基于变参数超混沌系统的多图像加密方法

罗 敏，何雨莲，李宜磊，张怀武，文岐业*

(电子科技大学电子科学与工程学院 成都 611731)

【摘要】针对数字图像计算、存储和传输过程中的数据窃取、隐私泄漏等问题，提出了一种基于变参数超混沌系统的多图像加密方法。首先，用一个混沌系统的状态变量对另一个混沌系统的状态参数施加扰动，构造了一个变参数超混沌系统；其次，将输入灰度图像对进行重构，并将其输入 SHA-512 算法生成初始密钥；然后，将初始密钥输入变参数超混沌系统，迭代生成 5 组混沌序列，进而对重构图像进行幻方变换，实现像素位置的变换；最后，对幻方变换得到的图像进行 S 形扩散，实现像素数值的变化，得到了近似均匀分布的密文图像。结果表明，该算法改善了传统图像加密方法的低随机性、低复杂度等缺陷，同时，提高了密文图像的无序性及抵抗常规攻击的能力。

关 键 词 超混沌系统； 图像加密； 幻方变换； S 形扩散

中图分类号 TP309.7 **文献标志码** A doi:10.12178/1001-0548.2022407

Multi-Image Encryption Method Based on Hyperchaotic System with Variable Parameters

LUO Min, HE Yulian, LI Yilei, ZHANG Huaiwu, and WEN Qiye*

(School of Electronic Science and Engineering, University of Electronic Science and Technology of China Chengdu 611731)

Abstract Aiming at the problems of data theft and privacy leakage in the process of digital image calculation, storage and transmission, a multi-image encryption method based on hyperchaotic system with variable parameters is proposed. Firstly, the state variables of one chaotic system are used to perturb the state parameters of the other chaotic system, and a hyperchaotic system with variable parameters is constructed. Secondly, the input gray image pair is reconstructed and input into SHA-512 algorithm to generate the initial key. Then, the initial key is input into the hyperchaotic system with variable parameters to generate five groups of chaotic sequences iteratively, and then the reconstructed image is transformed into a magic square to achieve the transformation of pixel positions. Finally, the S-shaped diffusion is performed on the image obtained by the magic square transformation to realize the change of the pixel value, and an approximately uniformly distributed ciphertext image is obtained. The results show that the algorithm improves the low randomness and low complexity of the traditional image encryption method, and at the same time, and improves the disorder of the ciphertext image and the ability of the encryption method to resist conventional attacks.

Key words hyperchaotic system; image encryption; magic square transformation; S-shaped diffusion

随着数字通信技术的飞速发展，数字图像以其易于获取、处理和存储的优势，成为人们传递信息和感知世界的重要方式，广泛应用于工业、医药、军事、航天等各个领域。与此同时，伴随而来的则是严重的安全隐患，包括未经授权地传播、复制、篡改及伪造等。因此，如何保护数字图像内容的安全成了亟待解决的问题。

目前图像加密主要采用基于混沌系统的图像加密技术[1-4]，简称混沌图像加密方法，主要包括图像置乱[5-7]与图像扩散[8-10]两种方法。图像置乱方法通过改变图像像素的位置来改变原始图像，使得肉眼无法直观地辨认明文图像，以此达到图像加密的目的。置乱方法主要包括 Arnold 变换[11]、Baker 变换[12]与幻方变换[13]这 3 种。图像扩散方法对图像中的像素及其相邻像素进行异或操作，再用变换后的像素替换原始像素，即打乱原始图像的像素值，以此达

收稿日期：2022－12－05；修回日期：2023－04－19
基金项目：国家自然科学基金 (62235004, 61831012)；国防科工局科学挑战计划 (TZ2018003)；科技部国际合作交流专项 (2015DFR50870)；四川省科技支撑计划 (2021JDTD0026, 2021YFG0144)；
作者简介：罗敏 (1989－)，男，高级工程师，主要从事人工智能、图像处理和太赫兹技术方面的研究.
*通信作者：文岐业，E-mail：qywen@uestc.edu.cn

到图像加密的目的。混沌系统用于对置乱和扩散提供索引矩阵，常用的混沌系统有 Logistic 混沌映射[14]、Chebychev 映射[15]、Lorenz 混沌系统[16-17]、Chen 混沌系统[18] 等。

与传统图像加密方法相比，混沌图像加密方法具有密钥空间大、加密速度快等优点。然而，当前混沌图像加密方法依然存在诸多问题亟待解决。具体为：1）普遍采用低维及参数固定的混沌系统，所设计的密钥系统的密钥空间不够大、复杂度较低，在计算机有限精度下，容易出现短周期现象及混沌退化，容易受到攻击者使用相空间重构方法进行的攻击破译；2）仅采用简单的像素置乱及像素扩散方法，如基于位置变换的置乱方法、基于异或运算的扩散方法，它们的复杂度较低、易于破译，即仅仅对图像进行简单的像素位置和大小上的变换；3）每一幅图像都使用相同的密钥流，安全性较差，攻击者只要破译一幅图像就可以对其他密文图像进行破译，未有效地将密钥与明文图像进行联系。

1 算法设计

为了解决图像加密方法的上述问题，提供了一种基于变参数超混沌系统与 S 形扩散的多图像加密方法，如图 1 所示。首先借助 Alpha 通道的概念，将输入灰度图像（原始图像）进行重构，然后将其作为初始信息输入 SHA-512 算法生成初始密钥，再利用变参数超混沌系统迭代生成的 5 组混沌序列对明文图像进行幻方变换，实现像素位置的变换，最后基于 S 形扩散实现像素数值的变换，从而得到密文图像。具体技术方案包括以下 3 个步骤。

