doi:10.12068/j.issn.1005-3026.2026.20269021

一种用于图像加密的骑士混沌巡游方法

陈 云[1]，唐 琦[1]，吴晓锋[2]
（1.海军工程大学，湖北 武汉 430033；2.泉州师范学院 数学与计算机科学学院，福建 泉州 362000）

摘 要：针对传统骑士巡游方法始终以日字形规则巡游，导致应用于图像加密时图像置乱程度较低、加密效率不高等问题，本文设计了1种骑士混沌巡游方法．该方法利用混沌伪随机序列动态控制骑士巡游在行和列方向上的移动步长，进行不规则巡游，克服了传统骑士巡游始终以日字形规则巡游的缺陷．将该方法应用于图像加密，提出了1种新的图像加密算法：通过三维Logistic混沌映射生成3个混沌整数伪随机序列，其中2个序列用于控制骑士巡游路径的生成，以实现像素置乱，另1个序列用于进行扩散操作，改变像素值，从而完成图像加密．最后，基于MATLAB软件仿真证实了所提的骑士混沌巡游图像加密算法在密钥敏感性、密钥空间、相邻像素相关性和置乱效率等方面均优于传统骑士巡游图像加密算法，并通过抗攻击实验证明了该算法具备良好的鲁棒性．

关 键 词：骑士巡游；混沌；三维Logistic映射；图像加密
中图分类号：TP 309.7 **文献标志码**：A **文章编号**：1005-3026(2026)07-0062-12

A Knight's Chaotic Tour Method for Image Encryption

CHEN Yun[1], *TANG Qi*[1], *WU Xiao-feng*[2]
(1. Naval University of Engineering, Wuhan 430033, China; 2. School of Mathematics and Computer Science, Quanzhou Normal University, Quanzhou 362000, China. Corresponding author: WU Xiao-feng, E-mail: mathwxf@sina.com)

Abstract: To address the problem that the traditional knight's tour always moves in a pattern based on the Ri (日) character, which results in a low degree of image scrambling and limited encryption efficiency when applied to image encryption, a knight's chaotic tour method was designed in this paper. By this method, chaotic pseudo-random sequences were used to dynamically control the step sizes of the knight's tour in the row and column directions to enable irregular movement, which overcame the limitation of the traditional knight's tour that always follows a pattern based on the Ri character. The method was applied to image encryption, and a new image encryption algorithm was proposed: three chaotic integer pseudo-random sequences were generated by using a three-dimensional Logistic chaotic map. Two of these sequences were used to control the generation of the knight's tour path to achieve pixel scrambling, and the other sequence was used for the diffusion operation to alter pixel values, thereby completing the image encryption. Finally, MATLAB-based numerical simulation confirms that the proposed knight's chaotic tour image encryption algorithm outperforms the traditional knight's tour image encryption algorithm in terms of key sensitivity, key space, adjacent pixel correlation, and scrambling efficiency. Furthermore, anti-attack tests prove that the proposed algorithm has good robustness.

Key words: knight's tour; chaos; three-dimensional Logistic map; image encryption

现今，图像凭借其直观、信息量大、相关性强等优点，在互联网、移动通信和多媒体系统中被广泛用作信息载体．但在传输过程中，图像信息也面临着被非法窃取等安全威胁．目前可用于文本数据保护的传统加密算法在应用于图像加密时，由于图像本身所具有的大数据量、强相关性

收稿日期：2026-03-28
作者简介：陈 云(1978—)，男，湖北钟祥人，海军工程大学副教授．
通信作者：吴晓锋，E-mail:mathwxf@sina.com.

及高冗余度等特性,存在着加密效率低、安全性不足等局限性[1].为此,亟待设计高效、安全、适合图像特点的图像加密算法.

目前图像加密常用的算法包括基于像素置乱和扩散的加密[2]、基于变换域的编码加密[3]、基于深度学习的端到端加密[4]等.而骑士巡游图像加密算法作为1种像素置乱技术,凭借其密钥空间大、置乱路径复杂、不可预测性强等优良特性,近年来在图像加密领域备受关注[5-11].Jiang 等[5]将骑士巡游与滑动滤波相结合,首先生成1个经修正的骑士巡游矩阵作为滑动加密滤波器模板,同时构建1个与待加密图像尺寸相同的骑士巡游矩阵以引导滤波路径滑动并进行卷积运算,从而完成加密.Singh 等[6]采用基于欧拉算法的骑士巡游路径对图像进行分块内像素重排置乱加密.Kumar 等[7]通过并行处理和交叉操作生成密钥序列,对选中的骑士位置与密钥进行异或运算以生成加密图像.Mahmood 等[8]将骑士巡游作为密钥生成器,运用改进的离散对角线扫描方法对像素进行置乱,再根据密钥决定每个像素的二进制旋转位数以实现扩散.Bisht 等[9]通过生成不同尺寸的骑士巡游矩阵作为密钥,将图像分割为相应大小的子块,再依据巡游路径所确定的顺序,对每个子块内的像素执行邻域加法运算,实现加密.兰红等[10]将图像划分成多个胞元数组矩阵,在每个胞元数组内进行 Arnold 变换,然后将每个胞元数组看作1个像素点,通过多次迭代骑士巡游路径并结合 Arnold 变换进行扩散,从而完成加密.Gao 等[11]首先利用 BP 神经网络对图像进行压缩和初步特征融合,随后运用骑士巡游路径对处理后的图像数据进行置乱,同步完成压缩与加密.

