DOI:10.11721/cqnuj20210509

基于变参超混沌与可逆向量积的图像加密算法*

周洪波[1]，尹文双[2]，刘静漪[2]，唐利明[2]
(1. 贵阳学院 数学与信息科学学院，贵阳 550005；2. 湖北民族大学 数学与统计学院，湖北 恩施 445000)

摘要:【目的】通过对混沌序列随机性的增强和可逆算法的研究,提出一种基于变参超混沌和可逆向量积的图像加密算法。【方法】提出的算法通过动态控制超混沌参数增强混沌序列的随机性,同时设计了一种可逆向量乘法运算规则。首先通过迭代变参超混沌系统得到混沌序列,其中一个混沌序列用来置乱图像,另外两个混沌序列生成两个整数随机密钥矩阵,按照可逆向量乘法运算规则分别左乘和右乘图像矩阵,完成加密的扩散过程,得到加密图像。【结果】通过 MATLAB 仿真实验,密文图像信息熵为 7.997 4,和理论值 8 相差不足 0.003,NPCR 值超过 98%,UACI 值超过 33%。【结论】仿真实验结果表明本算法具有较高的安全性。

关键词:图像加密;变参超混沌;可逆向量积;信息安全
中图分类号:TP393.08　　**文献标志码**:A　　**文章编号**:1672-6693(2021)05-0090-08

在网络空间安全领域中,数据的安全性显得尤为重要。目前随着网络技术的发展,数字图像数据在网络的传输量与日俱增。数字图像数据与文本数据相比,具有数据量和冗余量大的特点,这便对数据的加密算法提出了新的要求。混沌特别是超混沌,因对初值和参数变化的极端敏感性和内在随机性与密码学的扩散和置换高度吻合,因此受到学者们的广泛关注,也逐渐成为信息安全领域的研究热点[1-2]。

混沌图像加密主要是借助于混沌的初值敏感性和内在随机性特性,利用混沌序列的不可预测性来保证图像加密的安全性。一维混沌结构简单,易于实现,但存在混沌范围有界和不连续性以及混沌序列的数据分布的非均匀性等问题[3],高维混沌系统具有复杂的结构和参数以及更高的安全性[4],因此受到众多研究者的关注。张永红等人[5]利用 Logistic 混沌系统生成的混沌矩阵与明文图像进行异或运算,然后进行置乱运算,该加密法过程简单易行,但密文分布不均匀,难以抵抗统计攻击;Liu 等人[6]通过改进 Logistic 混沌系统,增强混沌序列的随机性以提高加密算法的安全性;张勋才等人[7]结合超混沌系统、DNA 计算和哈希函数提出了一种基于 DNA 编码和超混沌系统的图像加密方案,提高了密钥敏感性和传输数据的安全性,具有较好的抗穷举攻击、统计攻击和差分攻击的能力;彭再平等人[8]、马聪等人[9]以及庄志本等人[10]利用多维超混沌系统来解决低维混沌用于图像加密算法密钥空间小的问题,获得较高的安全性;Luo 等人[11]通过修改 Henon 混沌系统的非线性项得到一个新的混沌系统,将混沌序列与图像加密结合,取得了良好的加密效果;Liu 等人[12]在分析李雅普诺夫指数和分岔的基础上提出一种四阶混沌系统,并用于医学图像的加密,具有较强的抵抗统计攻击的能力;Manjit 等人[13]利用自适应差分变换(Adaptive differential evolution,ADE)优化 Lorenz 混沌系统的参数,并利用哈希算法(Secure hash algorithm,Sha-3)从明文图像中生成密钥,提高了算法的参数敏感性和明文图像敏感性;Zarebnia 等人[14]、Pan 等人[15]以及郭媛等人[16]利用复合混沌设计图像加密算法,具有良好的加密效果。

在上述文献的混沌迭代过程中,初值和参数是固定的,混沌序列的随机性主要由系统内在随机特性决定,因此混沌系统的行为特性起着决定性作用。王丽娟等人[17]为克服混沌系统的周期性和提高混沌序列的随机性,利用 Logistic 映射和 Tent 映射构建了一种基于动态参数控制的混沌系统映射,增强了混沌序列的不可预测性,但改善后的混沌序列仅用于图像像素的置乱。超混沌与普通混沌相比具有更为复杂的动力学特性。本文设计了一种基于变参超混沌和向量积的图像加密算法,在超混沌系统迭代过程中动态改变控制参数,达到改善混沌序