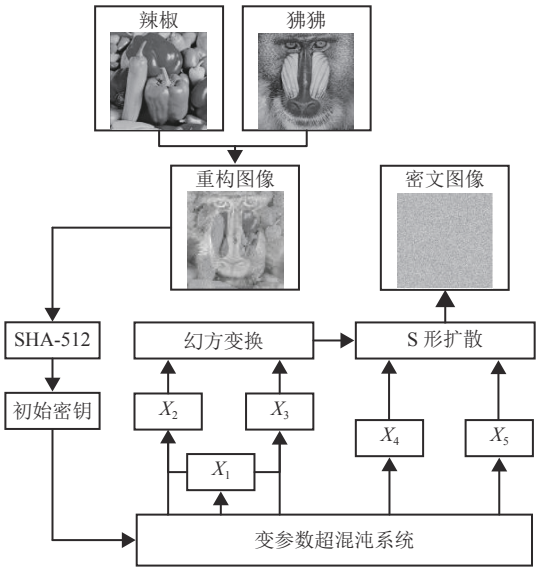


图 1 多图像加密方法的设计框架

1）首先对输入灰度图像对进行图像预处理，得到重构 GA 图像 P，并将其像素序列作为初始信息输入 SHA-512 哈希函数生成初始密钥流；

2）再将初始密钥流作为初始值，输入变参数超混沌系统迭代生成混沌序列 X_1、X_2、X_3、X_4 与 X_5，并基于混沌序列 X_1、X_2、X_3 计算得到索引序列；再根据索引序列对重构 GA 图像 P 采用幻方变换进行置乱，得到置乱后的密文图像 C；

3）最后对密文图像 C 进行顺向 S 形扩散得到顺向扩散后矩阵，再对顺向扩散后矩阵进行逆向 S 形扩散，得到最终密文图像 T。

1.1 变参数超混沌系统

根据 Fan 超混沌系统的定义[19]，其数学模型如式 (1) 所示，其典型特征是：当 a=30、b=10、c=15.7、d=5、e=2.5、f=4.45、g=38.5 时，该混沌系统存在两个正的 Lyapunov 指数，即存在复杂的混沌行为。

$$\begin{cases} \dot{x}_1 = a(x_2 - x_1) + x_2x_3x_4 \\ \dot{x}_2 = b(x_1 + x_2) + x_5 - x_1x_3x_4 \\ \dot{x}_3 = -cx_2 - dx_3 - ex_4 + x_1x_2x_4 \\ \dot{x}_4 = -fx_4 + x_1x_2x_3 \\ \dot{x}_5 = -g(x_1 + x_2) \end{cases} \tag{1}$$

式中，x_1、x_2、x_3、x_4、x_5 为系统变量；a、b、c、d、e、f、g 为系统参数；$\dot{x}_1$、$\dot{x}_2$、$\dot{x}_3$、$\dot{x}_4$、$\dot{x}_5$为每次迭代产生的新系统变量（Lyapunov 指数）。

为了增强混沌系统的复杂性和随机性，采用 Logistic 混沌映射作为扰动系统，对 Fan 超混沌系统的参数施加扰动来构造变参数混沌系统，以生成具有更高随机性的混沌序列，Logistic 映射为非线性的迭代方程，如式 (2) 所示，其典型特征是：当满足 3.57<μ<4 时，Logistic 映射工作于混沌状态，即为 Logistic 混沌映射。

$$\dot{y} = \mu y(1 - y) \tag{2}$$

式中，y 为系统变量；μ为系统参数；$\dot{y}$为每次迭代产生的新系统变量。

引入参数扰动项后的变参数超混沌系统的数学模型如式 (3) 所示，根据混沌系统的定义，无论初始值如何变化，系统变量都会回到一个固定的吸引域，由于式 (1)、(2) 均为混沌系统方程，因此 Lyapunov 指数的数值经过式 (3) 多次迭代后，只跟扰动强度 λ 有关，与 y、x_i (i=1,2,⋯,5) 的初始值无关，y、x_i 的初始值可取实数范围内的任意值，最终稳定的 Lyapunov 指数的数值只依赖于扰动强

度 λ。

$$\begin{cases} \dot{x}_1 = (a+\lambda y)(x_2 - x_1) + x_2 x_3 x_4 \\ \dot{x}_2 = (b+\lambda y)(x_1 + x_2) + x_5 - x_1 x_3 x_4 \\ \dot{x}_3 = -(c+\lambda y)x_2 - d x_3 - e x_4 + x_1 x_2 x_4 \\ \dot{x}_4 = -(f+\lambda y)x_4 + x_1 x_2 x_3 \\ \dot{x}_5 = -(g+\lambda y)(x_1 + x_2) \end{cases} \tag{3}$$

式中，x_1、x_2、x_3、x_4、x_5 为系统变量；a、b、c、d、e、f、g 为系统参数；$\dot{x}_1$、$\dot{x}_2$、$\dot{x}_3$、$\dot{x}_4$、$\dot{x}_5$为每次迭代产生的新系统变量；λ 为扰动强度参数；y 为 Logistic 混沌映射的系统参数。

为了确定扰动强度参数 λ 的取值范围，确保变参数超混沌系统始终处于混沌状态，对变参数超混沌系统的 Lyapunov 指数和系统相图进行仿真分析，在系统参数 a=30、b=10、c=15.7、d=5、e=2.5、f=4.45、g=38.5、μ=3.8 时，取 y=1、x_i=0.1 作为初始值，当变参数超混沌系统自身迭代 300 次后，Lyapunov 指数的数值趋于稳定，将第 301 次迭代产生的 y、x_i 以及系统参数代入式 (3)，得到了变参数超混沌系统（λ 在−5～4 之间变化）的 Lyapunov 指数变化曲线，如图 2 所示。当扰动强度参数 λ 在 −4.0～2.35 之间时，$x_1(\lambda)$ 和 $x_2(\lambda)$ 始终大于零，即始终存在两个正的 Lyapunov 指数，使变参数超混沌系统保持混沌状态。图 3 给出了扰动强度参数 λ 为 0 时，变参数超混沌系统的系统相图，通过系统相图能够更直观地表现出变参数超混沌系统的动力学行为。

