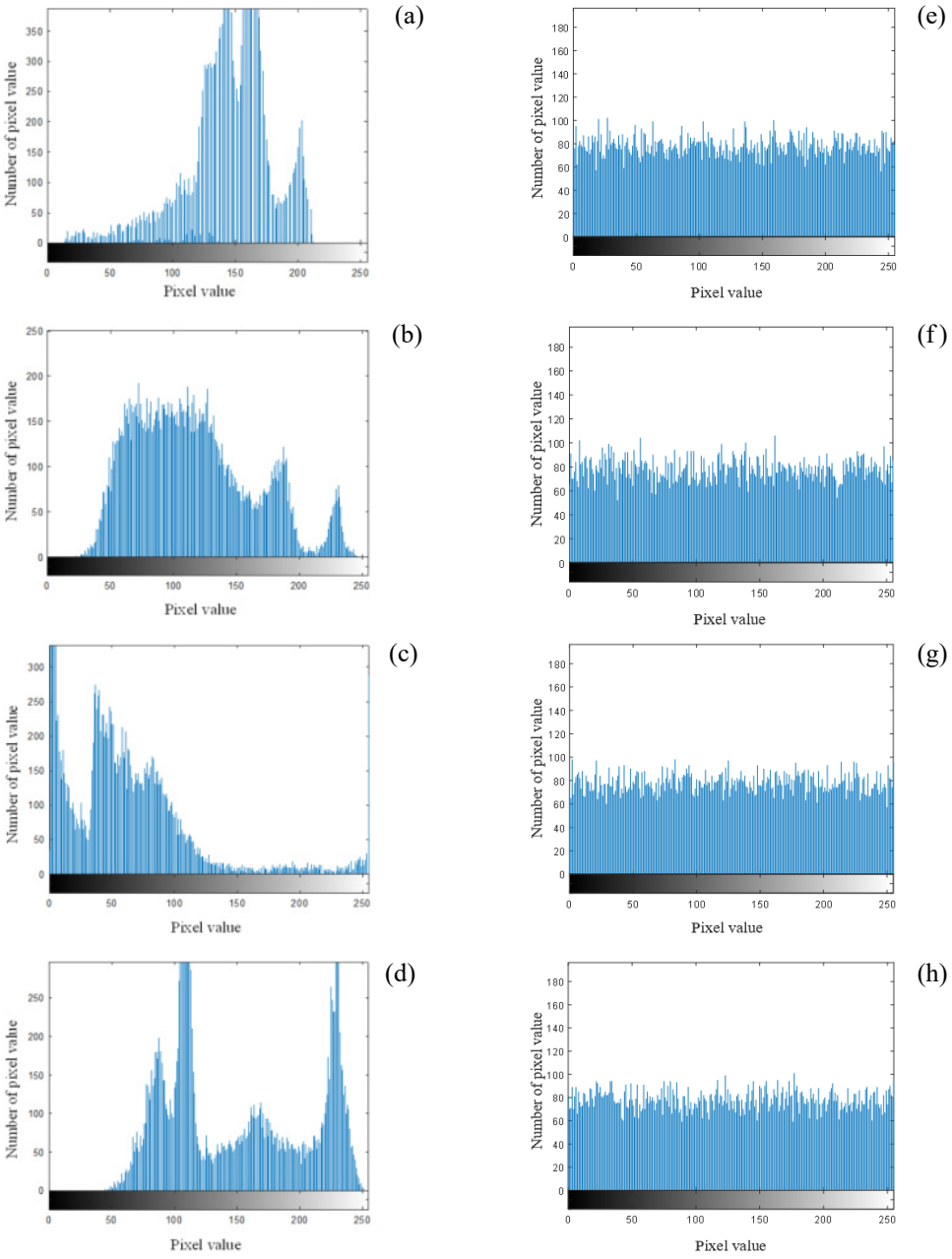

Fig. 7. Original image histogram: (a) *Coco*, (b) *Elaine*, (c) *Mit*, (d) *Milkdrop*. Ciphertext image histogram: (e) *Coco*, (f) *Elaine*, (g) *Mit*, (h) *Milkdrop*.