* **收稿日期**:2020-08-17　**修回日期**:2021-04-19　**网络出版时间**:2021-09-13 12:58
资助项目:国家自然科学基金(No. 62061016);贵州省科技合作计划项目(No. 黔科合 LH 字[2015]7294 号)
第一作者简介:周洪波,女,讲师,研究方向为信息安全,E-mail:zhb5278@163.com;**通信作者**:刘静漪,男,软件设计师,E-mail:369417266@qq.com
网络出版地址:https://kns.cnki.net/kcms/detail/50.1165.n.20210910.1856.014.html

列随机性的目的，并设计了一种可逆向量乘法规则，通过密钥矩阵左乘和右乘图像矩阵完成图像扩散过程。该算法经过 MATLAB 仿真实验和安全性分析，表现出良好的加密效果。

1 变参超混沌系统和可逆向量积

1.1 变参超混沌系统

王丽娟等人[17]利用 Logistic 映射和 Tent 映射构造了一个新混沌系统(LCT)，该系统方程式为：

$$\begin{cases} x_{n+1}=M(p_{n+1},x_n) \\ p_{n+1}=N(y_{n+1}) \\ y_{n+1}=F(\mu,y_n) \end{cases}, \tag{1}$$

其中：$F(\mu,y_n)=\mu y_n(1-y_n)$是控制函数，$x_{n+1}=M(p_{n+1},x_n)=\begin{cases} px_n, & 0<x_n\leqslant 0.5 \\ p(1-x_n), & 0.5<x_n\leqslant 1 \end{cases}$是种子混沌映射，$N(y_{n+1})$是转换关系函数，将 $F(\mu,y_n)$的输出值映射到函数 $M(p,x_n)$的参数 p 的取值范围中。

超混沌具有两个或两个以上正的 Lyapunov 指数，动力学行为比普通混沌更为复杂，更有利提高图像加密算法的安全性。因此，本文将系统(1)做了如下改进：

1) $F(\mu,y_n)=\mu y_n(1-y_n)$为 Logistic 映射，在 $\mu\in(3.569\ 95,4)$系统处于混沌状态，为规避周期窗口本文 $\mu\in(3.89,4)$[18]。

2) 超混沌动力学特性比普通混沌更为复杂，本文利用 Chen 超混沌系统作为种子混沌映射 $M(p,x_n)$，得到：

$$\begin{cases} \dot{x}=a(y-x)+w \\ \dot{y}=dx-xz+cy \\ \dot{z}=xy-bz \\ \dot{w}=yz-rw \end{cases}。 \tag{2}$$

当控制参数 $a=35,b=3,c=12,d=7,0.108\ 5\leqslant r<0.179\ 8$ 时，系统(2)处于超混沌状态。

3) 转换关系函数 $N(y_{n+1})=0.07\times y_{n+1}+0.109$，将 Logistic 映射的输出值从(0,1)映射到(0.109,0.179)，作为 Chen 超混沌系统的控制参数 r 的取值范围。

通过上述改进，得到一个变参数的 Chen 超混沌系统，相图如图 1 所示。

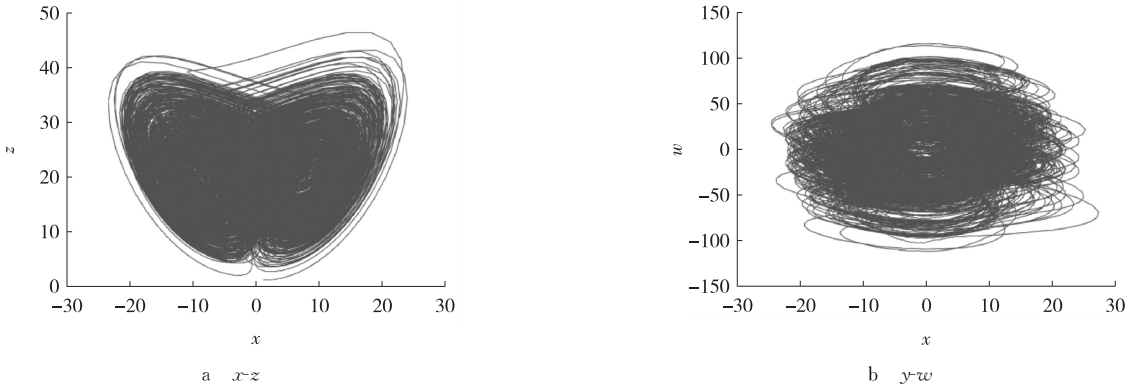


图 1　改进 Chen 系统的相图

Fig. 1　Phase diagram of improved Chen's system

1.2 可逆向量积

在代数中向量的乘积为：

$$\boldsymbol{A}\cdot\boldsymbol{B}=[a_1,a_2,\cdots,a_n]\begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{bmatrix}=a_1\times b_1+a_2\times b_2+\cdots+a_n\times b_n。$$