由于混沌系统具有初值敏感性、长期不可预测性等特有的动力学特征,与图像加密所需的密钥敏感性、混淆性等安全要求高度契合,在图像加密应用中表现出显著优势,已受到学者的广泛关注.Fridrich[12]将混沌与图像加密结合,提出了1种基于 Logistic 映射和 Arnold 变换的完整加密方案.Geng 等[13]结合改进希尔伯特曲线置乱、动态 DNA 编码、四维超混沌系统,设计了1种空域、频域交替置乱扩散的图像加密算法.Ghouate 等[14]将混沌序列控制变步长约瑟夫置乱用于图像加密,在不依赖高复杂度多维映射的前提下,有效提高了像素置乱的混乱程度.上述研究表明,混沌理论与其他置乱方法相结合,能有效地保护图像信息安全.

近年来,具有多个正 Lyapunov 指数的超混沌系统凭借其更复杂的混沌序列和更大的密钥空间等优势,在图像加密中得到了广泛应用[15].同时,如何将超混沌系统与骑士巡游置乱相结合的图像加密研究也得到了相关学者的关注[16-18].He 等[16]提出了1种结合骑士巡游算法与六维分数阶超混沌系统的图像加密算法,首先利用六维分数阶超混沌系统生成混沌序列,通过索引排序以实现置乱,然后选择骑士巡游的起始点,并在置乱后的图像上运行10轮骑士巡游进行2次置乱.Ullah 等[17]采用分数阶四维超混沌系统和二维 Henon 混沌映射生成混沌伪随机序列,从选定点出发,在置乱后的图像上进行指定轮数的骑士巡游,实现图像加密.但文献[16-17]均采用混沌系统生成伪随机序列以确定骑士巡游的起始位置,并在图像上执行固定轮数的巡游,其移动方式未作任何改变,置乱效果有限.Deng 等[18]基于新型四维超混沌系统,结合骑士巡游策略,设计了1种图像加密算法;但其置乱过程仍未脱离日字形的固定巡游方式,路径选择空间有限,难以获得充分的置乱效果.

因此,目前关于超混沌系统与骑士巡游置乱相结合的图像加密研究仍存在如下缺陷:一是用于图像加密的传统骑士巡游方法始终以日字形规则巡游,从而导致置乱效果不佳;二是部分文献[16-17]的加密算法需要进行多轮骑士巡游才能实现完全置乱,导致加密效率不高;三是虽然引入了混沌伪随机序列,但仅用于控制巡游起始点和巡游方向,并没有改变日字形的巡游规则,未充分利用混沌的伪随机性.

针对以上缺陷和混沌映射在图像加密中的优势,本文设计了1种骑士混沌巡游方法,通过混沌伪随机序列动态控制骑士巡游在行和列方向上的移动步长,实现不规则巡游;然后将该方法与三维 Logistic 混沌系统结合应用于图像加密,提出了1种图像加密算法.该图像加密算法有如下创新之处:一是通过骑士混沌巡游方法,突破了传统骑士日字形走法的限制,增强了置乱效果;二是该算法只需进行1轮骑士混沌巡游置乱,即可实现全局置乱,加密效率较高;三是该算法充分利用三维 Logistic 混沌映射生成混沌整数伪随机序列,不仅用于控制骑士巡游的起始点,还控制了巡游过程中每一步的行、列步长,显著增强了加密的伪随机性和不可预测性.

1 传统骑士巡游

骑士巡游问题[19]源于国际象棋,其目标是在棋盘上寻找1条遍历所有方格且不重复访问的哈密顿路径或回路.该问题的核心规则遵循国际象棋中骑士的日字形走法(横向走2格并纵向走1格,或横向走1格并纵向走2格),在任意位置,骑士的下一步共有8种可能的移动方向,且不可重复访问同一格子,如图1所示.

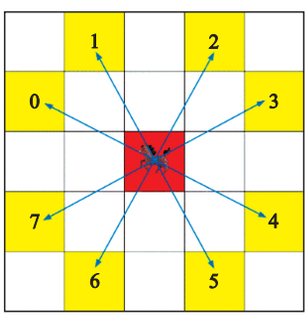


图1 巡游位置示意图

Fig. 1 Schematic diagram of tour positions

在数学上,骑士巡游问题可建模为图论问题:将棋盘方格作为顶点,骑士移动作为边,其解的存在性依赖于棋盘的维度与拓扑结构.例如,标准8×8棋盘已被证明存在闭合巡游解,而广义$M\times N$棋盘巡游解的存在性有待验证.回溯法是求解该问题的经典算法,其通过递归或迭代生成所有可能的移动序列,并利用剪枝策略及时终止超出边界、重复访问等无效路径搜索.例如,当某次移动导致后续没有尚未访问的方格时,算法将回溯至上一个状态并尝试其他方向[20].当遍历完所有棋盘方格后,算法得到1条完整的巡游路径.该路径构成的矩阵可作为加密密钥,而路径总数则对应密钥空间的大小.以5×5棋盘为例,定义棋盘格子坐标为(行号,列号),行、列均从"1"开始计数,如图2所示.