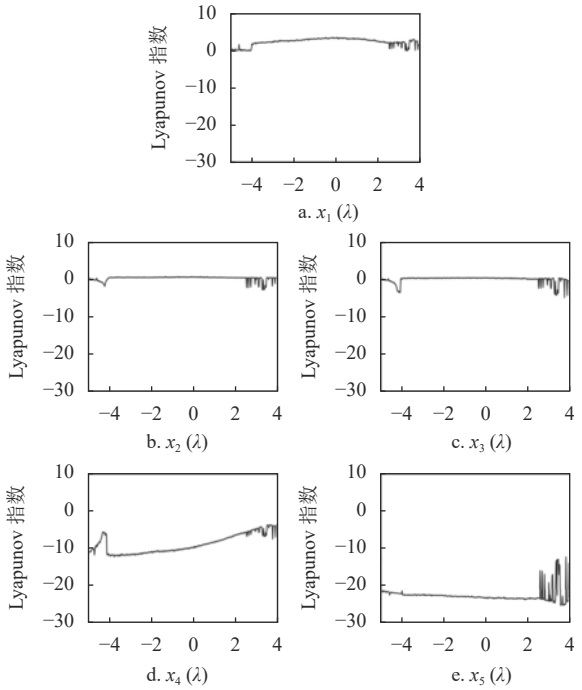


图 2　变参数超混沌系统的 Lyapunov 指数变化曲线

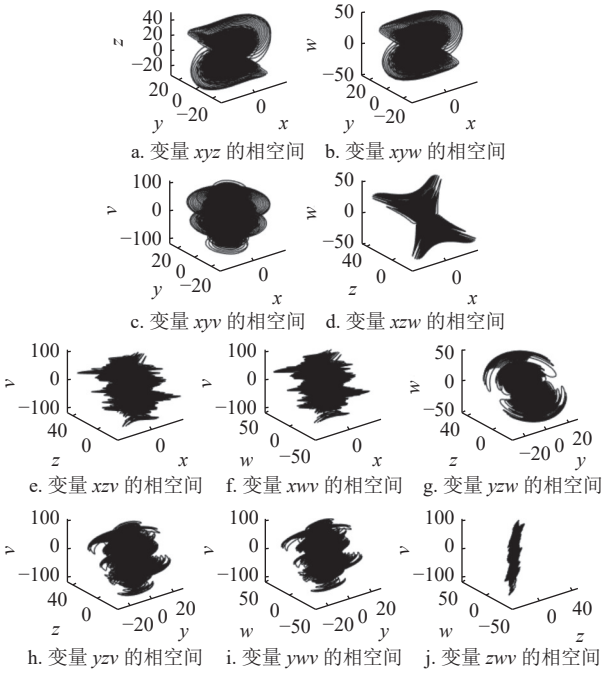


图 3　变参数超混沌系统的系统相图

1.2　多图像加密方法

多图像加密方法的流程图如图 4 所示，包括图像预处理与密钥生成、置乱阶段和扩散阶段 3 个步骤。以下使用如图 5 所示的传统图像辣椒（灰度图像 P_0）与狒狒（灰度图像 P_1）为例进行说明，两张图像的像素大小均为 512×512，记为 M×N，M 为图像像素长度、N 为图像像素宽度。

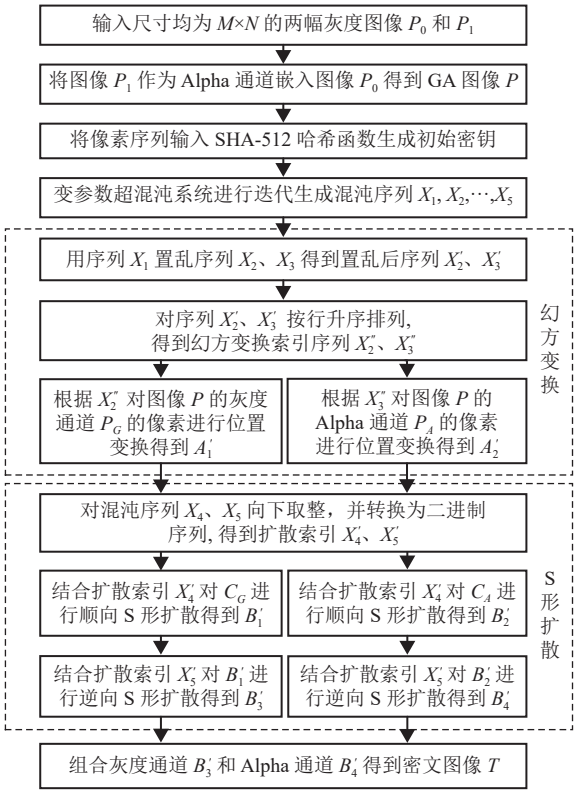


图 4　多图像加密方法的流程图

a. 辣椒 b. 狒狒

图 5 原始图像

1.2.1 图像预处理及密钥生成

1）引入 Alpha 通道的概念，将灰度图像 P_1 作为 Alpha 通道嵌入至灰度图像 P_0，进而形成一幅具有不同透明度的 Grayscale-Alpha(GA) 图像 P；

2）将图像 P 分解为灰度通道 P_G 与 Alpha 通道 P_A 两路数据矩阵（矩阵大小均为 $M\times N$），再将灰度通道 P_G 与 Alpha 通道 P_A 转换为一维矩阵，并拼接构成一维矩阵 P_C，将一维矩阵 P_C 作为初始信息，输入 SHA-512 哈希函数，生成 512 bit 的二进制哈希值，具体运算为：

$$P_C=[\text{reshape}(P_G,M\times N,1),\text{reshape}(P_A,M\times N,1)] \quad (4)$$

式中，reshape( ) 表示将指定矩阵变换为特定行列数的矩阵。

3）将二进制的哈希值以每 8 bit 为一位转化为十进制，进而得到 64 位十进制数据 $c_i(i=1,2,\cdots,64)$；

4）对 64 位十进制数据进行异或运算得到加密方法所需要的初始密钥流，具体运算为：

$$\begin{cases}\hat{x}_1=\dfrac{c_1\oplus c_2\oplus c_3\oplus\cdots\oplus c_{10}}{256}\\ \hat{x}_2=\dfrac{c_{11}\oplus c_{12}\oplus c_{13}\oplus\cdots\oplus c_{20}}{256}\\ \hat{x}_3=\dfrac{c_{21}\oplus c_{22}\oplus c_{23}\oplus\cdots\oplus c_{30}}{256}\\ \hat{x}_4=\dfrac{c_{31}\oplus c_{32}\oplus c_{32}\oplus\cdots\oplus c_{40}}{256}\\ \hat{x}_5=\dfrac{c_{41}\oplus c_{42}\oplus c_{43}\oplus\cdots\oplus c_{50}}{256}\\ \lambda=\text{mod}\left(\dfrac{c_{51}\oplus c_{52}\oplus c_{53}\oplus\cdots\oplus c_{64}}{256},6.35\right)-4\end{cases} \quad (5)$$

式中，$\hat{x}_1$、$\hat{x}_2$、$\hat{x}_3$、$\hat{x}_4$、$\hat{x}_5$为初始密钥；⊕表示异或操作；mod( ) 表示取余运算；

