frontiers | Frontiers in Physics

TYPE Original Research
PUBLISHED 14 October 2025
DOI 10.3389/fphy.2025.1655166

OPEN ACCESS

EDITED BY
Fei Yu,
Changsha University of Science and Technology, China

REVIEWED BY
Huihai Wang,
Central South University, China
Baoxiang Du,
Heilongjiang University, China

*CORRESPONDENCE
Li Niu,
8201501009@jiangnan.edu.cn

RECEIVED 27 June 2025
ACCEPTED 17 July 2025
PUBLISHED 14 October 2025

CITATION
Tu C, Niu L and Cui R (2025) A child information protection scheme based on hyperchaotic mapping.
Front. Phys. 13:1655166.
doi: 10.3389/fphy.2025.1655166

A child information protection scheme based on hyperchaotic mapping

Chenchen Tu[1,2], Li Niu[3]* and Rongrong Cui[4]

[1]College of Textile Science and Engineering, Jiangnan University, Wuxi, Jiangsu, China, [2]School of Fashion, Dalian Polytechnic University, Dalian, Liaoning, China, [3]School of Digital Technology & Innovation Design, Jiangnan University, Wuxi, Jiangsu, China, [4]School of Fashion Design and Engineering, Zhejiang Sci-Tech University, Hangzhou, Zhejiang, China

This paper proposes an encryption scheme based on hyperchaotic mapping for child information protection. First, phase diagrams of the hyperchaotic mapping are plotted under different parameter combinations, and the variation in phase trajectories confirms the sensitivity of the hyperchaotic mapping to control parameters. Then, the hyperchaotic mapping is iterated to obtain chaotic sequences, and the chaotic sequences are quantized to obtain pseudo-random sequences. Finally, based on those, a scrambling algorithm and a diffusion algorithm are designed to encrypt and protect the images. The original images are scrambled and diffused to obtain the ciphertext images and used to protect the information of missing children, which can effectively protect the safety of children's information and assist the public security bureaus to quickly contact the parents of missing children.

KEYWORDS

child information protection, hyperchaotic mapping, image encryption, children's clothes, information security

1 Introduction

In the digital era, data are increasingly becoming an important part of personal life and economic development [1, 2]. Among various data formats, images are widely used as information carriers for Internet transmission as they can carry large amounts of information and have high visibility [3, 4]. Due to the dependence of work life on the Internet, the rich information contained in images is at risk of being leaked [5–7]. Among these, the secure transmission and storage of image data face significant challenges as they contain sensitive information such as biometrics and geographic locations [8, 9]. Especially in the field of social welfare, such as missing children tracking, images need to be widely disseminated to expand the search scope, but they also must be prevented from being maliciously utilized to cause secondary damage [10, 11]. Image encryption can be used to encrypt an image into a noise-like ciphertext image by various means [12–15].

As an effective method to protect image information, image encryption techniques, especially those based on chaos theory, have been a hot topic of research in recent years [16]. This is because many inherent properties of chaotic systems, including ergodicity, acyclicity, high sensitivity to initial conditions and control parameters, and pseudo-randomness, meet the needs of cryptography and have an irreplaceable

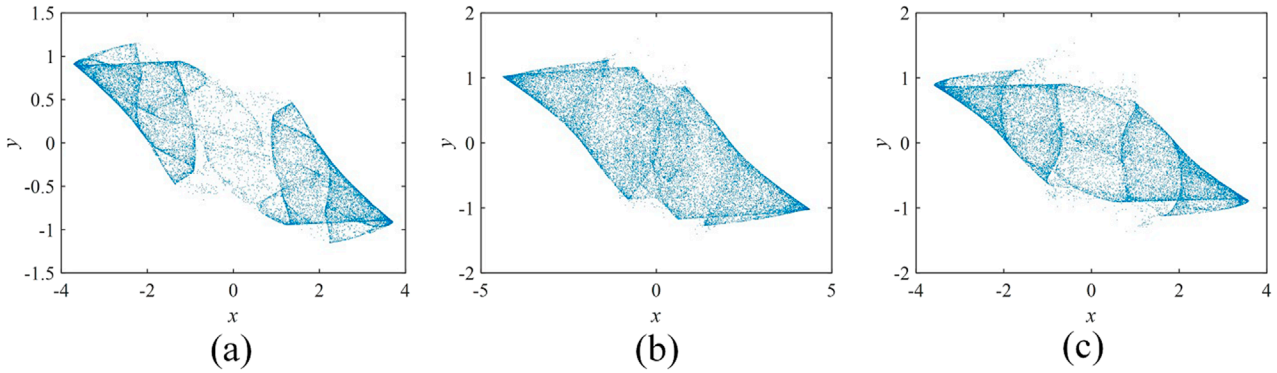

FIGURE 1
Phase diagrams of MCHM, (x_0, y_0) = [0.3, 0.5]: **(a)** (*a*, *b*, *c*, *d*, and *e*) = [-1, 1.5, −1, 1, 0.5]; **(b)** (*a*, *b*, *c*, *d*, and *e*) = [-1, 1.5, −1.1, 1, 0.5]; **(c)** (*a*, *b*, *c*, *d*, and *e*) = [-1, 1.5, −1, 1.2, 0.5].

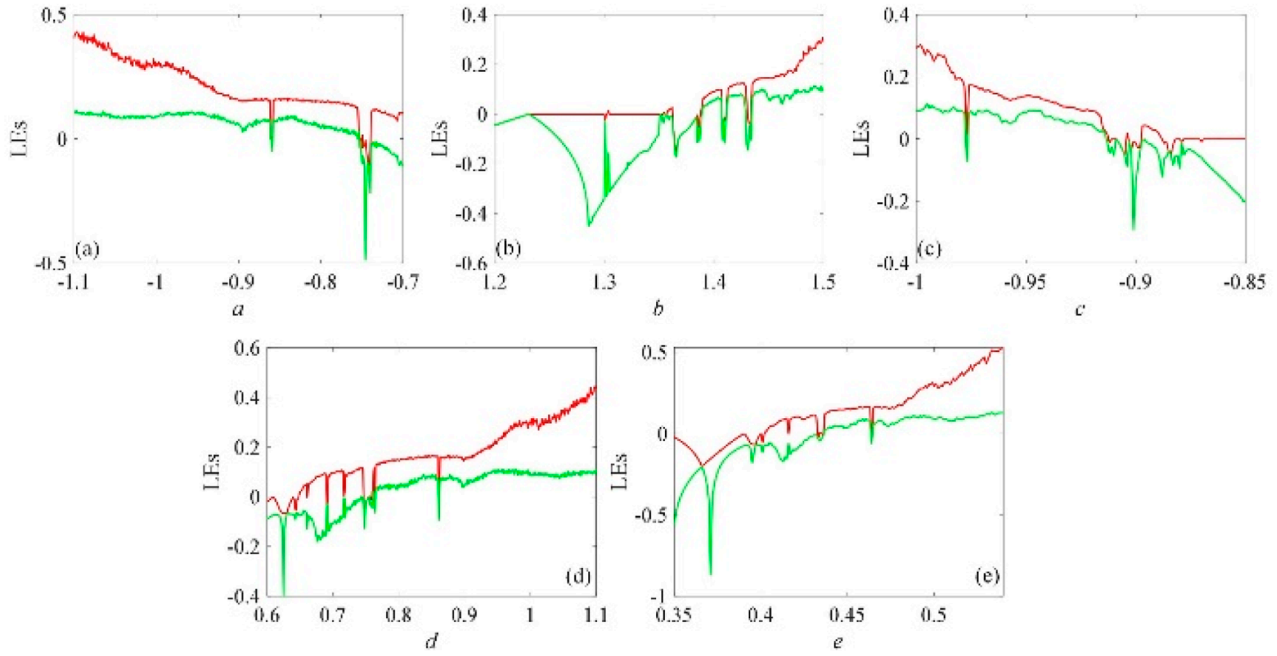

FIGURE 2
Distribution of LEs with different parameters. **(a)** Parameter *a*; **(b)** parameter *b*; **(c)** parameter *c*; **(d)** parameter *d*; **(e)** parameter *e*.

advantage in image encryption [17–21]. Meanwhile, some scholars have pointed out that hyperchaotic systems can provide higher security to encryption algorithms [22, 23]. In the context of information protection and verification of missing children, hyperchaotic mapping is preferred in view of the need for real-time performance. In this study, hyperchaotic mapping [24–30] is used in the design of the missing child information encryption scheme.