在图像加密中，加密算法必须是可逆的，本文对向量乘法及逆运算做出如下规定：

1) 密钥矩阵 $\boldsymbol{K}$ 为一个正整数的随机数矩阵，$\boldsymbol{P}$ 为待加密图像：

$$\boldsymbol{K}=\begin{bmatrix} k_{1,1} & k_{1,2} & \cdots & k_{1,n} \\ k_{2,1} & k_{2,2} & \cdots & k_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ k_{n,1} & k_{n,2} & \cdots & k_{n,n} \end{bmatrix},\ \boldsymbol{P}=\begin{bmatrix} p_{1,1} & p_{1,2} & \cdots & p_{1,n} \\ p_{2,1} & p_{2,2} & \cdots & p_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ p_{n,1} & p_{n,2} & \cdots & p_{n,n} \end{bmatrix}。$$

2) 在 $\boldsymbol{K}\times\boldsymbol{P}$ 时,对图像 $\boldsymbol{P}$ 逐个像素进行运算,运算方法为:

$$\boldsymbol{P}'(i,j)=\mathrm{mod}(\boldsymbol{K}(i,:)\times\boldsymbol{P}(:,j)-(\boldsymbol{K}(i,j)-1)\times\boldsymbol{P}(i,j),256)。\tag{3}$$

其中:mod(a,b)是取模运算,运算结果为参数 a 整除参数 b 所得的余数。当图像中任一像素(如 $\boldsymbol{P}(i,j)$)发生变化时,通过(3)式的加密,在加密图像 $\boldsymbol{P}'$ 中第 j 列中的像素都会发生变化,从而完成加密图像的列扩散。在 $\boldsymbol{K}\times\boldsymbol{P}$ 时,矩阵的逆运算公式为:

$$\boldsymbol{P}(i,j)=256+\boldsymbol{P}'(i,j)-\mathrm{mod}(\boldsymbol{K}(i,:)\times\boldsymbol{P}(:,j)-\boldsymbol{K}(i,j)\times\boldsymbol{P}(i,j),256)。\tag{4}$$

即(4)式为(3)式的逆运算。

3) 在 $\boldsymbol{P}\times\boldsymbol{K}$ 时,运算方法为:

$$\boldsymbol{P}''(i,j)=\mathrm{mod}(\boldsymbol{P}(i,:)\times\boldsymbol{K}(:,j)-\boldsymbol{P}(i,j)\times(\boldsymbol{K}(i,j)-1),256)。\tag{5}$$

当图像中任一像素(如 $\boldsymbol{P}(i,j)$)发生变化时,通过(5)式的加密,在加密图像 $\boldsymbol{P}''$ 中第 i 行中的像素都会发生变化,从而完成加密图像的行扩散。在 $\boldsymbol{P}\times\boldsymbol{K}$ 时,矩阵的逆运算公式为:

$$\boldsymbol{P}(i,j)=256+\boldsymbol{P}''(i,j)-\mathrm{mod}(\boldsymbol{P}(i,:)\times K(:,j)-\boldsymbol{P}(i,j)\times\boldsymbol{K}(i,j),256)。\tag{6}$$

即(6)式为(5)式的逆运算。

4) 在加密算法中有两种扩散方式:① 先执行列扩散,再执行行扩散,即先执行(3)式再执行(5)式;② 先执行行扩散,再执行列扩散,即先执行(5)式再执行(3)式。通过扩散运算后,改变待加密图像 $\boldsymbol{P}$ 的任何一个像素值,这个变化都能扩散到密文图像各个像素。

2 算法描述

2.1 加密算法

算法 1

步骤 1:读入待加密图像 $\boldsymbol{P}$,图像大小为 $m\times n$,计算出图像的像素个数 l_p。

步骤 2:输入控制函数 Logistic 映射的控制参数和初值[μ,y_0],迭代 t_r+l_p 次,得到一个 t_r+l_p 长的混沌序列 s_1,其中 t_r 为消除混沌暂态效应舍去的前 t_r 个混沌序列值。

步骤 3:通过转换关系函数 $N(y_{n+1})=y_{n+1}\times 0.07+0.109$,将混沌序列 s_1 转换成区间[0.109,0.179]的随机数序列 s_2。

步骤 4:输入 Chen 超混沌的初值[x_0,y_0,z_0,w_0],利用随机数序列 s_2 控制(2)式中参数 r 的变化,迭代(2)式 t_r+l_p 次,舍去前 t_r 个序列值,得到 4 个 l_p 长的混沌序列 $\boldsymbol{x}$,$\boldsymbol{y}$,$\boldsymbol{z}$,$\boldsymbol{w}$。