需要说明的是：式 (5) 中 λ 的归一化过程能够保证其取值在−4.0～2.35 之间，进而保证变参数混沌系统保持混沌状态。

1.2.2 置乱阶段

1）根据初始密钥流，应用四阶龙格库塔算法对变参数超混沌系统进行迭代，为避免暂态效应的影响，舍弃前 500 组数据，从第 501 个数据进行截取，最终得到 5 组一维混沌序列 X_1、X_2、X_3、X_4 与 X_5，其中，每组混沌序列的长度均为 $M\times N$；

2）将混沌序列 X_1 按行升序排列，得到置乱后矩阵 $\boldsymbol{I}_1$ 与索引序列X_1'，具体运算为：

$$\left[\boldsymbol{I}_1,X_1'\right]=\text{sort}(X_1,2,\text{ascend}) \quad (6)$$

式中，sort( ) 表示排序函数；‘2’表示按行排序；ascend表示升序排列；

3）根据混沌索引序列X_1'，对混沌序列 X_2、X_3 分别进行位置上的置乱，即根据混沌序列所对应索引序列相应位置的数值，将序列记录的数据移动到索引序列指定的位置，置乱示意图如图 6 所示；再对置乱后的混沌序列X_2'、X_3'按行升序排列，得到置乱后矩阵 $\boldsymbol{I}_2$、$\boldsymbol{I}_3$ 与幻方变换所需的索引序列X_2''、X_3''，具体运算为：

$$\begin{cases}\left[\boldsymbol{I}_2,X_2''\right]=\text{sort}\left(X_2',2,\text{ascend}\right)\\ \left[\boldsymbol{I}_3,X_3''\right]=\text{sort}\left(X_3',2,\text{ascend}\right)\end{cases} \quad (7)$$

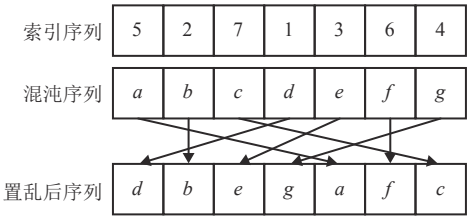


图 6 混沌序列置乱示意图

4）根据索引序列X_2''、X_3''，分别对图像 P 的灰度通道 P_G 与 Alpha 通道 P_A 采用幻方变换进行置乱，对应得到置乱后的二维矩阵$\boldsymbol{A}_1'$、$\boldsymbol{A}_2'$，具体置乱过程如图 7 所示。以灰度通道 P_G 为例，首先将灰度通道 P_G（二维矩阵）变换为一维序列P_G'，再根据索引序列X_2''将序列P_G'中的像素移动到相应位置得到置乱后的一维序列 A_1，最后将置乱后的一维序列 A_1 变换为置乱后的二维矩阵A_1'，矩阵变换运算为：

$$\begin{cases}P_G'=\text{reshapd}(P_G,M\times N,1)\\ A_1'=\text{reshapd}(A_1,1,M\times N)\end{cases} \quad (8)$$

式中，reshape( ) 表示将指定矩阵变换为特定行列数的矩阵。

5）将置乱后矩阵$\boldsymbol{A}_1'$作为灰度通道，置乱后矩阵$\boldsymbol{A}_2'$作为 Alpha 通道，组合得到置乱后的密文图像 C。

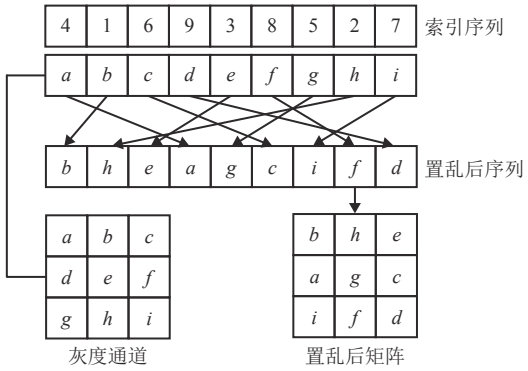


图 7　幻方变换示意图

1.2.3　扩散阶段

1）将混沌序列 X_4 与 X_5 进行向下取整数运算，得到十进制整数的混沌序列，然后将十进制转换为二进制的一维序列X_4'与X_5'（长度均为 $M\times 8N$）：

$$\begin{cases} X_4' = \text{dec2bin}(\text{floor}(X_4)) \\ X_5' = \text{dec2bin}(\text{floor}(X_5)) \end{cases} \tag{9}$$

式中，dec2bin( ) 表示将十进制转换为二进制；floor( ) 为向下取整函数。

2）将密文图像 C 分解为灰度通道 C_G 和 Alpha 通道 C_A 两路数据矩阵（矩阵大小均为 $M\times N$），先对灰度通道 C_G 和 Alpha 通道 C_A 分别进行顺向 S 形扩散，再进行十进制到二进制的转换，得到二进制的一维矩阵C_G'与c_A'（长度均为 $M\times 8N$）；然后根据式 (10) 进行异或运算，得到二进制的一维矩阵 B_1 与 B_2（长度均为 $M\times 8N$），将二进制矩阵 B_1 与 B_2 转换为十进制矩阵，并将一维变换为二维，得到顺向扩散后矩阵B_1'与B_2'（矩阵大小均为 $M\times N$）：

$$\begin{cases} B_1(1) = \text{floor}\left(\text{mod}\left(\sum_{j=1}^{M\times N} X_4(j), 2\right)\right) \oplus C_G'(1) \oplus X_4'(1) \\ B_1(i) = C_G'(i-1) \oplus C_G'(i) \oplus X_4'(i) \quad i = 2,3,\cdots,M\times 8N \\ B_2(1) = \text{floor}\left(\text{mod}\left(\sum_{j=1}^{M\times N} X_4(j), 2\right)\right) \oplus C_A'(1) \oplus X_4'(1) \\ B_2(i) = C_A'(i-1) \oplus C_A'(i) \oplus X_4'(i) \quad i = 2,3,\cdots,M\times 8N \end{cases} \tag{10}$$

$$\begin{cases} B_1' = \text{reshape}(\text{bin2dec}(B_1), 1, M\times N) \\ B_2' = \text{reshape}(\text{bin2dec}(B_2), 1, M\times N) \end{cases} \tag{11}$$