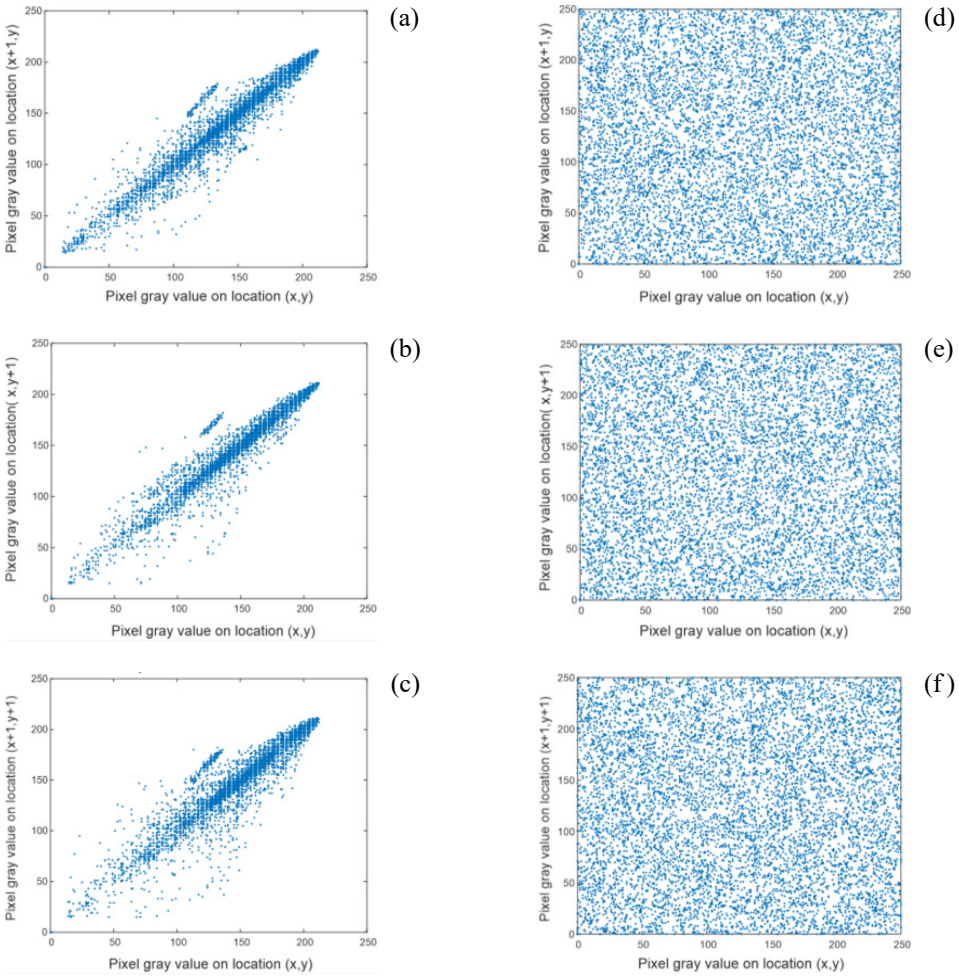

Fig. 8. Adjacent pixel correlation distribution of *Coco*: (a) horizontal, (b) vertical, and (c) diagonal. Encrypted *Coco* adjacent pixel correlation distribution: (d) horizontal, (e) vertical, and (f) diagonal.

T a b l e 2. The correlation coefficient between adjacent pixels.