步骤 5:为改善混沌序列的分布状况和相关性,利用(7)式对混沌序列 $\boldsymbol{x}$,$\boldsymbol{y}$,$\boldsymbol{z}$,$\boldsymbol{w}$ 进行改进。

$$\begin{cases} \boldsymbol{x}=\boldsymbol{x}\times 10^4-\mathrm{round}(\boldsymbol{x}\times 10^4) \\ \boldsymbol{y}=\boldsymbol{y}\times 10^4-\mathrm{round}(\boldsymbol{y}\times 10^4) \\ \boldsymbol{z}=\boldsymbol{z}\times 10^4-\mathrm{round}(\boldsymbol{z}\times 10^4) \\ \boldsymbol{w}=\boldsymbol{w}\times 10^4-\mathrm{round}(\boldsymbol{w}\times 10^4) \end{cases},\tag{7}$$

其中:round(x)函数是将变量 x 的小数四舍五入,取最接近的整数。

步骤 6:将混沌序列 $\boldsymbol{x}$ 按从小到大的顺序排列,得到一个位置序列 S_{Num}。

步骤 7:将图像 $\boldsymbol{P}$ 转换成一维向量 $\boldsymbol{P}_1$,利用(8)式和位置序列 S_{Num} 进行置乱,得到置乱后的一维向量 $\boldsymbol{P}_1'$,然后再将 $\boldsymbol{P}_1'$ 转换成 $m\times n$ 的图像矩阵 $\boldsymbol{P}_2$:

$$\boldsymbol{P}_2(i)=\boldsymbol{P}_1(S_{\mathrm{Num}}(i))。\tag{8}$$

步骤 8:从 $\boldsymbol{x}$,$\boldsymbol{y}$,$\boldsymbol{z}$,$\boldsymbol{w}$ 中任选 2 个序列,利用(9)式截取小数点后 10~12 位,转换成 $m\times n$ 大小的 1~7 的整数随机矩阵 $\boldsymbol{K}_1$,$\boldsymbol{K}_2$,作为向量运算的密钥矩阵。

$$\boldsymbol{K}_i=\mathrm{mod}(\mathrm{floor}(\boldsymbol{S}\times 10^{12})-\mathrm{floor}(\boldsymbol{S}\times 10^9)\times 1\ 000,7)+1,\ i=1,2。\tag{9}$$

其中：$\boldsymbol{S}$ 是 $\boldsymbol{x}$，$\boldsymbol{y}$，$\boldsymbol{z}$，$\boldsymbol{w}$ 中任一序列，floor(x)表示取小于 x 的最大整数。

步骤 9：按照 1.2 节中的第 1 种扩散方式进行，即依次执行(10)式和(11)式计算，$\boldsymbol{P}_4$ 为最终所得密文图像。

$$\boldsymbol{P}_3=\boldsymbol{K}_1\times\boldsymbol{P}_2, \tag{10}$$

$$\boldsymbol{P}_4=\boldsymbol{P}_3\times\boldsymbol{K}_2。 \tag{11}$$

2.2 解密算法描述

解密算法是加密算法的逆运算，输入密文图像和混沌系统的控制参数和初值，通过迭代混沌系统得到混沌序列，并转换成随机整数密钥矩阵，先进行两轮向量乘法逆运算，再进行像素位置还原即可得到解密图像。

3 仿真实验结果

本文以 256×256 大小的 Lena、Baboon 和 Pepper 灰度图像为样本图像，具体仿真实验的环境为：CPU 为 Intel(R)core(TM)i5-8250U，内存 8 GB，WIN10 操作系统。仿真软件为 MATLAB 2016A。实验中以 Logistic 系统的参数和初值以及 Chen 超混沌系统作为密钥，其中 Logistic 系统的参数和初值分别为 3.901 和 0.6，Chen 超混沌系统的参数为：$a=35$，$b=3$，$c=12$，$d=7$，$r\in[0.109,0.179]$，初值为：(1.256，1.387，1.566，1.867)。图 2 为 Lena 的密文图像和解密图像。

a　Lena 密文图像　　b　Lena 解密图像

图 2　Lena 图像仿真实验结果

Fig. 2　Lena's simulation experiment results

4 安全性分析

4.1 信息熵分析

在数字图像中，像素灰度值分布越均匀，信息熵越大，灰度值分布的随机性越强。信息熵的计算公式如下所示：

$$H(X)=-\sum_{i=0}^{255}p(x_i)\log p(x_i),$$

其中：$p(x_i)$表示灰度值 x_i 出现的概率，8 bit 灰度图像的信息熵的理想值为 8。表 1 为 Lena 图像信息熵的对比，从数据中可以看出，用本算法加密的密文图像信息熵为 7.997 4，和理想值 8 相差不足 0.003。