In the previous image encryption scheme design and application, usually, the image is compressed and encrypted to realize the fast transmission and protection of the image on the Internet [31–33]; another method includes encoding and encryption of the image to realize the safe storage of the information and prevent leakage or tampering [31, 34–36]; there is also the encryption and steganography of the image to realize the double-layer protection of the image [37–39]. However, information protection and verification of missing children are different from the previous image encryption protection processes, where the main idea is to encrypt children's information to obtain ciphertext images and apply the ciphertext images to children's products as stickers, such as on children's school bags, water cups, and clothes. In the process of children getting lost or being found, the children's information is verified, and it is convenient to get in touch with the children's

TABLE 1 NIST test results for MCHM.

Items	MCHM	
	P-value	PR (%)
Frequency	0.198732	98
Block frequency	0.346291	99
Cumulative sums	0.637462	99
Runs	0.029485	97
Longest run	0.875123	100
Rank	0.372634	99
FFT	0.082712	99
Non-overlapping template	0.028374	100
Overlapping template	0.192734	100
Universal	0.876123	98
Approximate entropy	0.468102	98
Random excursions	0.076390	100
Random excursions variant	0.048716	100
Serial	0.419021	99
Linear complexity	0.289667	100

parents quickly. In view of this application idea, this paper designs a missing child information protection and verification scheme based on hyperchaotic mapping. The information protection scheme is divided into two steps: image scrambling and diffusion, which when combined with chaotic sequences can effectively hide the original information of children, and the reversible encryption scheme ensures that the information of children can be decrypted and verified quickly.

This paper carries out the following tasks:

1. Memristor-coupled hyperchaotic mapping (MCHM) is presented in this paper, and its phase diagram is analyzed.
2. The image or photo containing a child's information is encrypted with a confusion algorithm and a diffusion algorithm.
3. Security analysis of encrypted images to highlight the superiority of the scheme.

2 Chaotic mapping

MCHM is obtained by coupling the memristor and the iterative chaotic map with infinite collapse (ICMIC), and its mathematical model is described as Equation 1:

$$\begin{cases} x_{i+1} = \sin\left(\frac{a}{x_i}\right) + b(c + dy_i^2)x_i \\ y_{i+1} = y_i + ex_i \end{cases}. \quad (1)$$

When the initial value is $(x_0, y_0) = [0.3, 0.5]$ and the system parameters a, b, c, d, and e are $[-1, 1.5, -1, 1, 0.5]$, $[-1, 1.5, -1.1, 1, 0.5]$, and $[-1, 1.5, -1, 1.2, 0.5]$, the phase diagrams of MCHM are as shown in Figure 1. Comparing Figures 1a–c, the trajectory of the MCHM clearly changes when the control parameters are changed. That is, when the key changes slightly during the operation of the encryption scheme, the chaotic sequences generated by the MCHM also change, which changes the cipher images. This means that the mapping can provide great security for the design and operation of the encryption scheme.

The chaotic range of the system parameters is decided by analyzing the Lyapunov exponent (LE) response. If one of the LEs is greater than 0, it is in a chaotic state, and if two LEs are greater than 0, it is in a hyperchaotic state. Encryption is carried out in the chaotic state situation by selecting the parameters. As shown in Figure 2, the range case of each parameter in a chaotic state is $a\in$[-1.1,-0.75], $b\in$[1.35,1.5], $c\in$[-1,-0.9], $d\in$[0.7,1.1], and $e\in$[0.4,0.54]. When parameter a is at [-1.1, -0.875] or [-0.87, -0.747], parameter b is at [1.43, 1.5], parameter c is at [-1, -0.975] or [-0.96, -0.92], parameter d is at [0.85, 1.1], and parameter e is at [0.47, 0.54], the system is in a hyperchaotic state. More complex dynamic characteristics are shown in this state, and the pseudo-random sequence generated by the system through iteration has higher randomness.

To test the randomness of the chaotic sequences, an NIST test (NIST SP800-22) is performed. It includes 15 tests. When the p-value is greater than or equal to 0.01 and the pass rate is greater than 96%, the sequence passes the randomness test. The specific test results are shown in Table 1. It can be seen from the results that this random sequence exhibits good randomness characteristics in statistical tests. It is shown that it is suitable for the proposed encryption scheme.

3 Encryption scheme

The encryption process includes three stages: parameter setting, image confusion, and diffusion. The encryption schematic is shown in Figure 3. The detailed steps are described as follows:

Step 1: The image containing the child's information and photo is imported, and the size of the ith image is recorded as $m_i \times n_i \times l_i$.

Step 2: All images are converted into column vectors, and all column vectors are stitched into a whole, which is denoted as vector A, with length vl.

Step 3: Column vector A is converted to cube B with dimensions $M \times N \times L$, where M and N are the height and width of each plane of the cube, respectively, and L is the height of the cube. M and N can be set as desired, and L is obtained by Equation 2.

$$\boldsymbol{L} = \text{ceil}\left(\frac{vl}{MN}\right). \quad (2)$$

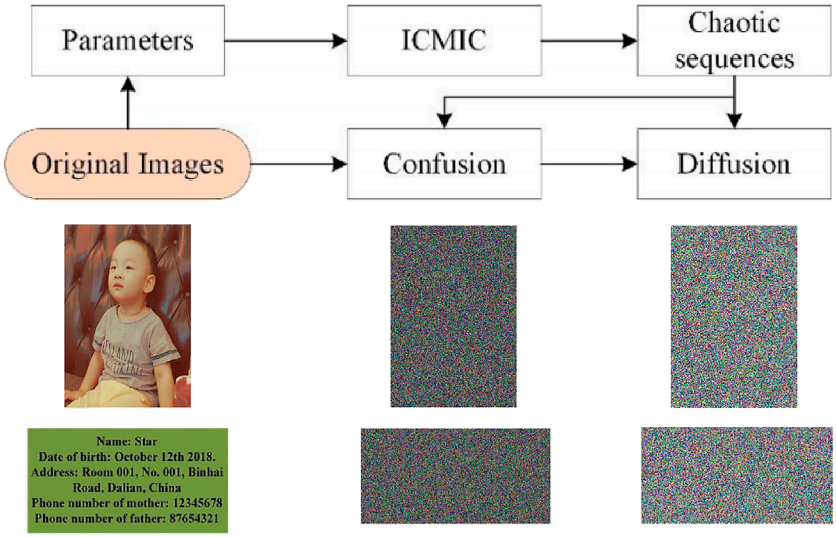

FIGURE 3
Encryption schematics.

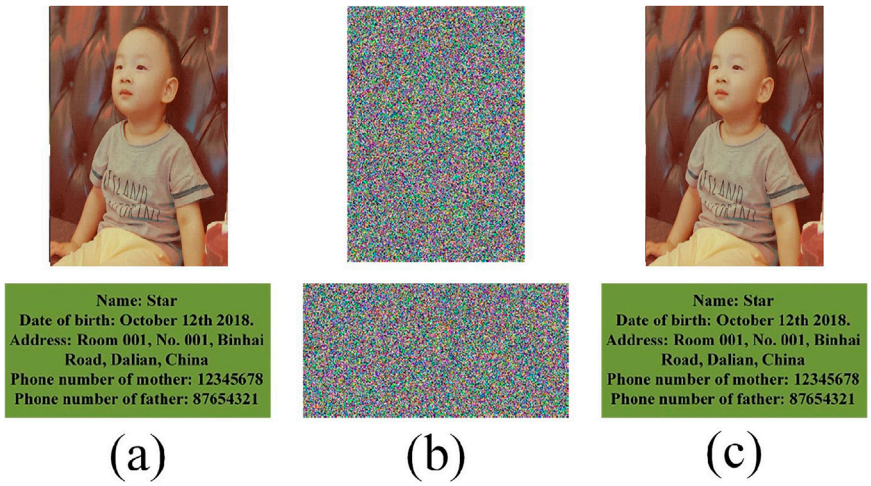

FIGURE 4
Simulation results: **(a)** original images, "kid" and "information1"; **(b)** encryption images; **(c)** decryption images.