Size ($M \times N$)	Image	Horizontal	Vertical	Diagonal
100×200	Original *Coco*	0.9684	0.9636	0.9323
	Encrypted *Coco*	−0.0056	−0.0058	−0.0029
	Original *Elaine*	0.9451	0.9447	0.9303
	Encrypted *Elaine*	−0.0012	0.0081	−0.0047
128×256	Original *Goldhill*	0.9364	0.9538	0.9356
	Encrypted *Goldhill*	−0.0038	0.0026	0.0043
	Original *Livingroom*	0.8977	0.8626	0.8725
	Encrypted *Livingroom*	−0.0034	0.0037	−0.0062

4.2. Information entropy

The information entropy values for both plaintext and encrypted images are shown in Table 3. The entropy of the encrypted versions of the four grayscale images is nearly equal to the ideal value of 8 bits. The information entropy of B channel and G channel of carrier image changes little before and after embedding secret information. This shows that the scheme can effectively deal with information entropy attack and ensure the visualization of transmitted images.

T a b l e 3. Information entropy (bit).

Original images	Carrier images	Information entropy					
		Original images	Encrypted images	Carrier images		Visual meaning images	
				B	G	B	G
Coco	*Baboon*	6.4511	7.9975	7.2895	6.3175	7.4271	6.5823
Elaine	*Plane*	7.4291	7.9973	7.2136	7.6429	7.3161	7.7632
Mit	*Baboon*	7.0269	7.9976	7.2895	6.3175	7.3574	6.7564
Milkdrop	*Plane*	7.2162	7.9969	7.2136	7.6429	7.2856	7.7142

4.3. Key sensitivity analysis

Figure 9(a) displays the decrypted grayscale image *Coco* obtained with the correct key. When the key with a slight deviation from the correct one is used for decryption, the decryption image is shown in Figs. 9(b)–(h). It is proved that the algorithm is highly sensitive to key changes.

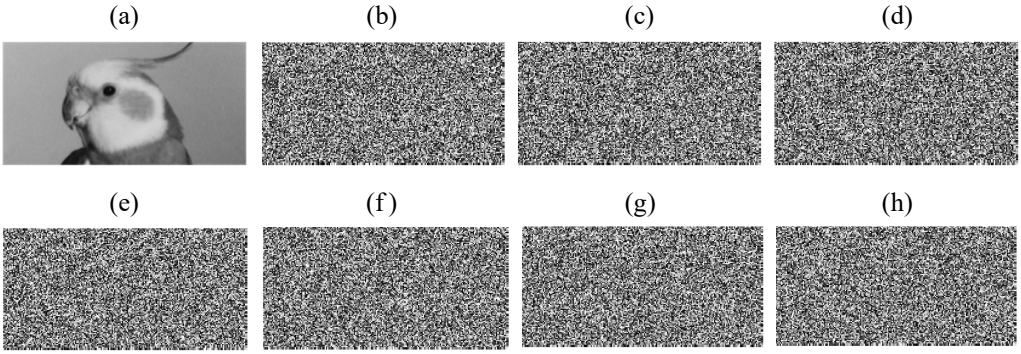

Fig. 9. (a) Correct keys, (b) wrong x_0, (c) wrong y_0, (d) wrong z_0, (e and g) wrong a, (f and h) wrong b.

4.4. Invisibility analysis

The PSNR metric effectively captures the differences introduced by secret information embedding. The SSIM index comprehensively considers the brightness, contrast and structure of the image, providing a more comprehensive evaluation for the analysis of

T a b l e 4. PSNR and SSIM.

Original images	Carrier images	PSNR [dB]	SSIM
Coco	*Baboon*	42.11	0.9745
Elaine	*Sailboat*	43.06	0.9867
Mit	*Baboon*	39.94	0.9650
Milkdrop	*Sailboat*	42.38	0.9546

invisibility. Table 4 provides the PSNR and the SSIM values of the encrypted images and the carrier images (*Baboon* and *Sailboat*) after embedding the text information. The data within the table reveals that the mean PSNR value exceeds 30 decibels, and the SSIM value approaches 1, thereby satisfying the visibility criteria for the algorithm. The difficulty in discerning meaningful data by the human eye from the carrier images demonstrates the algorithm has strong invisibility.