表 1　信息熵对比

Tab. 1　Information entropy of plaintext and ciphertext image

Lena 明文图像	Lena 密文图像	文献[6]	文献[19]	文献[20]
7.483 2	7.997 4	7.995 9	7.991 7	7.997 0

4.2 直方图分析

灰度统计攻击是利用图像灰度值的分布规律进行攻击，像素灰度值分布越均匀，抵御统计攻击能力越强。像素灰度值分布的均匀程度可通过直方图的平滑程度直观地反映。从图 3 可以看出密文图像直方图十分平滑，说明密文图像的像素值在[0，255]范围内分布十分均匀，打破了像素之间的相关性，有效掩盖了像素值的统计特性。

4.3 差分攻击分析

差分攻击是指通过对明文图像做微小变化,分析密文图像的变化来攻击加密算法的已知明文攻击方法。抵抗差分攻击的能力依赖于加密算法的明文敏感性,明文敏感性越高抵抗差分攻击能力越强,像素变化率(V_{NPCR})和归一化像素值平均变化强度(V_{UACI})是衡量敏文敏感性的重要指标,具体计算公式如下:

$$V_{NPCR}=\frac{\sum_{i=1}^{m}\sum_{j=1}^{n}D(i,j)}{m\times n}\times 100\%,$$

$$D(i,j)=\begin{cases}1, & P_1(i,j)\neq P_2(i,j)\\ 0, & P_1(i,j)=P_2(i,j)\end{cases},$$

$$V_{UACI}=\frac{\sum_{i=1}^{m}\sum_{j=1}^{n}|P_1(i,j)-P_2(i,j)|}{m\times n\times 255}\times 100\%。$$

其中:m,n 分别表示图像的行数和列数,P_1 表示原图像的密文图像,P_2 表示改变后的图像的密文图像。本文为测试抵抗差分攻击能力,随机改变明文图像的一个像素值,使之增加1,所得 V_{NPCR} 和 V_{UACI} 如表2所示,表中数据显示 V_{NPCR} 均超过98%,V_{UACI} 均超过33%,说明本文提出的算法具有较好的明文敏感性,能够有效地较强抵抗差分攻击。