Step 4: Based on the input image, the parameters associated with the plaintext h_i are obtained.

$$\begin{cases} Hm(i) = -\sum_{j=1}^{255} p_j \log_2(p_j), i = 1 \cdots L \\ hm(i) = Hm(i) - \text{floor}(Hm(i)), i = 1 \cdots L \\ h_i = \frac{1}{L} \sum_{j=(i-1)\text{floor}(l)+1}^{i\text{floor}(l)} hm(j), i = 1 \cdots 7 \\ l = \frac{L}{7} \end{cases}, \quad (3)$$

where P_j stands for the pixel value and Hm stands for information entropy.

Step 5: All the keys are inputted, and the MCHM is iterated based on the total image data volume vl to obtain the chaotic sequences of length $2 \times vl$, and they are quantized to finally obtain two pseudo-random sequences x and y. The pseudo-random sequences q_1–q_{12} used in the algorithm are obtained by Equations 4–8.

$$\alpha = \max(M, N, L). \quad (4)$$

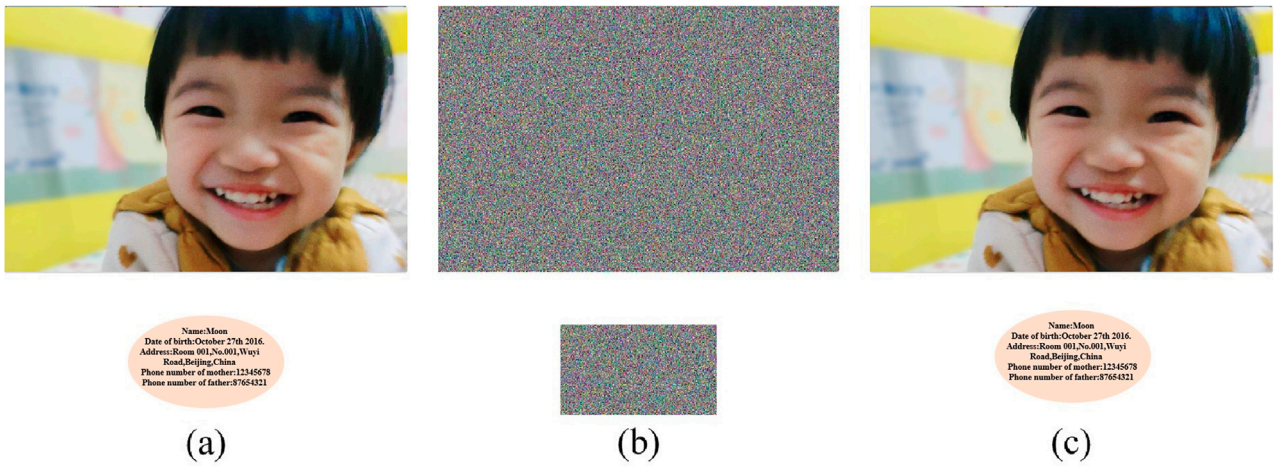

FIGURE 5
Simulation results: **(a)** original images, "girl" and "information2"; **(b)** encryption images; **(c)** decryption images.

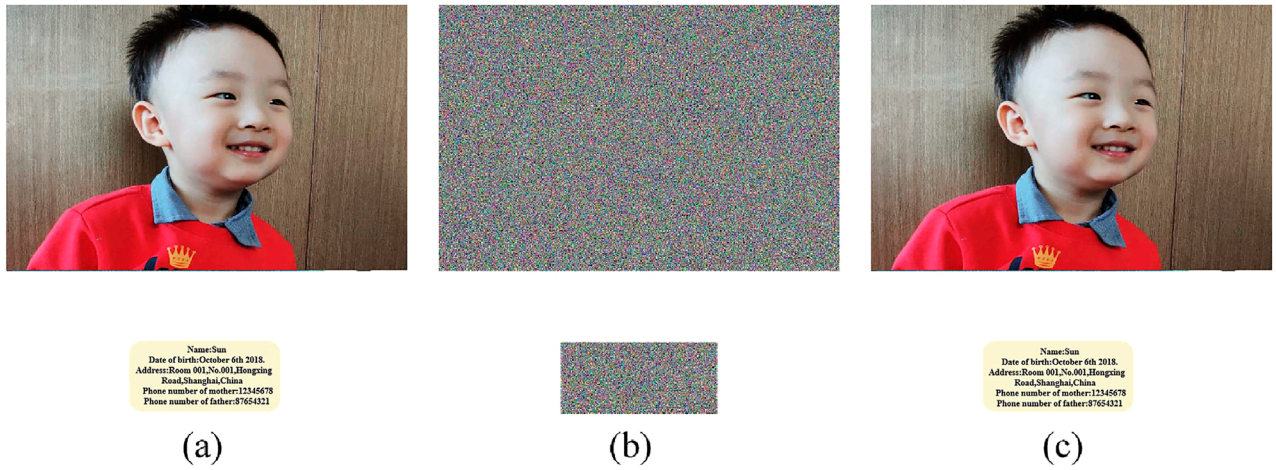

FIGURE 6
Simulation results: **(a)** original images, "boy" and "information3"; **(b)** encryption images; **(c)** decryption images.

$$\begin{cases} q_1 = ((x(1{:}\alpha) + y(1{:}\alpha)) \bmod N) + 1 \\ q_2 = ((x(\alpha + 1{:}2\alpha) + y(\alpha + 1{:}2\alpha)) \bmod N) + 1 \end{cases}. \tag{5}$$

$$\begin{cases} q_3 = (x(2\alpha + 1{:}3\alpha) \bmod M) + 1 \\ q_4 = (y(2\alpha + 1{:}3\alpha) \bmod L) + 1 \\ q_5 = (x(3\alpha + 1{:}4\alpha) \bmod M) + 1 \\ q_6 = (y(3\alpha + 1{:}4\alpha) \bmod L) + 1 \end{cases}. \tag{6}$$

$$\begin{cases} q_7 = (x(4\alpha + 1{:}5\alpha) \bmod N) + 1 \\ q_8 = (y(4\alpha + 1{:}5\alpha) \bmod L) + 1 \\ q_9 = (x(5\alpha + 1{:}6\alpha) \bmod N) + 1 \\ q_{10} = (y(5\alpha + 1{:}6\alpha) \bmod L) + 1 \end{cases}. \tag{7}$$

$$\begin{cases} q_{11} = x(end - MNL + 1{:}end) \\ q_{12} = y(end - MNL + 1{:}end) \end{cases}. \tag{8}$$

Step 6: The sequences q_1 and q_2 are processed and used to control the length of the permutation sequence, and q_1 and q_2 can be obtained by Equations 9, 10.

$$\boldsymbol{q}1(i) = \begin{cases} q1(i) + \text{ceil}\left(\frac{N}{4}\right), q1(i) < \frac{N}{4} \\ q1(i) - floor\left(\frac{N}{4}\right), q1(i) > \frac{3N}{4} \\ q1(i), other \end{cases}. \tag{9}$$