4.5. Robustness analysis

To evaluate the security and resilience of the image encryption and authentication method introduced in this document, a cutting attack is used to evaluate. Throughout the manipulation and conveyance of images, there is a possibility that a minor portion of the data could be either lost or compromised by unauthorized individuals. Table 5 summarizes the bit error rate of identity information and image NC value extracted when the carrier image *Sailboat* is clipped in four different proportions, which are used as quantitative indicators to analyze the recovery degree of ciphertext images and the authentication results of identity information. The decrypted image extracted from the cropped carrier image can still identify useful information. In addition, the bit error rate of the text information selected for testing is calculated

According to the data in the table, under a certain degree of attack, the bit error rate of the extracted text information is 0, which can effectively identify the identity information. When subjected to 1/4 degree cropping attack, the extracted text information although there will be a few errors, there are still some useful information can be received. The result proves that the algorithm can resist clipping attack to some extent.

T a b l e 5. Decryption and authentication effects under different attacks.

Attack type		*Coco*		*Milkdrop*	
		‘0:Tomato1:406100211234’		‘0:Tomato1:406100211234’	
		NC	BER	NC	BER
Noise	0.005	0.9992	0	0.9987	0
	0.01	0.9968	0	0.9971	0
	0.05	0.9913	0	0.9926	0.0313
Cutting	1/64	0.9987	0	0.9892	0
	1/16	0.9362	0.0313	0.8941	0
	1/4	0.8421	0.1250	0.9137	0.1250

5. Conclusions

This work presents a novel framework by fusing quantum-based encryption with dual watermarking for simultaneous image protection and authentication. The combination of quantum affine transformation, Hénon mapping, and quantum Haar wavelet transform not only bolsters the cryptographic strength but also suggests a flexible structure for embedding identity information in a visually meaningful manner. The experimental analysis demonstrates superior resistance against differential, statistical, and noise-based attacks, validating the robustness of the approach. Beyond its immediate contribution to secure image transmission, the method lays a foundation for future research on quantum-inspired multimedia security, where both encryption and authentication are jointly optimized to meet the demands of emerging applications such as remote sensing, medical imaging, and intelligent surveillance.

Acknowledgements
This work was supported by the National Natural Science Foundation of China (Grant No. 62466036), the Science and Technology Research Project of Jiangxi Education Department (GJJ2203915) and the Higher Education Reformation Project of Jiangxi Province (JXJG-22-30-5).

References

[1] YE G.D., LIU S.K., XIAO X.C., HUANG X.L., *Image hiding algorithm based on local binary pattern and compressive sensing*, Mathematics and Computers in Simulation **237**, 2025: 316-334. https://doi.org/10.1016/j.matcom.2025.05.005

[2] HU L.L., CHEN M.X., WANG M.M., ZHOU N.R., *Visually meaningful triple images encryption algorithm based on 2D compressive sensing and multi-region embedding*, Knowledge-Based Systems **324**, 2025: 113804. https://doi.org/10.1016/j.knosys.2025.113804

[3] ZOU J.Z., CHEN M.X., GONG L.H., *Invisible and robust watermarking model based on hierarchical residual fusion multi-scale convolution*, Neurocomputing **614**, 2025: 128834. https://doi.org/10.1016/j.neucom.2024.128834

[4] GUO Z., CHEN S.H., ZHOU L., GONG L.H., *Optical image encryption and authentication scheme with computational ghost imaging*, Applied Mathematical Modelling **131**, 2024: 49-66. https://doi.org/10.1016/j.apm.2024.04.012

[5] ABD-EL-ATTY B., *A robust medical image steganography approach based on particle swarm optimization algorithm and quantum walks*, Neural Computing and Applications **35**, 2023: 773-785. https://doi.org/10.1007/s00521-022-07830-0

[6] GONG L.H., LUO H.X., *Dual color images watermarking scheme with geometric correction based on quaternion FrOOFMMs and LS-SVR*, Optics & Laser Technology **167**, 2023: 109665. https://doi.org/10.1016/j.optlastec.2023.109665