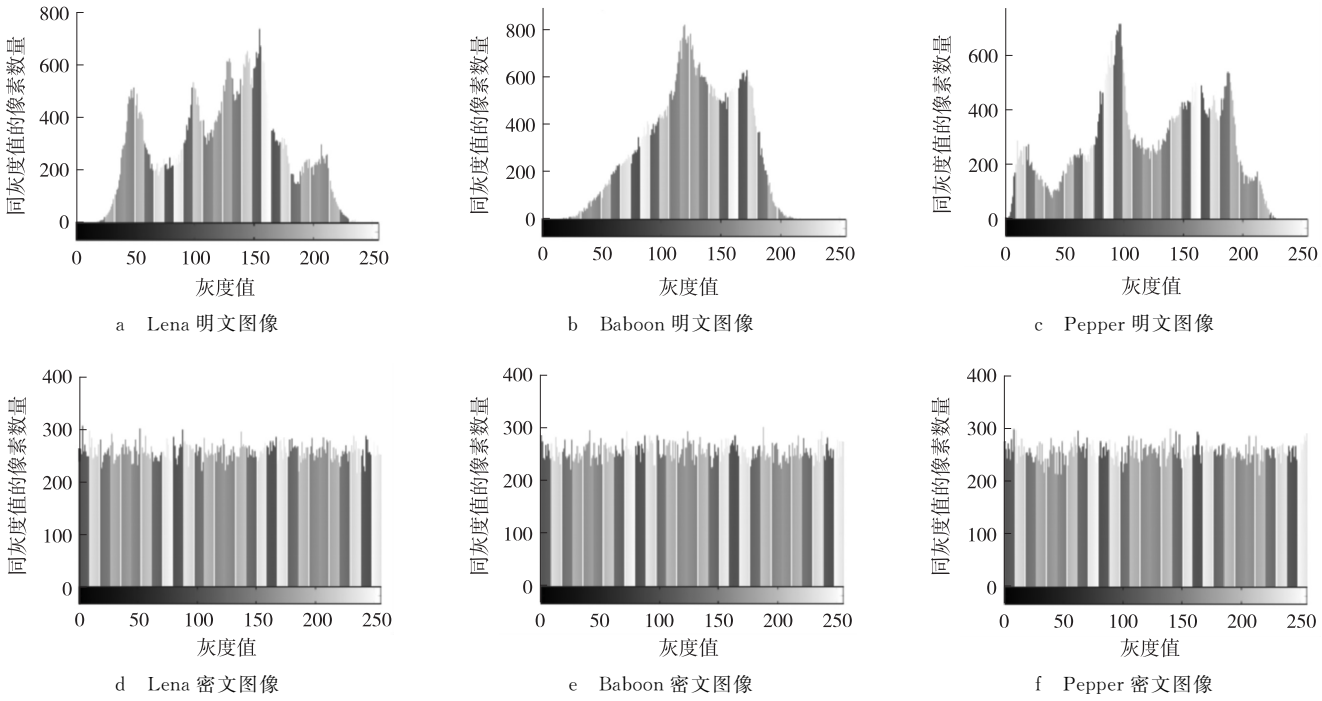


图3 明文图像和密文图像的直方图对比

Fig. 3 Histogram of plaintext and ciphertext image

表2 图像的 V_{NPCR} 和 V_{UACI}

Tab. 2 V_{NPCR} and V_{UACI} of image

图像	指标	(1,1)	(100,100)	文献[6]	文献[19]	文献[20]
Lena	V_{NPCR}	98.21%	98.53%	93.76%	99.61%	98.78%
	V_{UACI}	33.30%	33.37%	16.86%	33.55%	32.99%
Baboon	V_{NPCR}	98.21%	98.54%			
	V_{UACI}	33.29%	33.38%			
Pepper	V_{NPCR}	98.21%	98.54%			
	V_{UACI}	33.30%	33.40%			

4.4 相邻像素相关性分析

数字图像的特点之一是相邻像素的相关性很高，加密应消除或有效降低密文图像相邻像素间的这种相关性，计算公式如下：

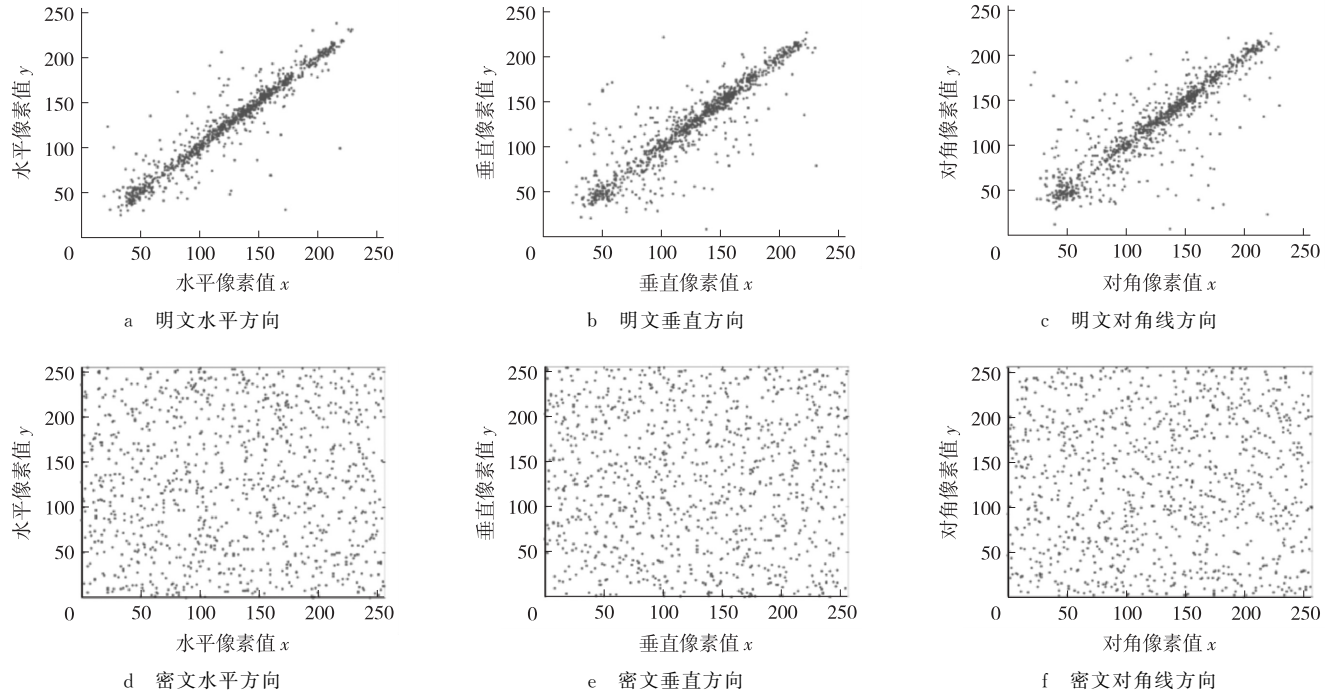
$$\sigma_{xy}=\frac{\sum_{i=1}^{n}(x_i-\overline{x})\times(y_i-\overline{y})}{\sqrt{\left(\sum_{i=1}^{n}(x_i-\overline{x})^2\right)\times\left(\sum_{i=1}^{n}(y_i-\overline{y})^2\right)}},$$