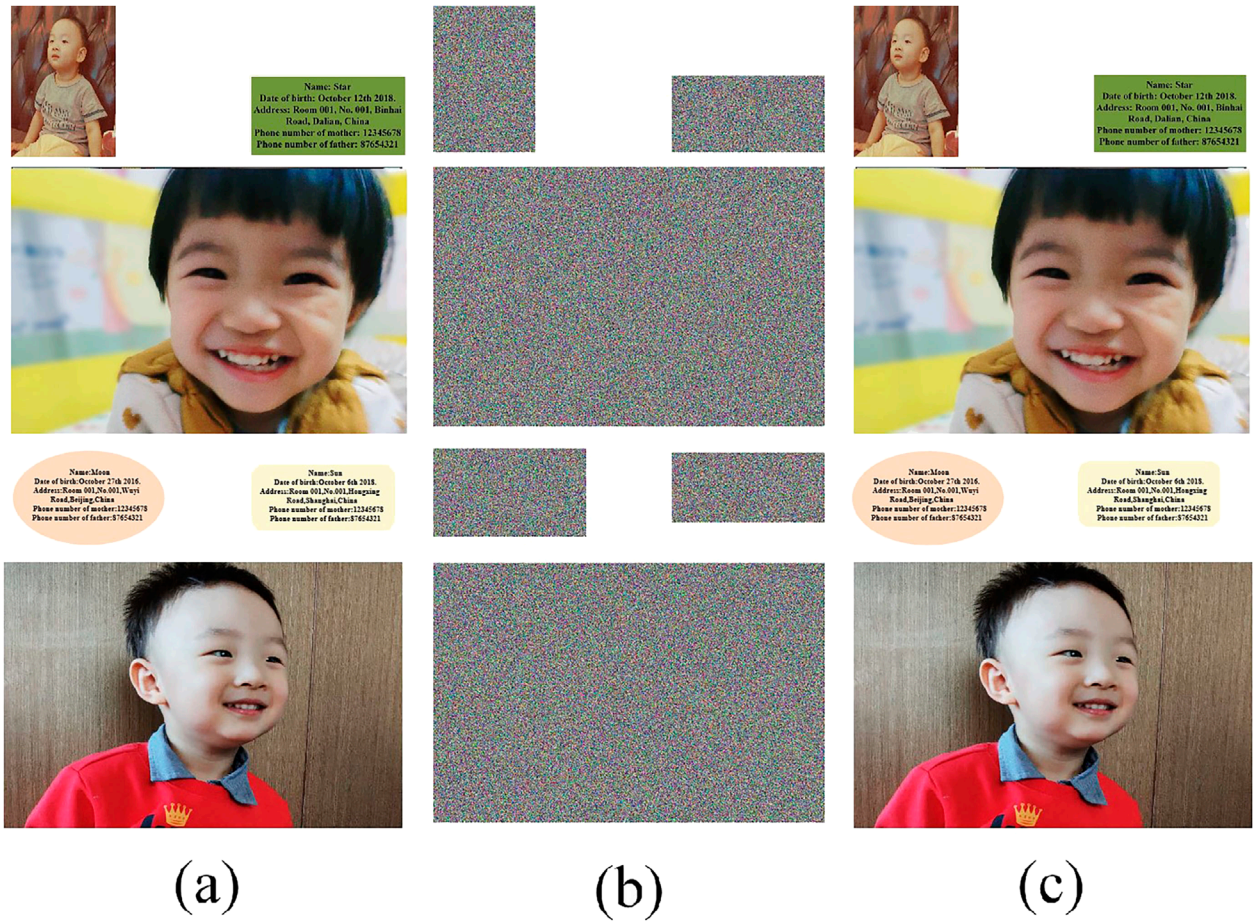

FIGURE 7
Simulation results: **(a)** original images; **(b)** encryption images; **(c)** decryption images.

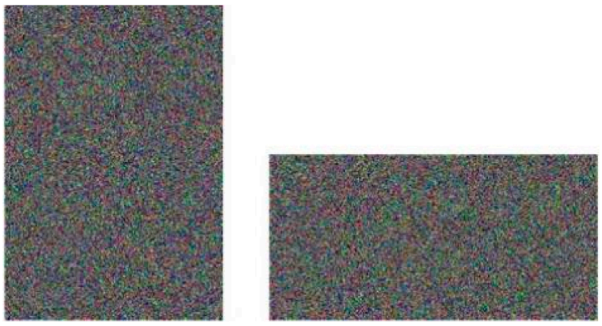

FIGURE 8
Key sensitivity test results, $a = a+10^{-16}$.

$$\boldsymbol{q}2(i) = \begin{cases} q2(i) + \text{ceil}\left(\frac{M}{4}\right), q1(i) < \frac{M}{4} \\ q2(i) - floor\left(\frac{M}{4}\right), q1(i) > \frac{3M}{4} \\ q2(i), other \end{cases}. \quad (10)$$

Step 7: Each row vector of cube B is split into two parts of random length, and the positions are swapped with the row vectors at random locations.

$$\begin{cases} t1 = B(i, 1{:}q1(i), k) \\ t2 = B(i, q1(i)+1{:}end, k) \\ t3 = B(q3((ik \bmod M)+1), 1{:}q1(i), q4((ik \bmod L)+1)) \\ t4 = B(q5((ik \bmod M)+1), q1(i)+1{:}end, q6((ik \bmod L)+1)) \end{cases} \begin{matrix} i = 1 \ldots M \\ , \\ k = 1 \ldots L \end{matrix}. \quad (11)$$

$$\begin{cases} B(i, 1{:}q1(i), k) = t3 \\ B(q3((ik \bmod M)+1), 1{:}q1(i), q4((ik \bmod L)+1)) = t1 \\ B(i, q1(i)+1{:}end, k) = t4 \\ B(q5((ik \bmod M)+1), q1(i)+1{:}end, q6((ik \bmod L)+1)) = t2 \end{cases} \begin{matrix} i = 1 \ldots M \\ , \\ k = 1 \ldots L \end{matrix}. \quad (12)$$

Step 8: Each column vector of cube B is split into two parts of random length, and the positions are swapped with the column vectors at random locations. The cube with the completed column swap is noted as C. It can be obtained by Equations 13, 14.

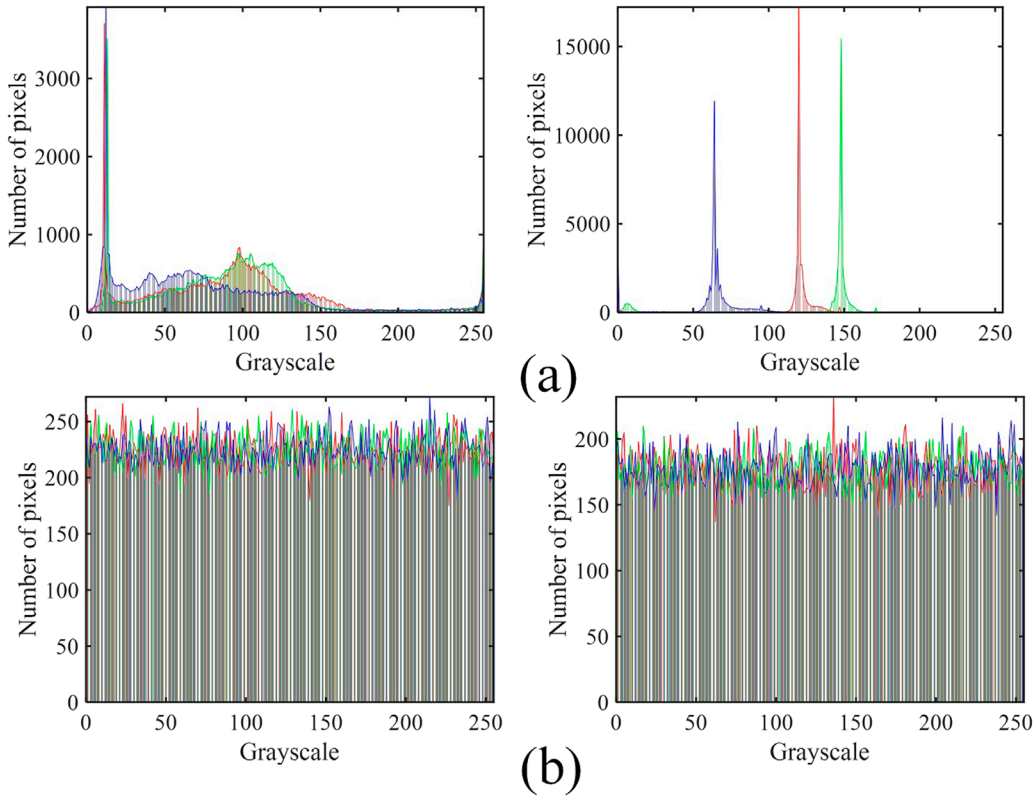

FIGURE 9
Histogram of "kid" and "information1": **(a)** original images and **(b)** encryption images.