[7] NAZIR H., BAJWA I.S., ABDULLAH S., KAZMI R., SAMIULLAH M., *A color image encryption scheme combining hyperchaos and genetic codes*, IEEE Access **10**, 2022: 14480-14495. https://doi.org/10.1109/ACCESS.2022.3143096

[8] KAMAL F.M., ELSONBATY A., ELSAID A., *A novel fractional nonautonomous chaotic circuit model and its application to image encryption*, Chaos, Solitons & Fractals **144**, 2021: 110686. https://doi.org/10.1016/j.chaos.2021.110686

[9] LIU X.L., XU K.S., KANG Z.C., XU M.T., WANG M.M., *New 2D inserting log-logistic-sine chaotic map with applications in highly robust image encryption algorithm*, Nonlinear Dynamics **113**, 2025: 17227-17256. https://doi.org/10.1007/s11071-025-10979-7

[10] Houshmand M., Khorrampanah M., Alkhudhari A.H.M., *Optimized quantum computing technique to encrypt medical images*, Optical and Quantum Electronics **56**(3), 2024: 442. https://doi.org/10.1007/s11082-023-06041-8

[11] Wang Z.B., Xu M.Z., Zhang Y.N., *Review of quantum image processing*, Archives of Computational Methods in Engineering **29**(2), 2022: 737-761. https://doi.org/10.1007/s11831-021-09599-2

[12] Su J., Guo X.C., Liu C.Q., Lu S.H., Li L., *Improved novel quantum image representation and its experimental test on IBM quantum experience*, Scientific Reports **11**, 2021: 13879. https://doi.org/10.1038/s41598-021-93471-7

[13] Venegas-Andraca S., Bose S., *Storing, processing and retrieving an image using quantum mechanics*, Proceedings of the SPIE, Vol. 5105, Quantum Information and Computation, 2003: 137-147. https://doi.org/10.1117/12.485960

[14] Le P.Q., Dong F., Hirota K., *A flexible representation of quantum images for polynomial preparation, image compression, and processing operations*, Quantum Information Processing **10**, 2011: 63-84. https://doi.org/10.1007/s11128-010-0177-y

[15] Zhang Y., Lu K., Gao Y.H., Wang M., *NEQR: a novel enhanced quantum representation of digital images*, Quantum Information Processing **12**, 2013: 2833-2860. https://doi.org/10.1007/s11128-013-0567-z

[16] Jiang N., Wang J., Mu Y., *Quantum image scaling up based on nearest-neighbor interpolation with integer scaling ratio*, Quantum Information Processing **14**, 2015: 4001-4026. https://doi.org/10.1007/s11128-015-1099-5

[17] Liang J.Y., Peng H.P., Li L.X., Tong F.H., Bao S., Wang L.L., *A secure and effective image encryption scheme by combining parallel compressed sensing with secret sharing scheme*, Journal of Information Security and Applications **75**, 2023: 103487. https://doi.org/10.1016/j.jisa.2023.103487

[18] Gao Y.J., Xie H.W., Zhang J., Zhang H., *A novel quantum image encryption technique based on improved controlled alternated quantum walks and hyperchaotic system*, Physica A: Statistical Mechanics and its Applications **598**, 2022: 127334. https://doi.org/10.1016/j.physa.2022.127334

[19] Zhou N.R., Huang L.X., Gong L.H., Zeng Q.W., *Novel quantum image compression and encryption algorithm based on DQWT and 3D hyper-chaotic Henon map*, Quantum Information Processing **19**(9), 2020: 284. https://doi.org/10.1007/s11128-020-02794-3

[20] Mou D.K., Dong Y.M., *Color image encryption algorithm based on quantum random walk and multiple reset scrambling*, Physica Scripta **99**(3), 2024: 035106. https://doi.org/10.1088/1402-4896/ad22c2