其中：σ_{xy} 表示某个方向（水平、垂直、对角线）上的相邻像素相关系数，x_i，y_i 表示第 i 个相邻像素对的两个像素灰度值，n 表示在各方向（水平、垂直、对角线）上选取像素对的总数。本文在图像的水平、垂直和对角线 3 个方向上随机选取 1 000 个相邻的像素对，计算出明文图像和密文图像的相关系数如表 3 所示。表 3 数据显示明文图像在平、垂直、对角线 3 个方向上的相关系数均大于 0.8，说明明文图像在 3 个方向的相关性非常强，密文图像 3 个方向上的相关系数趋于 0，几乎不相关。图 4 用灰度值描点法画出 Lena 明文和密文图像在 3 个方向的分布图，图中明文图像的点集中分布在对角线附近，具有很高的相关性，密文图像的点随机地均匀布满了整个矩形空间，说明密文图像上的相邻像素值几乎没有关系。

表 3　相邻像素相关系数

Tab. 3　Correlation coefficient of adjacent pixels

图像	明文图像	密文图像	文献[6]	文献[19]	文献[20]
水平	0.949 1	0.006 5	0.001 2	−0.013 1	−0.020 8
垂直	0.907 3	−0.008 9	0.023 2	0.014 2	−0.042 4
对角线	0.857 7	0.008 5	−0.025 9	−0.004 4	0.021 2



a　明文水平方向　　b　明文垂直方向　　c　明文对角线方向

d　密文水平方向　　e　密文垂直方向　　f　密文对角线方向

图 4　Lena 相邻像素相关性图

Fig. 4　Correlation map of Lena's adjacent pixels

5 结论

本文通过 Logistic 混沌系统和 Chen 超混沌系统构建了一个变参数超混沌系统，迭代变参数超混沌系统所得到的混沌序列值的随机性更高，首先利用混沌序列 x 对图像进行位置置乱，然后再随机选择两个混沌序列转

换成整数随机矩阵,通过本文所设计的向量积规则,分别左乘和右乘图像矩阵,得到密文图像。经过MATLAB仿真实验和直方图、信息熵、相邻像素相关性分析,表明本文算法具有较高的安全性。

参考文献:

[1] 林青,王延江,王珺.基于超混沌系统的图像加密算法[J].中国科学:技术科学,2016,46(9):910-918.
LIN Q,WANG Y J,WANG J. The image encryption scheme with optional dynamic state variables based on hyperchaotic system [J]. Science China Technological Sciences,2016,46(9):910-918.

[2] 杨志宏,屈双惠,张彩霞,等.一个四翼超混沌系统在图像加密技术中的应用[J].西南大学学报(自然科学版),2018,40(5):170-177.
YANG Z H,QU S H,ZHANG C X,et al. A four-winged hyper-chaotic system and its application in image encryption[J]. Journal of Southwest University (Natural Science Edition),2018,40(5):170-177.

[3] 班多晗,吕鑫,王鑫元.基于一维混沌映射的高效图像加密算法[J].计算机科学,2020,47(4):278-284.
BAN D H,LÜ X,WANG X Y. Efficient image encryption algorithm based on 1*D* chaotic map[J]. Cumputer Science,2020,47(4):278-284.

[4] HUA Z,ZHOU Y,PUN C M,et al. 2D Sine Logistic modulation map for image encryption[J]. Information Sciences,2015,297:80-94.

[5] 张永红,张博.基于Logistic混沌系统的图像加密算法研究[J].计算机应用研究,2015,32(6):1770-1773.
ZHANG Y H, ZHANG B. Algorithm of image encrypting based on Logistic chaotic system[J]. Application Research of Computers,2015,32(6):1770-1773.

[6] LIU J,YANG D,ZHOU H,et al. A digital image encryption algorithm based on bit-planes and an improved logistic map[J]. Multimedia Tools and Applications,2018,77(8):10217-10233.

[7] 张勋才,刘奕杉,崔光照.基于DNA编码和超混沌系统的图像加密算法[J].计算机应用研究,2019,36(4):1139-1143.
ZHANG X C,LIU Y S,CUI G Z. Image encryption algorithm based on DNA encoding and hyper-chaotic system[J]. Application Research of Computers,2019,36(4):1139-1143.

[8] 彭再平,王春华,林愿,等.一种新型的四维多翼超混沌吸引子及其在图像加密中的研究[J].物理学报,2014,63(24):240506.
PENG Z P,WANG C H,LIN Y,et al. A novel four-dimensional multi-wing hyper-chaotic attractor and its application in image encryption[J]. Acta Physica Sinica,2014,63(24):240506.