TABLE 2 Comparison of key spaces

Algorithms	Reference [40]	Reference [16]	Reference [41]	Reference [42]	Proposed
Key space	2^{249}	2^{266}	2^{352}	2^{398}	2^{471}

$$\begin{cases} t1 = B(1{:}q2(j), j, k) \\ t2 = B(q2(i)+1{:}end, j, k) \\ t3 = B(1{:}q2(j), q7((jk \bmod N)+1), q8((jk \bmod L)+1)) \\ t4 = B(q2(i)+1{:}end, q9((jk \bmod N)+1), q10((jk \bmod L)+1)) \end{cases}, \begin{matrix} j = 1 \ldots N \\ k = 1 \ldots L \end{matrix}. \tag{13}$$

$$\begin{cases} B(1{:}q2(j), j, k) = t3 \\ B(1{:}q2(j), q7((jk \bmod N)+1), q8((jk \bmod L)+1)) = t1 \\ B(q2(i)+1{:}end, j, k) = t4 \\ B(q2(i)+1{:}end, q9((jk \bmod N)+1), q10((jk \bmod L)+1)) = t2 \end{cases}, \begin{matrix} j = 1 \ldots N \\ k = 1 \ldots L \end{matrix}. \tag{14}$$

Step 9: Cube C is converted into column vector D, and the first pixel value is combined with the pseudo-random sequence to get the new pixel value. It can be obtained by Equations 15, 16.

$$\boldsymbol{E}(1) = D(1) \oplus q11(1). \tag{15}$$

$$\begin{cases} E(i) = D(i) \oplus q11(i) \oplus E(i-1), i \bmod 2 = 1 \\ E(i) = D(i) \oplus q12(i) \oplus E(i-1), i \bmod 2 = 0 \end{cases}, i = 2 \ldots MNL. \tag{16}$$

Step 10: The vector E is segmented and shaped according to the dimensions of the original images to obtain the corresponding ciphertext images.

4 Simulation result

Being able to completely encrypt and decrypt children's information and photos is the first requirement for practical applications. In the simulation experiment, three sets of images are used ("kid" with size 200 × 289 × 3, "information1" with size 300 × 152 × 3; "girl" with size 768 × 512 × 3, "information2" with size 300 × 174 × 3; and "boy" with size 768 × 512 × 3, "information3" with size 300 × 138 × 3), and they are encrypted and decrypted separately and in a hybrid manner. The simulation results are shown in Figures 4–7. From Figures 4–6, it can be seen that the scheme can successfully encrypt and decrypt children's information and photographs. As shown in Figure 7, it is also possible to securely encrypt and decrypt a large number of children's information and photographs if necessary. In other words, the proposed encryption and decryption scheme can perform both individual

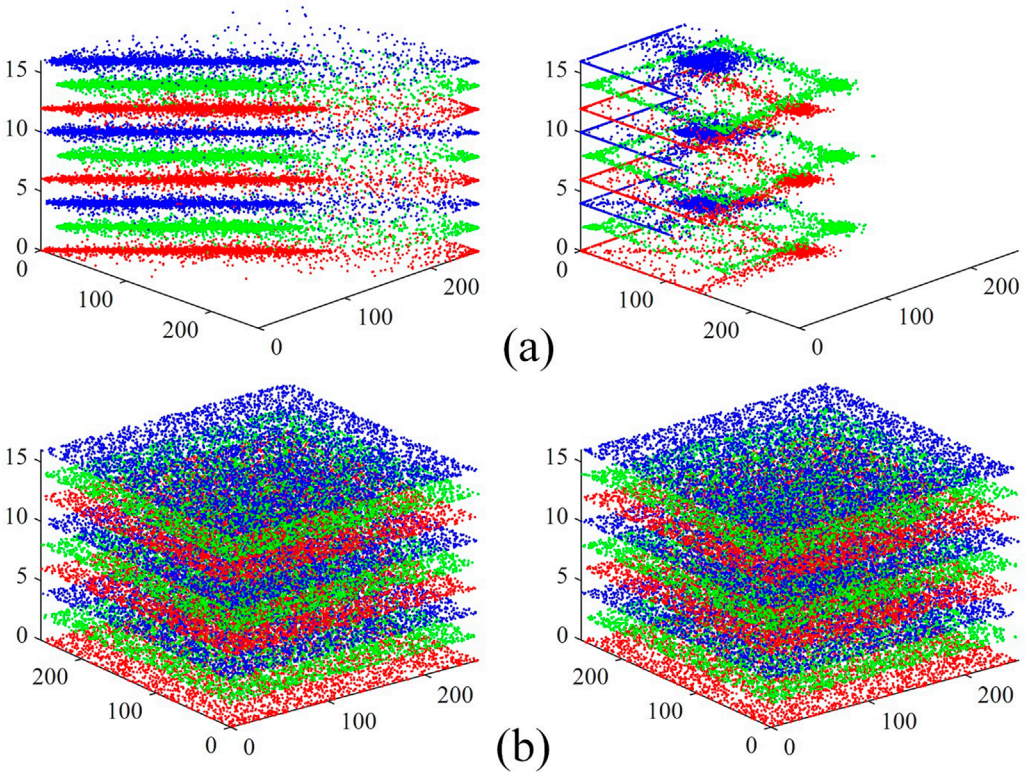

FIGURE 10
Correlation coordinate diagram of "kid" and "information1": **(a)** original images and **(b)** encryption images.

TABLE 3 Correlation coefficients of different images.

Images	Original images			Encryption images		
	Horizontal	Vertical	Diagonal	Horizontal	Vertical	Diagonal
Kid	0.9739	0.9776	0.9551	0.0015	0.0009	−0.0023
Information-1	0.8458	0.7476	0.6864	−0.0016	0.0018	−0.0008
Girl	0.9924	0.9879	0.9813	0.0019	0.0022	−0.0009
Information-2	0.7887	0.6612	0.6005	−0.0008	0.0016	−0.0012
Boy	0.9718	0.9638	0.9534	−0.0012	−0.0016	−0.0036
Information-3	0.7692	0.6208	0.5325	−0.0021	0.0013	−0.0024

processing and batch protection of children's information and photographs.

5 Performance tests

5.1 Key security

5.1.1 Key space

The size of the key space determines whether the encryption scheme can resist exhaustive attacks. Generally, when the key space reaches 2^{100}, it is considered to be capable of resisting exhaustive attacks, and the more the key space is, the better the scheme. In this encryption scheme, the key comprises two components: parameters related to the original images and those associated with hyperchaotic mapping. All the keys are tested one by one; the key space of parameters b and d is 10^{15}, and the key space of the remaining parameters is 10^{16}, so the total key space is $10^{(15\times 2+16\times 7)} = 10^{142} \approx 2^{471}$. The key space of different algorithms is shown in Table 2 [16, 40–42]. The key space test and comparison results indicate that the proposed encryption scheme has adequate capability to resist brute-force attacks.

TABLE 4 Information entropy of different images.

Images	Original images			Encryption images		
	R	G	B	R	G	B
Kid	7.3133	7.1356	7.2659	7.9972	7.9973	7.9972
Information1	4.2216	4.4069	4.6804	7.9962	7.9966	7.9963
Girl	7.8485	7.0813	7.2107	7.9996	7.9995	7.9996
Information2	4.0338	4.3841	4.7260	7.9973	7.9972	7.9972
Boy	7.5723	7.5670	7.5405	7.9995	7.9995	7.9995
Information3	3.1523	4.6179	5.2750	7.9959	7.9958	7.9959

5.1.2 Key sensitivity

The encryption scheme can be considered key-sensitive when a small error in the key can cause decryption failure on the decryption side. In the key sensitivity test, "kid" and "information1" are used as the test images. During the test, each key on the encryption side is kept constant, and the key $a = a + 10^{-16}$ on the decryption side. The decryption results are shown in Figure 8. The ciphertext image cannot be decrypted successfully with smaller parameter variations. As shown in Figure 8, a small error in the key causes the decryption to fail, verifying the key sensitivity of this scheme.

5.2 Statistical characterization

5.2.1 Histogram

A histogram can visually depict the strength of the pixels in the image. By comparing the histograms of the original image and the encrypted image, the ability of the encryption scheme to change the pixel values of the image can be verified. The histograms of "kid" and "information1" are shown in Figure 9. The histograms of the original images have distinct crests and varying distributions at each pixel level. The histograms of the encrypted images show an undifferentiated uniform distribution, which means that the pixel-level distribution of the original images is effectively changed and hidden by the encryption scheme.