式中，mod( ) 表示取余运算；M、N 为输入灰度图像的像素长度和像素宽度；bin2dec( ) 表示将二进制转换为十进制。

3）对矩阵B_1'与B_2'分别进行逆向 S 形扩散，再进行十进制到二进制的转换，得到二进制的一维矩阵B_1''与B_2''（长度均为 $M\times 8N$）；然后根据式 (12) 进行异或运算，得到二进制的一维矩阵 B_3 与 B_4（长度均为 $M\times 8N$），将二进制矩阵 B_3 与 B_4 转换为十进制矩阵，并将一维变换为二维，得到逆向扩散后矩阵B_3'与B_4'（矩阵大小均为 $M\times N$），具体运算如式 (13)所示；最后将二维矩阵B_4'作为 Alpha 通道嵌入二维矩阵B_3'中，得到最终密文图像 T。

$$\begin{cases} B_3(1) = \text{floor}\left(\text{mod}\left(\sum_{j=1}^{M\times N} X_5(j), 2\right)\right) \oplus B_1''(1) \oplus X_5'(1) \\ B_3(i) = B_1''(i-1) \oplus B_1''(i) \oplus X_5'(i) \quad i = 2,3,\cdots,M\times 8N \\ B_4(1) = \text{floor}\left(\text{mod}\left(\sum_{j=1}^{M\times N} X_5(j), 2\right)\right) \oplus B_2''(1) \oplus X_5'(1) \\ B_4(i) = B_2''(i-1) \oplus B_2''(i) \oplus X_5'(i) \quad i = 2,3,\cdots,M\times 8N \end{cases} \tag{12}$$

$$\begin{cases} B_3' = \text{reshape}(\text{bin2dec}(B_3), 1, M\times N) \\ B_4' = \text{reshape}(\text{bin2dec}(B_4), 1, M\times N) \end{cases} \tag{13}$$

顺向 S 形扩散的定义如图 8a 所示，具体运算为：

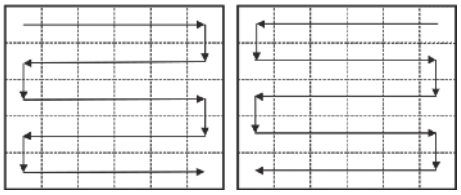
$$\begin{cases} Q' = S_{\text{forward}}(\boldsymbol{Q}) \\ \boldsymbol{Q} = \begin{bmatrix} q_{1,1} & q_{1,2} & \cdots & q_{1,N} \\ q_{2,1} & q_{2,2} & \cdots & q_{2,N} \\ \vdots & \vdots & & \vdots \\ q_{M,1} & q_{M,2} & \cdots & q_{M,N} \end{bmatrix} \\ Q' = [q_{1,1}, q_{1,2}, \cdots, q_{1,N}, q_{2,N}, q_{2,N-1}, \cdots, q_{2,1}, q_{3,1}, \\ \quad q_{3,2}, \cdots, q_{3,N}, q_{4,N}, \cdots] \end{cases} \tag{14}$$

式中，S_{forward}( ) 表示顺向 S 形扩散运算；$\boldsymbol{Q}$ 为原始矩阵；Q'为顺向 S 形扩散结果。

逆向 S 形扩散的定义如图 8b 所示，具体运算为：

$$\begin{cases} Q'' = S_{\text{reverse}}(\boldsymbol{Q}) \\ \boldsymbol{Q} = \begin{bmatrix} q_{1,1} & q_{1,2} & \cdots & q_{1,N} \\ q_{2,1} & q_{2,2} & \cdots & q_{2,N} \\ \vdots & \vdots & & \vdots \\ q_{M,1} & q_{M,2} & \cdots & q_{M,N} \end{bmatrix} \\ Q'' = [q_{1,N}, q_{1,N-1}, \cdots, q_{1,1}, q_{2,1}, q_{2,2}, \cdots, q_{2,N}, q_{3,N}, \\ \quad q_{3,N-1}, \cdots, q_{3,1}, q_{4,1}, \cdots] \end{cases} \tag{15}$$

式中，S_{reverse}( ) 表示逆向 S 形扩散运算；$\boldsymbol{Q}$ 为原始矩阵；Q''为逆向 S 形扩散结果。



a. 顺向 S 形扩散　　b. 逆向 S 形扩散

图 8　顺向和逆向 S 形扩散示意图

1.3 多图像解密方法

图像解密方法使用与加密方法相同的密钥，具体包括以下 3 个步骤。

1）将密文图像分解为两通道十进制数据矩阵，即灰度通道 $\boldsymbol{J}$ 与 Alpha 通道 $\boldsymbol{K}$（矩阵大小均为 $M\times N$），对 $\boldsymbol{J}$ 与 $\boldsymbol{K}$ 分别进行顺向 S 形扩散的逆操作，再进行十进制到二进制的转换，得到二进制的一维矩阵 $\boldsymbol{J}'$与$\boldsymbol{K}'$（长度均为 $M\times 8N$）；根据式 (16) 进行异或运算，得到二进制的一维矩阵 J_1 和 K_1（长度均为 $M\times 8N$），将二进制矩阵 $\boldsymbol{J}_1$ 和 $\boldsymbol{K}_1$ 转换为十进制矩阵，并将其变换为二维矩阵$\boldsymbol{J}_1'$与$\boldsymbol{K}_1'$（矩阵大小均为 $M\times N$），具体运算如式 (17) 所示：

$$\begin{cases} J_1(1)=\mathrm{floor}\left(\mathrm{mod}\left(\sum_{j=1}^{M\times N}X_4(j),2\right)\right)\oplus J'(1)\oplus X_4'(1) \\ J_1(i)=J'(i-1)\oplus J'(i)\oplus X_4'(i)\quad i=2,3,\cdots,M\times 8N \\ K_1(1)=\mathrm{floor}\left(\mathrm{mod}\left(\sum_{j=1}^{M\times N}X_4(j),2\right)\right)\oplus K'(1)\oplus X_4'(1) \\ K_1(i)=K'(i-1)\oplus K'(i)\oplus X_4'(i)\quad i=2,3,\cdots,M\times 8N \end{cases} \tag{16}$$

$$\begin{cases} \boldsymbol{J}_1'=\mathrm{reshape}(\mathrm{bin2dec}(J_1),1,M\times N) \\ \boldsymbol{K}_1'=\mathrm{reshape}(\mathrm{bin2dec}(K_1),1,M\times N) \end{cases} \tag{17}$$