[9] 伍朝阳,孙树亮,刘庆.基于像素层与比特层置乱的超混沌图像加密算法[J].中国科技论文,2018,13(14):1609-1613.
WU C Y,SUN S L,LIU Q. Hyperchaotic image encryption scheme based on pixel-level permutation[J]. China Science Paper,2018,13(14):1609-1613.

[10] 庄志本,李军,刘静漪,等.基于新的五维多环多翼超混沌系统的图像加密算法[J].物理学报,2020,69(4):50-63.
ZHUANG Z B, LI J, LIU J Y, et al. Image encryption algorithm based on new five-dimensional multi-ring multi-wing hyperchaotic system[J]. Acta Physica Sinica,2020,69(4):50-63.

[11] LUO H B,GE B. Image encryption based on Henon chaotic system with nonlinear term[J]. Multimedia Tools and Applications,2019,78(24):34323-34352.

[12] LIU J Z,TANG S,LIAN J,et al. A novel fourth order chaotic system and its algorithm for medical image encryption[J]. Multidimensional Systems and Signal Processing,2019,30(4):1637-1657.

[13] MANJIT K,VIJAY K. Adaptive differential evolution- based Lorenz chaotic system for image encryption[J]. Arabian Journal for Science and Engineering,2018,43:8127-8144.

[14] ZAREBNIA M,PAKMANESH H,PARVAZ R. A fast multiple-image encryption algorithm based on hybrid chaotic systems for gray scale images[J]. Optik,2019,179:761-773.

[15] PAN S,WEI J G,HU S B. A novel image encryption algorithm based on hybrid chaotic mapping and intelligent learning in financial security system[J/OL]. Multimedia Tools and Applications. https://doi.org/10.1007/s11042-018-7144-5.

[16] 郭媛,陈炜.一种复合混沌与卷积运算的图像加密算法[J].中国科技论文,2019,14(7):783-788.
GUO Y,CHEN W. Image encryption algorithm for complex chaos and convolution operation[J]. China Science Paper,2019,14(7):783-788.

[17] 王丽娟,李国东,吕冬梅.基于动态参数控制的混沌系统图像加密算法[J].计算机科学,2019,46(11A):469-472.
WANG L J,LI D G,LÜ D M. Chaotic system image encryption algorithm based on dynamic parameter control [J]. Cumputer Science,2019,46(11A):469-472.

[18] WANG X,SUN H. A chaotic image encryption algorithm based on zigzag-like transform and DNA-like coding[J]. Multimedia Tools and Applications,2019,78(24):34981-34997.

[19] 杨吉云,吴昊. 基于混沌系统和动态 DNA 编码与运算的彩色图像加密算法[J]. 计算机工程,2018,44(2):151-157.
YANG J Y,WU H. Color image encryption algorithm based on chaotic system and dynamic DNA coding and operation[J]. Computer Engineering,2018,44(2):151-157.

[20] 马聪,李国东. 基于 L-K 双混沌系统的彩色位级图像加密算法[J]. 计算机应用与软件,2020,37(3):321-326.
MA C,LI G D. Color bit-level image encryption algorithm based on L-K double chaotic system[J]. Computer Applications and Software,2020,37(3):321-326.

A Novel Image Encryption Scheme Based on Varying-Parameter Hyper-Chaos and Invertible Vector Product

ZHOU Hongbo[1], YIN Wenshuang[2], LIU Jingyi[2], TANGLiming[2]

(1. School of Mathematics and Information Science, Guiyang University, Guiyang 550005;
2. School of Mathematics and Statistic, Hubei Minzu University, Enshi Hubei 445000, China)

Abstract: [**Purposes**] By investigating the randomness enhancement of chaotic sequences and reversible algorithm, an image encryption algorithm based on variable parameter hyper-chaos and reversible vector product is proposed. [**Methods**] The algorithm enhances the randomness of chaotic sequences by dynamically controlling the hyper-chaos parameters. Meanwhile, a reversible vector product rule is designed. The chaotic sequences are obtained by iterating the variable parameter hyper-chaotic system. One chaotic sequence is used to scramble the image, and the other two chaotic sequences are generated two integer random key matrices. According to the reversible vector product rule, the image matrix is left and right multiplied by the key matrices. The encryption diffusion process is completed and an encrypted image is obtained. [**Findings**] Through the MATLAB simulation experiment, the result of the ciphertext image information entropy is 7.9974, the difference between it and the theoretical value 8 is less than 0.003, UPCR exceeds 98%, and UACI exceeds 33%. [**Conclusions**] The simulation results demonstrate that the algorithm has high security.

Keywords: image encryption; varying-parameter Hyper-chaos; invertible vector product; information security

(责任编辑 许 甲)