5.2.2 Correlation

The property of local smoothing of the image determines a strong correlation between the adjacent pixels of the image, and the intensity of the correlation is measured by both the coordinate plot and the coefficient, which are shown in Figure 9 and Table 2, respectively. As shown in Figure 10, neighboring pixels of "kid" and "information1" are compactly distributed on a straight line with slope 1, which means that the neighboring pixels have the same or similar values. The adjacent pixels of the corresponding encrypted images are distributed throughout the coordinate space, and the values of the adjacent pixels are not correlated. As shown in Table 3, the correlation coefficients of the original images are large, while the correlation coefficients of the encrypted images are close to 0. The change in the correlation between the adjacent pixels of the image indicates that the encryption scheme effectively swaps the location and changes the values of the pixels, thus hiding the correlation characteristics of the original images.

5.2.3 Information entropy

Information entropy is used to test the statistical characteristics of an image. For an image, the higher the information entropy is, the more information it contains, and the more confusing the image is. The original images contain a certain amount of visual information, and their information entropy is a constant value. The information of the encrypted images is confusing, and the information entropy increases with a theoretical maximum value of 8 [43]. The information entropy test results for different images are shown in Table 4, and the information entropy test results for different algorithms are shown in Table 5 [35, 42, 44–46]. As shown in Table 4, compared to the original images, the information entropy of the encrypted images increases significantly and is close to the theoretical maximum. As shown in Table 5, the designed encryption scheme has some advantages in hiding the statistical features of the image data.

5.3 Anti-rolling edge test

The encrypted images containing children's information are printed on the clothes, and if the edge of the image rolls up as the clothes are used, then the edge information may be invalidated. When the edge information of the images is invalidated, the decryption effects of the encrypted images are shown in Figure 11. The edge of the original images is cropped by one circle, and the invalidated information accounts for 23.44%; the cropping effects are shown in Figure 10a. The visual effects of the damaged ciphertext images after being decrypted on the decryption side are shown in Figure 10b. As shown in Figure 11, the original information can still be recovered even if the child's information and photo edges are rolled up to some extent.

5.4 Noise test

The cipher image is usually acquired using the photographing method, which produces noise on the cipher image. Salt and pepper noise and Gaussian noise are chosen to model the effect of noise on image restoration. Figure 12 shows the cipher image subjected to salt and pepper (S&P) noise with 0.1, 0.01, and 0.001 intensity and Gaussian noise with 0.001 intensity. The content of the image can be clearly seen at the reduction end, which in turn illustrates the feasibility of the scheme.

TABLE 5 Information entropy of different algorithms.

Algorithms	Image size	Encryption images (average)		
		R Channel	G channel	B Channel
Reference [44]	256 × 256	7.99720		
Reference [35]	256 × 256	7.99698		
Reference [42]	256 × 256	7.99705		
Reference [45]	256 × 256 × 3	7.9958	7.9950	7.9949
Reference [46]	256 × 256 × 3	7.9837	7.9916	7.9950
Proposed	200 × 289 × 3	7.9972	7.9973	7.9972

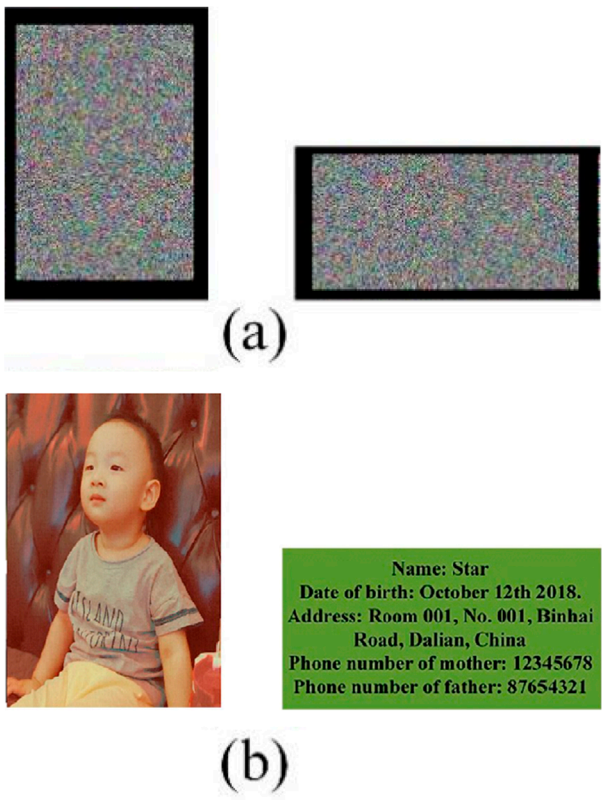

FIGURE 11
Anti-rolling edge test results: **(a)** cipher image and **(b)** restored image.

5.5 Differential attack

Differential attack is a common method used by attackers to crack algorithms. The attacker randomly changes one pixel point of the plaintext image to get the cipher image and analyzes the difference between the two cipher images to crack the scheme.

In the differential attack test, the plaintext image is encrypted twice; the first time is normal encryption, and the cipher image is T_1; the second time, the attacker randomly changes one pixel point of the plaintext image to get the cipher image, and the cipher image is T_2. Since the scheme plaintext information is associated with the initial value of the chaotic system, randomly changing one pixel value of the plaintext image will again result in a different initial value of the chaotic system, and its chaotic sequence also changes. Therefore, the encrypted structure and content are changed, and the resulting encrypted image is also changed.

The difference between T_1 and T_2 is evaluated by the number of pixels change rate (NPCR) and the unified average changing intensity (UACI). The test results are shown in Table 6.

$$\begin{cases} \mathrm{NPCR}(T_1, T_2) = \dfrac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}|\mathrm{Sign}(T_1(i,j) - T_2(i,j))| \times 100\% \\ \mathrm{UACI}(T_1, T_2) = \dfrac{1}{MN}\sum_{i=0}^{M}\sum_{j=0}^{N}\dfrac{|T_1(i,j) - T_2(i,j)|}{255 - 0} \times 100\% \end{cases},$$

where Sign (•) is a symbolic function.

5.6 Comparison with other state-of-the-art encryption schemes

In conclusion, the various performance metrics mentioned above are discussed to compare the proposed encryption algorithm with other state-of-the-art chaotic and non-chaotic encryption algorithms. Reference [46] and Reference [47] proposed chaotic encryption schemes. Reference [48] used the advanced encryption standard (AES) scheme. The comparison results are shown in Table 7.

6 Discussion and conclusion

6.1 Discussion

In recent years, significant progress has been made in visual information mapping techniques based on deep learning [49, 50]. The visual consistency of feature embedding has been optimized

FIGURE 12
Noise test results: **(a)** S&P 0.1; **(b)** S&P 0.01; **(c)** S&P 0.001; **(d)** Gaussian noise 0.001.

TABLE 6 Test results of different images.

Images	NPCR (%)	UACI (%)
Kid	99.6012	33.4311
Girl	99.6114	33.4821
Boy	99.6241	33.4636
Average	99.6122	33.4589

TABLE 7 Comparison with other encryption schemes.

Process	Proposed	[46]	[47]	[48]
Key space	2^{471}	2^{326}	2^{448}	2^{128}
NPCR (%)	99.6122	99.6025	99.60	99.5650
UACI (%)	33.4589	33.4612	33.42	33.4675
Entropy	7.9972	7.9993	7.9993	7.9971

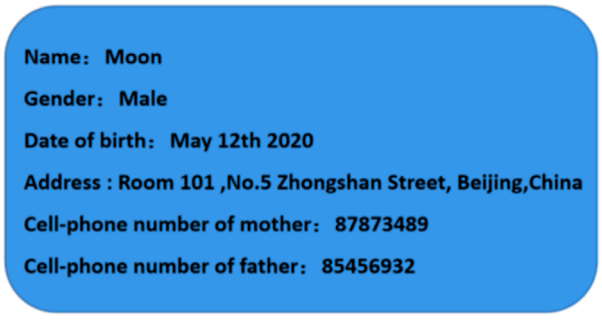

FIGURE 13
Lost children information.

through the cascading attention mechanism, and the robustness of cross-modal information has been improved using adversarial generative networks [51, 52]. These techniques are better able to print child-protective cipher information on clothing in the future.