2）对矩阵$\boldsymbol{J}_1'$与$\boldsymbol{K}_1'$分别进行逆向 S 形扩散的逆操作，再进行十进制到二进制的转换，得到二进制的一维矩阵$\boldsymbol{J}_1''$与$\boldsymbol{K}_1''$（长度均为 $M\times 8N$）；根据式 (18) 进行异或运算，得到二进制的一维矩阵 $\boldsymbol{J}_2$ 和 $\boldsymbol{K}_2$（长度均为 $M\times 8N$），将二进制矩阵 J_2 和 K_2 转换为十进制矩阵，并将其变换为二维矩阵$\boldsymbol{J}_2'$与$\boldsymbol{K}_2'$（矩阵大小均为 $M\times N$）：

$$\begin{cases} J_2(1)=\mathrm{floor}\left(\mathrm{mod}\left(\sum_{j=1}^{M\times N}X_5(j),2\right)\right)\oplus J_1''(1)\oplus X_5'(1) \\ J_2(i)=J_1''(i-1)\oplus J_1''(i)\oplus X_5'(i)\quad i=2,3,\cdots,M\times 8N \\ K_2(1)=\mathrm{floor}\left(\mathrm{mod}\left(\sum_{i=1}^{M\times N}X_5(j),2\right)\right)\oplus K_1''(1)\oplus X_s'(1) \\ K_2(i)=K_1''(i-1)\oplus K_1''(i)\oplus X_5'(i)\quad i=2,3,\cdots,M\times 8N \end{cases} \tag{18}$$

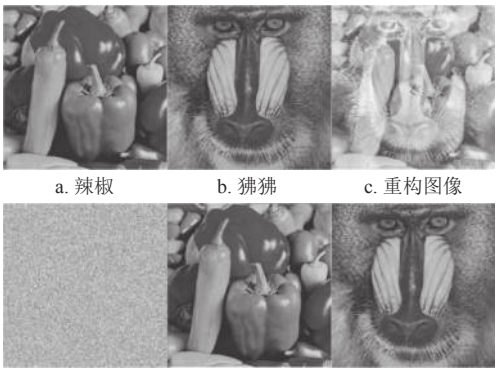
$$\begin{cases} \boldsymbol{J}_2'=\mathrm{reshape}(\mathrm{bin2dec}(\boldsymbol{J}_2),1,M\times N) \\ \boldsymbol{K}_2'=\mathrm{reshape}(\mathrm{bin2dec}(\boldsymbol{J}_2),1,M\times N) \end{cases} \tag{19}$$

3）对$\boldsymbol{J}_2'$与$\boldsymbol{K}_2'$进行逆幻方运算，得到十进制的二维矩阵 $\boldsymbol{J}_3$ 与 $\boldsymbol{K}_3$（矩阵大小均为 $M\times N$），矩阵 $\boldsymbol{J}_3$ 对应灰度通道，即为原始图像 P_0，矩阵 $\boldsymbol{K}_3$ 对应 Alpha 通道，即为原始图像 P_1。

2 实验结果与分析

2.1 加解密实验结果

通过上述多图像加解密方法，对如图 5 所示的传统图像辣椒与狒狒进行加解密实验，得到的仿真图如图 9 所示。由图可见，密文图像是完全无序的，无法分辨出原始图像的任何有效信息。