[21] Huang X.L., Dong Y.X., Ye G.D., Shi Y., *Meaningful image encryption algorithm based on compressive sensing and integer wavelet transform*, Frontiers of Computer Science **17**(3), 2023: 173804. https://doi.org/10.1007/s11704-022-1419-8

[22] Guan Z.Y., Jing J.P., Deng X., Xu M., Jiang L., Zhang Z., Li Y.P., *DeepMIH: Deep invertible network for multiple images hiding*, IEEE Transactions on Pattern Analysis and Machine Intelligence **45**(1), 2023: 372-390. https://doi.org/10.1109/TPAMI.2022.3141725

[23] Sun J.Y., Cai H., Wang G., Gao Z.B., Zhang H., *FPGA image encryption-steganography using a novel chaotic system with line equilibria*, Digital Signal Processing **134**, 2023: 103889. https://doi.org/10.1016/j.dsp.2022.103889

[24] Dutta S., Dash N.R., Banerjee S., Srikanth R., *Quantum steganography using catalytic and entanglement-assisted quantum codes*, arXiv preprint, 2025: 2505.15869v1. https://arxiv.org/abs/2505.15869

[25] Zhou N.R., Wu J.W., Chen M.X., Wang M.M., *A quantum image encryption and watermarking algorithm based on QDCT and baker map*, International Journal of Theoretical Physics **63**(4), 2024: 100. https://doi.org/10.1007/s10773-024-05630-x

[26] Wang M.X., Yang H.M., Jiang D.H., Yan B., Pan J.S., Liu T., *A novel quantum color image steganography algorithm based on turtle shell and LSB*, Quantum Information Processing **21**(4), 2022: 148. https://doi.org/10.1007/s11128-022-03494-w

[27] SUN J.Y., WANG W.T., ZHANG H., ZHANG J., *Color image quantum steganography scheme and circuit design based on DWT+DCT+SVD*, Physica A: Statistical Mechanics and its Applications **617**, 2023: 128688. https://doi.org/10.1016/j.physa.2023.128688

[28] NARENDRA M., VALARMATHI M.L., ANBARASI L.J., *Watermarking techniques for three-dimensional (3D) mesh models: A survey*, Multimedia Systems **28**(2), 2022: 623-641. https://doi.org/10.1007/s00530-021-00860-z

[29] GHAI D., GIANEY H.K., JAIN A., UPPAL R.S., *Quantum and dual-tree complex wavelet transform -based image watermarking*, International Journal of Modern Physics B **34**(4), 2020: 2050009. https://doi.org/10.1142/S0217979220500095

[30] ZHANG H., KONE M.M.K., MA X.Q., ZHOU N.R., *Frequency-domain attention-guided adaptive robust watermarking model*, Journal of the Franklin Institute **362**(3), 2025: 107511. https://doi.org/10.1016/j.jfranklin.2025.107511

[31] ANAND A., SINGH A.K., *SDH: secure data hiding in fused medical image for smart healthcare*, IEEE Transactions on Computational Social Systems **9**(4), 2022: 1265-1273. https://doi.org/10.1109/TCSS.2021.3125025

[32] ABD EL-LATIF A.A., ABD-EL-ATTY B., HOSSAIN M.S., RAHMAN M.A., ALAMRI A., GUPTA B.B., *Efficient quantum information hiding for remote medical image sharing*, IEEE Access **6**, 2018: 21075 -21083. https://doi.org/10.1109/ACCESS.2018.2820603

[33] DHALL S., GUPTA S., *Multilayered highly secure authentic watermarking mechanism for medical applications*, Multimedia Tools and Applications **80**(12), 2021: 18069-18105. https://doi.org/10.1007/s11042-021-10531-w

[34] WANG H.K., XU G.B., JIANG D.H., *Quantum grayscale image encryption and secret sharing schemes based on Rubik's Cube*, Physica A: Statistical Mechanics and its Applications **612**, 2023: 128482. https://doi.org/10.1016/j.physa.2023.128482

Received July 21, 2025
in revised form September 3, 2025