The existing solutions mainly conduct anti-edge curling and noise tests for image encryption on carriers such as clothing and schoolbags. However, in practical applications, children's information may be printed on more complex carriers (such as clothes with rough fabric textures and easily worn plastic labels). In the future, the decryption effect of encrypted images under extreme physical conditions (such as high temperature, water stains, and tensile deformation) can be further tested, and combined with image restoration algorithms (such as damaged area completion based on deep learning), the adaptability of the scheme to diverse carriers and environments can be enhanced.

6.2 Conclusion

An image encryption scheme is proposed in this paper for the protection and verification of missing children's information. First, the dynamical behavior of the hyperchaotic mapping used in the design of the encryption scheme is analyzed, and the analysis results prove that the hyperchaotic mapping is suitable for image-encryption design. Then, the pseudo-random sequences are used to swap the missing child image information with random length random positions, divided into row swap and column swap. Next, a selective XOR is used between the image sequence and the pseudo-random sequences. Finally, the effectiveness of the encryption scheme is verified by simulation. Considering that the missing child's information should be decrypted by a specific person, the security of the encryption scheme should also be guaranteed. The sensitivity to the key and the large key space guarantee the resistance of the encryption scheme to exhaustive attacks. Comparing the statistical characteristics of the data between the cipher images and the original images, the pixel-level distribution status of the original images, the correlation between the adjacent pixels, and the amount of information contained in the image are hidden or broken. Considering that children's clothes will have curled edges in the process of use, the image encryption scheme is tested against curled edges. The test results show that even if the missing child information has a certain degree of curled edges,

FIGURE 14
Encrypted image (represented by the blue labels) integrated into different areas of the garment.

it can be recovered. In summary, this scheme provides technical support for the protection and verification of missing children's information.

Moreover, this technique can be applied to prevent the missing of children. For example, the detailed information of children, along with those of their parents (Figure 13), can be encoded. The encrypted image will be attached to the clothes (Figure 14). In instances where children go missing, law enforcement agencies can employ specialized readers to decrypt the encrypted information, thereby facilitating accurate and expeditious contact with designated guardians. Moreover, the amalgamation of image encryption significantly amplifies the computational complexity faced by malicious entities attempting to breach the encryption, effectively impeding easy access to children's information and mitigating concerns regarding privacy breaches. It can enhance the probability of successfully locating missing children.

Data availability statement

The data used in this study is available from the corresponding author upon reasonable request.

Ethics statement

Written informed consent was obtained from the minor(s)' legal guardian/next of kin for the publication of any potentially identifiable images or data included in this article.

Author contributions

CT: Conceptualization, Methodology, Software, Writing – original draft. LN: Funding acquisition, Supervision, Writing – review and editing. RC: Validation, Formal analysis, Writing – review and editing.

Funding

The author(s) declare that financial support was received for the research and/or publication of this article. The research was supported by the Scientific Research Project of Dalian Polytechnic University (KJ20250095) and the Liaoning Provincial Department of Education Scientific Research Project (JYTMS20230410).

Conflict of interest

The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Generative AI statement

The author(s) declare that no Generative AI was used in the creation of this manuscript.

Publisher's note

References

1. Cao Y, Tan L, Xu X, Li B. A universal image compression sensing–encryption algorithm based on DNA-triploid mutation. *Mathematics* (2024) 12(13):1990. doi:10.3390/math12131990

2. Tan L, Cao Y, Banerjee S, Mou J. Multi-medical image protection: compression-encryption scheme based on TLNN and mask cubes. *J Supercomputing* (2025) 81(1):96. doi:10.1007/s11227-024-06624-6

3. Liu Z, Li P, Cao Y, Mou J. A novel multimodal joint information encryption scheme based on multi-level confusion and hyperchaotic map. *Int J Mod Phys C* (2025). doi:10.1142/S012918312550038X

4. Zhang Z, Cao Y, Zhou N, Xu X, Mou J. Novel discrete initial-boosted tabu learning neuron: dynamical analysis, DSP implementation, and batch medical image encryption. *Appl Intelligence* (2025) 55(1):61. doi:10.1007/s10489-024-05918-9

5. Chu R, Zhang S, Gao X. A novel 3D image encryption based on the chaotic system and RNA crossover and mutation. *Front Phys* (2022) 10:1–14. doi:10.3389/fphy.2022.844966

6. Bi X, Shuai C, Liu B, Xiao B, Li W, Gao X. Privacy-preserving color image feature extraction by quaternion discrete orthogonal moments. *IEEE Trans Inf Forensics Security* (2022) 17:1655–68. doi:10.1109/tifs.2022.3170268

7. Mou J, Zhang Z, Banerjee S, Zhang Y. Combining Semi-tensor product compressed sensing and session keys for low-cost encryption of batch information in WBANs. *IEEE Internet Things J* (2024) 11(20):33565–76. doi:10.1109/jiot.2024.3429349

8. Yuan S, Chen D, Liu X, Zhou X. Optical encryption based on biometrics and single-pixel imaging with random orthogonal modulation. *Opt Commun* (2022) 522:128643. doi:10.1016/j.optcom.2022.128643

9. Mou J, Tan L, Cao Y, Zhou N, Zhang Y. Multi-face image compression encryption scheme combining extraction with STP-CS for face database. *IEEE Internet Things J* (2025) 12:19522–31. doi:10.1109/JIOT.2025.3541228

10. Liang W, Yang Y, Yang C, Hu Y, Xie S, Li KC, et al. PDPChain: a consortium blockchain-based privacy protection scheme for personal data. *IEEE Trans Reliability* (2022) 72(2):586–98. doi:10.1109/tr.2022.3190932

11. Liu Y, Hao X, Ren W, Xiong R, Zhu T, Choo KKR, et al. A blockchain-based decentralized, fair and authenticated information sharing scheme in zero trust internet-of-things. *IEEE Trans Comput* (2022) 72(2):501–12. doi:10.1109/tc.2022.3157996

12. Cai C, Cao Y, Mou J, Banerjee S, Sun B. A versatile image encryption scheme based on optical hologram technology and chess rules. *Int J Bifurcation Chaos* (2024) 34(15):2450185. doi:10.1142/s0218127424501852

13. Zhang Z, Mou J, Zhou N, Banerjee S, Cao Y. Multi-cube encryption scheme for multi-type images based on modified klotski game and hyperchaotic map. *Nonlinear Dyn* (2024) 112(7):5727–47. doi:10.1007/s11071-024-09292-6

14. Han Z, Cao Y, Banerjee S, Mou J. Hybrid image encryption scheme based on hyperchaotic map with spherical attractors. 34(3), 030503 (2025).

15. Yu F, He S, Yao W, Cai S, Xu Q. Bursting firings in memristive hopffeld neural network with image encryption and hardware implementation. *IEEE Trans Computer-Aided Des Integrated Circuits Syst* (2025) 1. doi:10.1109/tcad.2025.3567878

16. Yang F, An X, xiong L. A new discrete chaotic map application in image encryption algorithm. *Physica Scripta* (2022) 97(3):035202. doi:10.1088/1402-4896/ac4fd0

17. Ma T, Mou J, Yan H, Cao Y. A new class of hopfield neural network with double memristive synapses and its DSP implementation. *The Eur Phys J Plus* (2022) 137(10):1135. doi:10.1140/epjp/s13360-022-03353-8

18. Yu F, Su D, He S, Wu 吴 Y亦, Zhang 张 S善, Yin 尹 H挥. Resonant tunneling diode cellular neural network with memristor coupling and its application in police forensic digital image protection. *Chin Phys B* (2025) 34(5):050502. doi:10.1088/1674-1056/adb8bb

19. Ma Y, Mou J, Jahanshahi H, Abdulhameed A, Bi X. Design and DSP implementation of a hyperchaotic map with infinite coexisting attractors and intermittent chaos based on a novel locally active memcapacitor. *Chaos, Solitons and Fractals* (2023) 173:113708. doi:10.1016/j.chaos.2023.113708

20. Ma T, Mou J, Banerjee S, Cao H. Analysis of the functional behavior of fractional-order discrete neuron under electromagnetic radiation. *Chaos, Solitons and Fractals* (2023) 176:114113. doi:10.1016/j.chaos.2023.114113