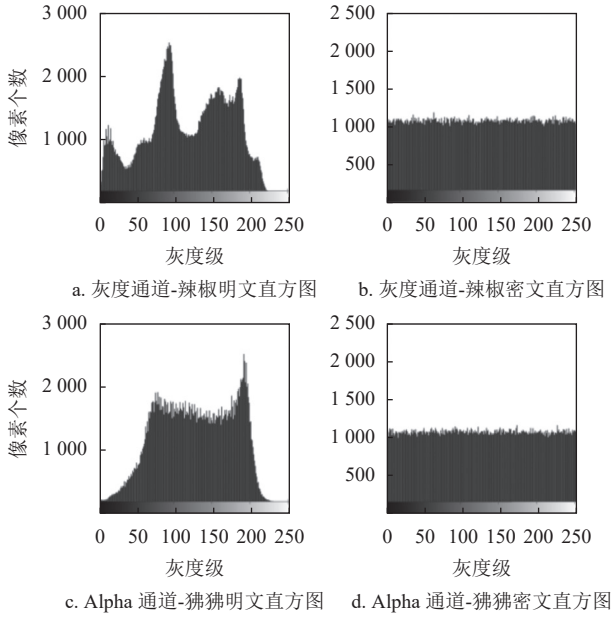
a. 辣椒 b. 狒狒 c. 重构图像

d. 密文图像 e. 解密辣椒 f. 解密狒狒

图 9 原始图像加解密实验的结果展示图

2.2 算法的性能分析

为了验证多图像加密方法的安全性能，图 10 给出了加解密前后的直方图；由图可见，图像辣椒与图像狒狒的密文图像直方图均近似均匀分布，攻击者很难从中获取有效信息。

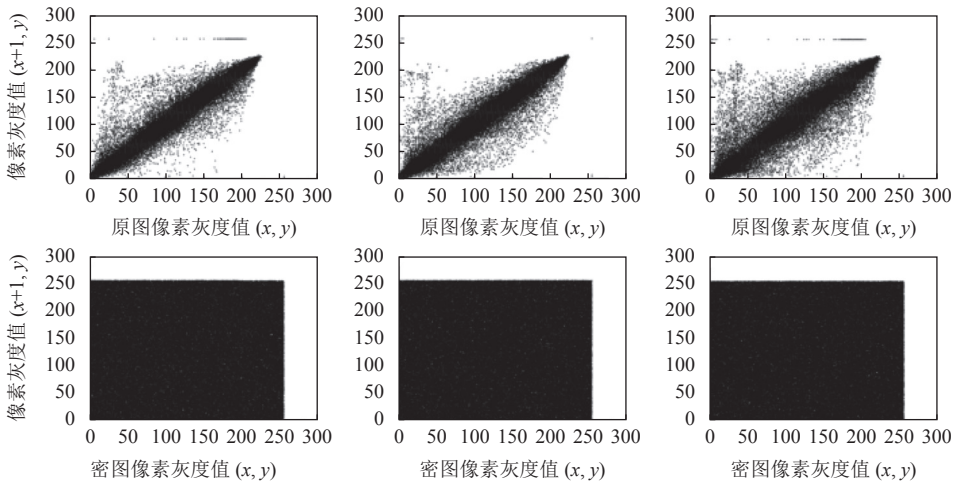


a. 灰度通道-辣椒明文直方图 b. 灰度通道-辣椒密文直方图

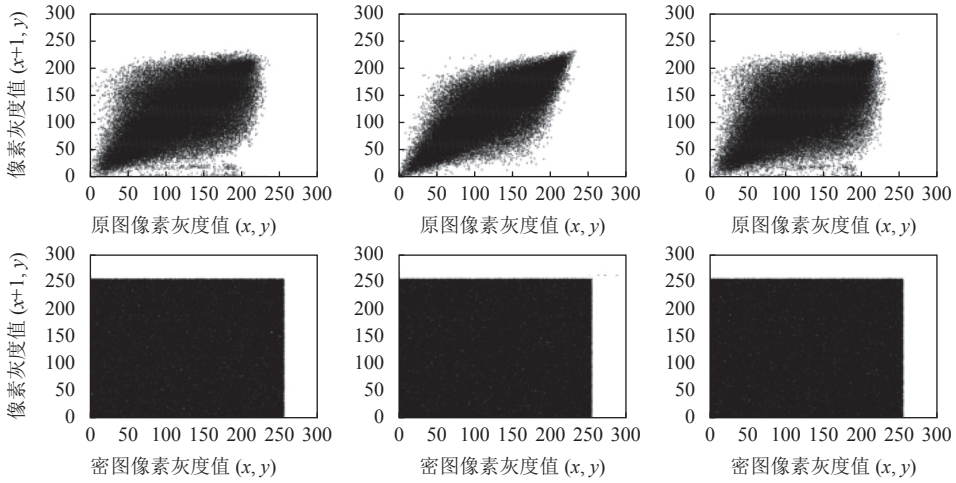
c. Alpha 通道-狒狒明文直方图 d. Alpha 通道-狒狒密文直方图

图 10 灰度通道和 Alpha 通道的明文和密文直方图

此外，为了更加直观地说明多图像加密方法打破相邻像素相关性的能力，图 11 给出了加密前后灰度通道与 Alpha 通道的像素相关性分布图。由图可见，加密后的相关性分布遍布整个区域，有效地破坏了明文图像的像素相关性分布。



a. 灰度通道相邻像素的相关性



b. Alpha 通道相邻像素的相关性

图 11　灰度通道和 Alpha 通道的明文和密文相邻像素相关性对比图

信息熵用于表征一个数字图像像素的分布情况，信息熵越接近理想值 8，像素分布越随机。为验证加密算法扰乱明文图像像素分布的能力，对辣椒和狒狒加密前后图像进行信息熵分析。表 1 给出了经加密算法加密后，明文图像与密文图像的信息熵。可以看出，密文图像的信息熵接近理想值 8，这证明设计的加密算法可以更加有效地打乱明文像素分布。

表 1　信息熵分析表

图像	明文信息熵	密文信息熵
辣椒	6.796 1	7.999 2
狒狒	6.504 4	7.999 3

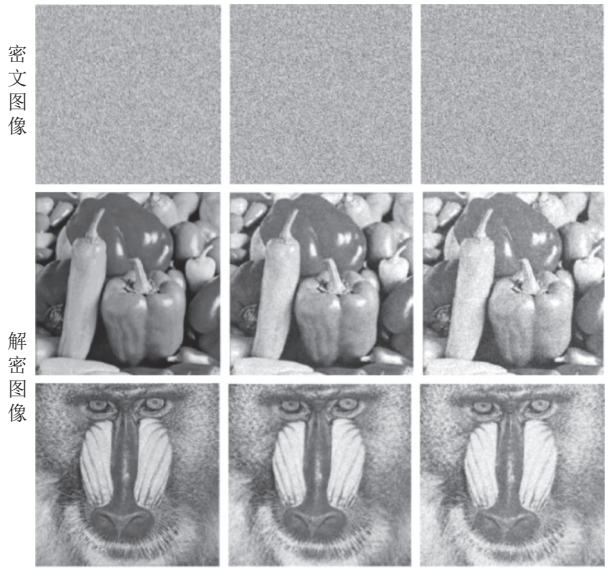
加密算法的抗差分攻击能力主要体现在对同一明文图像任一像素点施加微小改变，密文图像随之产生相应变化的能力。本文将明文图像某一像素点的像素值减 1，然后通过计算 NPCR 和 UACI，对抗差分攻击能力进行评估，结果如表 2 所示。可以看出，加密算法的 NPCR 和 UACI 接近理想值 99.609 4% 和 33.463 5%，说明设计的加密算法对明文的微小变化具有更高的敏感性，可以更加有效地抵御差分攻击。

表 2　抗差分攻击能力分析表　　%

图像	NPCR	UACI
辣椒	99.60	33.49
狒狒	99.63	33.48

当图像进行网络传输时，可能会引入各种噪声干扰，导致密文图像某些像素点的像素值发生改变，进而影响到原始图像有效信息的恢复。本文对辣椒和狒狒加密后的密文图像分别加入 5%、10% 和 20% 的椒盐噪声，以此验证加密算法的抗噪声

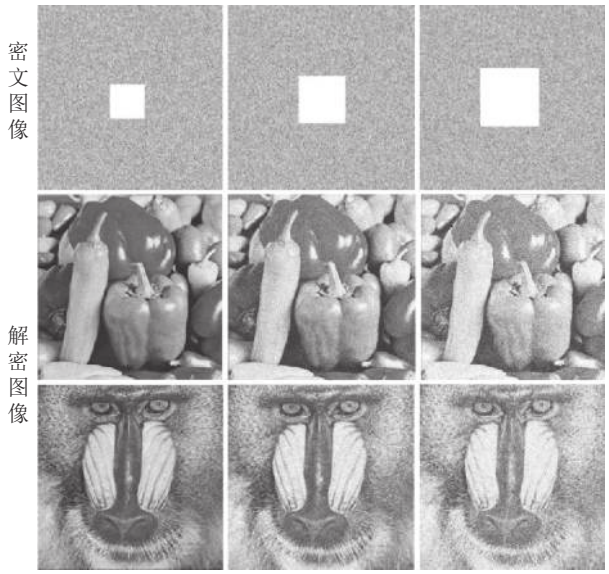
能力。图 12 为辣椒和狒狒引入椒盐噪声后的密文图像以及运用解密算法解密后的图像。可以看出，引入不同程度的椒盐噪声后，解密图像虽然受到一定程度的损坏，但是依旧可以分辨出大部分有效信息，因此所提加密算法具有良好的抗噪声能力。