21. Chen Y, Cao Y, Mou J, Sun B, Banerjee S. A simple photosensitive circuit based on a mutator for emulating memristor, memcapacitor, and meminductor: light illumination effects on dynamical behaviors. *Int J Bifurcation Chaos* (2024) 34(6):2450069. doi:10.1142/s021812742450069x

22. Wang X, Xu X, Sun K, Jiang Z, Li M, Wen J. A color image encryption and hiding algorithm based on hyperchaotic system and discrete cosine transform. *Nonlinear Dyn* (2023) 111(15):14513–36. doi:10.1007/s11071-023-08538-z

23. Toktas F, Erkan U, Yetgin Z. Cross-channel color image encryption through 2D hyperchaotic hybrid map of optimization test functions. *Expert Syst Appl* (2024) 249:123583. doi:10.1016/j.eswa.2024.123583

24. Gao X, Mou J, Banerjee S, Cao Y, Xiong L, Chen X. An effective multiple-image encryption algorithm based on 3D cube and hyperchaotic map. *J King Saud Univ - Computer Inf Sci* (2022) 34(4):1535–51. doi:10.1016/j.jksuci.2022.01.017

25. Wang X, Mou J, Cao Y, Jahanshahi H. Modeling and analysis of cellular neural networks based on memcapacitor. *Int J Bifurcation Chaos* (2025) 35. doi:10.1142/S0218127425300101

26. Jun M, Cao H, Zhou N, Cao Y. An FHN-HR neuron network coupled with a novel locally active memristor and its DSP implementation. *IEEE Trans Cybernetics* (2024) 54(12):7333–42. doi:10.1109/TCYB.2024.3471644

27. Jun M, Zhang Z, Zhou N, Zhang Y, Cao Y. Mosaic tracking: lightweight batch video frame awareness multi-target encryption scheme based on a novel discrete tabu learning neuron and YoloV5. *IEEE Internet Things J* (2024). doi:10.1109/JIOT.2024.3482289

28. Cao H, Cao Y, Lei Q, Mou J (2025). Dynamical analysis, multi-cavity control and DSP implementation of a novel memristive autapse neuron model emulating brain behaviors. *Chaos, Solitons and Fractals*, 191, 115857. doi:10.1016/j.chaos.2024.115857

29. Shi F, Cao Y, Xu X, Mou J. A novel memristor-coupled discrete neural network with multi-stability and multiple state transitions. *The Eur Phys J Spec Top* (2025). doi:10.1140/epjs/s11734-024-01440-8

30. Yu F, Wu C, Xu S, Yao W, Xu C, Cai S, et al. Color video encryption transmission in IoT based on memristive hopfield neural network. *Signal Image Video Process.* (2025) 19(77):77. doi:10.1007/s11760-024-03697-x

31. Gan Z, Chai X, Bi J, Chen X. Content-adaptive image compression and encryption *via* optimized compressive sensing with double random phase encoding driven by chaos. *Complex & Intell Syst* (2022) 8:2291–309. doi:10.1007/s40747-022-00644-6

32. Abuturab MR, Alfalou A. Multiple color image fusion, compression, and encryption using compressive sensing, chaotic-biometric keys, and optical fractional fourier transform. *Opt & Laser Technology* (2022) 151:108071. doi:10.1016/j.optlastec.2022.108071

33. Wang X, Liu C, Jiang D. A novel triple-image encryption and hiding algorithm based on chaos, compressive sensing and 3D DCT. *Inf Sci* (2021) 574:505–27. doi:10.1016/j.ins.2021.06.032

34. Zhang J, Yang D, Ma R, Shi Y. Multi-image and color image encryption *via* multi-slice ptychographic encoding. *Opt Commun* (2021) 485:126762. doi:10.1016/j.optcom.2021.126762

35. Yan X, Wang X, Xian Y. Chaotic image encryption algorithm based on arithmetic sequence scrambling model and DNA encoding operation. *Multimedia Tools Appl* (2021) 80(7):10949–83. doi:10.1007/s11042-020-10218-8

36. Wang X, Su Y. Image encryption based on compressed sensing and DNA encoding. *Signal Processing: Image Commun* (2021) 95:116246. doi:10.1016/j.image.2021.116246

37. Ghanbari-Ghalehjoughi H, Eslami M, Ahmadi-Kandjani S, Ghanbari-Ghalehjoughi M, Yu Z. Multiple layer encryption and steganography *via* multi-channel ghost imaging. *Opt Lasers Eng* (2020) 134:106227. doi:10.1016/j.optlaseng.2020.106227

38. Yang Y-G, Wang B-P, Yang Y-L, Zhou Y-H, Shi W-M, Liao X. Visually meaningful image encryption based on universal embedding model. *Inf Sci* (2021) 562:304–24. doi:10.1016/j.ins.2021.01.041

39. Hua Z, Zhang K, Li Y, Zhou Y. Visually secure image encryption using adaptive-thresholding sparsification and parallel compressive sensing. *Signal Process.* (2021) 183:107998. doi:10.1016/j.sigpro.2021.107998

40. Zhu S, Deng X, Zhang W, Zhu C. Image encryption scheme based on newly designed chaotic map and parallel DNA coding. *Mathematics* (2023) 11(1):231. doi:10.3390/math11010231

41. Zhu S, Deng X, Zhang W, Zhu C. Secure image encryption scheme based on a new robust chaotic map and strong S-box. *Mathematics Comput Simulation* (2023) 207:322–46. doi:10.1016/j.matcom.2022.12.025

42. Wu Y, Zhou Y, Saveriades G, Agaian S, Noonan JP, Natarajan P. Local shannon entropy measure with statistical tests for image randomness. *Inf Sci* (2013) 222:323–42. doi:10.1016/j.ins.2012.07.049

43. Kaur G, Agarwal R, Patidar V. Color image encryption system using combination of robust chaos and chaotic order fractional hartley transformation. *J King Saud Univ - Computer Inf Sci* (2021) 34:5883–97. doi:10.1016/j.jksuci.2021.03.007

44. Lu Q, Yu L, Zhu C. Symmetric image encryption algorithm based on a new product trigonometric chaotic map. *Symmetry* (2022) 14(2):373. doi:10.3390/sym14020373

45. Kaur G, Agarwal R, Patidar V. Color image encryption scheme based on fractional hartley transform and chaotic substitution–permutation. *The Vis Computer* (2021) 38(3):1027–50. doi:10.1007/s00371-021-02066-w

46. Li S-Y, Gai Y, Shih K-C, Chen C-S. An efficient image encryption algorithm based on innovative DES structure and hyperchaotic keys. *IEEE Trans Circuits Syst Regular Pap* (2023) 70(10):4103–11. doi:10.1109/tcsi.2023.3296693

47. Zhou S, Wang X, Zhang Y. Novel image encryption scheme based on chaotic signals with finite-precision error. *Inf Sci* (2023) 621:782–98. doi:10.1016/j.ins.2022.11.104

48. Yi G, Cao Z. An algorithm of image encryption based on AES & rossler hyperchaotic modeling. *Mobile Networks Appl* (2023) 29:1451–9. doi:10.1007/s11036-023-02216-5

49. Wu Z, Sun C, Xuan H, Yan Y. Deep stereo video inpainting. In: *Proceedings of the IEEE/CVF conference on computer vision and pattern recognition* (2023). p. 5693–702.

50. Wu Z, Sun C, Xuan H, Liu G, Yan Y. WaveFormer: wavelet transformer for noise-robust video inpainting. *Proc AAAI Conf Artif Intelligence* (2024) 38(6):6180–8. doi:10.1609/aaai.v38i6.28435

51. Zhang W, Li Z, Li G, Zhuang P, Hou G, Zhang Q, et al. GACNet: generate adversarial-driven cross-aware network for hyperspectral wheat variety identification. *IEEE Trans Geosci Remote Sensing* (2023) 62:1–14. doi:10.1109/tgrs.2023.3347745

52. Gao X, Sun B, Cao Y, Banerjee S, Mou J. A color image encryption algorithm based on hyperchaotic map and DNA mutation. *Chin Phys B* (2023) 32(3):030501. doi:10.1088/1674-1056/ac8cdf