a. 加入 5% 椒盐噪声 b. 加入 10% 椒盐噪声 c. 加入 15% 椒盐噪声

图 12 算法性能对比：抗噪声分析

为验证加密算法的抗剪切能力，本文将辣椒和狒狒加密后的密文图像，在不同位置剪切不同像素大小的信息，然后再对其进行解密，剪切后的密文图像以及相应的解密图像如图 13 所示。从图中可以看出，密文图像受到人为剪切后，加密算法仍然可以恢复出原始图像的主要信息，具备良好的抗剪切能力。



a. 剪切 5% 数据 b. 剪切 10% 数据 c. 剪切 15% 数据

图 13 算法性能对比：抗剪切分析

3 结 束 语

基于变参数超混沌系统的多图像加密方法，主要由 4 个部分构成：变参数超混沌系统构建、图像预处理与密钥生成、幻方变换置乱和 S 形扩散。首先借助 Alpha 通道的概念，将输入灰度图像对进行重构，然后将重构图像作为初始信息输入 SHA-512 算法生成初始密钥，再将其输入变参数超混沌系统迭代生成 5 组混沌序列，进而对重构图像进行幻方变换，实现像素位置的变换，最后基于 S 形扩散实现像素数值的变化，从而得到密文图像。

与传统图像加密方法相比，基于变参数超混沌系统的多图像加密方法，具有如下优点：

1）将混沌系统的参数作为加密过程中的控制变量之一，运用另一个混沌系统的状态变量对其施加一定的扰动，以构造变参数超混沌系统，同时确保该混沌系统依旧处于混沌状态，生成具有更高复杂度和随机性的伪随机序列，有效地改善了传统混沌系统的低随机性、低复杂度以及混沌系统退化等缺陷；

2）采用幻方变换的置乱方法，最大程度地对图像像素进行位置上的置乱，并创造性地提出 S 形扩散方法，提高了密文图像的无序性，打破了像素相关性分布，具有更优越的加密性能表现，难以被暴力破译；

3）采用 SHA-512 算法，结合明文图像生成初始密钥，保证一幅图像仅仅对应一种密钥流，有效地提高了加密算法抵抗明文攻击的能力；

4）本文设计的加密算法可以有效地打乱明文像素分布、有效地抵御差分攻击，具有良好的抗噪声能力和具备良好的抗剪切能力。

参 考 文 献

[1] WANG X, ZHAO M. An image encryption algorithm based on hyper-chaotic system and DNA coding[J]. Optics and Laser Technology, 2021, 143: 107316.

[2] XUE Q Y, LUO Y L, LIU J X, et al. A color image encryption method based on memristive hyperchaotic system and DNA encryption[J]. International Journal of Modern Physics B, 2020, 34: 2050014.

[3] HOSNY K M, KAMAL S T, DARWISH M M, et al. New image encryption algorithm using hyperchaotic system and fibonacci Q-matrix[J]. Electronics, 2021, 10: 1066.

[4] ZHOU S, WANG X Y, ZHANG Y Q. Novel image encryption scheme based on chaotic signals with finite precision error[J]. Information Sciences, 2022, 22: 01395.

[5] GAO X Y, YU J W, BANERJEE S, et al. A new image

encryption scheme based on fractional-order hyperchaotic system and multiple image fusion[J]. Scientific Reports, 2021, 11: 15737.

[6] SHEELA S J, SANJAY A, SURESH K V, et al. Image encryption based on 5D hyperchaotic system using hybrid random matrix transform[J]. Multidimensional Systems and Signal Processing, 2022, 33: 579-595.

[7] HUI Y Y, LIU H, FANG P F. A DNA image encryption based on a new hyperchaotic system[J]. Multimedia Tools and Applications, 2021, 82: 21983-22007.

[8] WANG Y Z, YANG F F. A fractional-order CNN hyperchaotic system for image encryption algorithm[J]. Physica Scripta, 2021, 96: 035209.

[9] QI G Y, VAN WYK M A, VAN WYK B J, et al. On a new hyperchaotic system[J]. Physics Letters A, 2008, 372: 124-136.

[10] FAN C L, DING Q. A universal method for constructing non-degenerate hyperchaotic systems with any desired number of positive Lyapunov exponents[J]. Chaos, Solitons and Fractals, 2022, 161: 112323.

[11] WU L L, ZHANG J W, DENG W T, et al. Arnold transformation algorithm and anti-arnold transformation algorithm[C]//1st International Conference on Information Science and Engineering. [S.l.]: IEEE, 2009: 1164-1167.

[12] WANG X Y, SUN H H, GAO H. An image encryption algorithm based on improved baker transformation and chaotic S-box[J]. Chinese Physics B, 2021, 30: 060507.

[13] WANG J, LIU L F. A novel chaos-based image encryption using magic square scrambling and octree diffusing[J]. Mathematics, 2022, 10: 457.

[14] HERBADJI D, DEROUICHE N, BELMEGUENAI A, et al. A tweakable image encryption algorithm using an improved logistic chaotic map[J]. Traitement du Signal, 2019, 36: 407-417.

[15] LIU L D, JIANG D H, WANG X Y, et al. 2D logistic-adjusted-chebyshev map for visual color image encryption[J]. Journal of Information Security and Applications, 2021, 60: 102854.

[16] ZOU C Y, ZHANG Q, WEI X P, et al. Image encryption based on improved lorenz system[J]. IEEE Access, 2020, 60: 75728-75740.

[17] LIN R G, LI S. An image encryption scheme based on lorenz hyperchaotic system and RSA algorithm[J]. Security and Communication Networks, 2021, 5: 1-18.

[18] CHEN G R, MAO Y B, CHUI C K. A symmetric image encryption scheme based on 3D chaotic cat maps[J]. Chaos, Solitons and Fractals, 2004, 21: 749-761.

[19] FAN B, TANG L R. A new five-dimensional hyperchaotic system and its application in DS-CDMA[C]//9th International Conference on Fuzzy Systems and Knowledge Discovery. [S.l.]: IEEE, 2012: 2069-2073.

编　辑　叶　芳