(1,1)	(1,2)	(1,3)	(1,4)	(1,5)
(2,1)	(2,2)	(2,3)	(2,4)	(2,5)
(3,1)	(3,2)	(3,3)	(3,4)	(3,5)
(4,1)	(4,2)	(4,3)	(4,4)	(4,5)
(5,1)	(5,2)	(5,3)	(5,4)	(5,5)

图2 棋盘示意图

Fig. 2 Schematic diagram of chessboard

利用回溯法从棋盘左上角的第1个格子开始巡游,可得到1条巡游路径:(1,1)→(3,2)→(5,1)→(4,3)→(5,5)→(3,4)→(1,5)→(2,3)→(4,4)→(2,5)→(1,3)→(2,1)→(4,2)→(5,4)→(3,5)→(1,4)→(2,2)→(4,1)→(5,3)→(4,5)→(2,4)→(1,2)→(3,1)→(5,2)→(3,3),如图3所示.

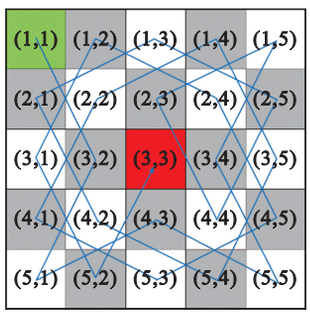


图3 传统骑士巡游路径示意图

Fig. 3 Schematic diagram of traditional knight's tour path

当棋盘大小为5×5时,一共存在304条不同的有向骑士巡游路径.而随着棋盘的扩大,在标准8×8棋盘上,巡游路径总数可达1.305×10^{35}条[21].这些不同的巡游路径保证了骑士巡游方法在图像加密应用中具有庞大的密钥空间,能够为加密算法提供坚实的安全基础.

但是,传统骑士巡游方法受限于固定的日字形巡游规则,巡游范围局限于邻近位置,导致其在图像加密应用中置乱效果欠佳.而通过多轮骑士巡游来增强置乱效果,又会带来效率下降的问题.此外,并非所有尺寸的图像都能找到1条完整的骑士巡游遍历路径.

2 骑士混沌巡游方法

鉴于传统骑士巡游方法的局限性,本文引入混沌伪随机序列,设计1种骑士混沌巡游方法,其核心思想是通过混沌整数伪随机序列动态选择每一步的巡游位置,以依次遍历棋盘中的所有格子.在每次迭代中,首先使用1个混沌整数伪随机序列$\{x_i\}$(i=1,2,3,…)通过模运算从可用行中随机选取1个行坐标;然后使用另1个混沌整数伪随机序列$\{y_i\}$(i=1,2,3,…)从该行当前可选列中随机选取1个列坐标.每次选取后,通过列更新移除该坐标对应的格子.在此过程中,若某一行内的所有位置都已被选取,则将该行从可用行集合中剔除.通过动态更新可用行和可用列,排除已

访问过的像素,确保每个像素仅被访问1次,最终遍历所有格子,实现对原始棋盘的置乱.其主要步骤如下:

步骤1　将大小为$M\times N$棋盘中的所有格子映射为二维坐标(行,列),其中行索引的范围是1到M,列索引的范围是1到N,M和N可为任意正整数,且不必相等.

步骤2　采用2个混沌整数伪随机序列$\{x_i\}$(i=1,2,3,…)和$\{y_i\}$(i=1,2,3,…)控制骑士巡游的路径.将混沌整数伪随机序列$\{x_i\}$中的第i个元素x_i代入式(1)中先确定目标行索引值row,式(1)中模数current_rows的值为当前可用行的数量,current_rows的取值范围为1到M,经过式(1)的模运算后,其值的范围为0到M–1,进行加1操作后其结果能够对应行索引的所有值.再将混沌整数伪随机序列$\{y_i\}$中的第i个元素y_i代入式(2)以确定该步定位到的目标列索引值col,其中模数current_cols的值为当前所选行中可用列的数量,进行加1后其结果能够对应列索引的所有值.根据式(1)和式(2)可确定该步骑士巡游的位置:

$$\mathrm{row}=\left(x_i \bmod \mathrm{current_rows}\right)+1, \tag{1}$$

$$\mathrm{col}=\left(y_i \bmod \mathrm{current_cols}\right)+1. \tag{2}$$

步骤3　更新当前行中剩余格子的坐标,其他行的格子坐标不变,位于当前巡游位置之前的格子列坐标保持不变,之后的格子列坐标减1.通过更新调整,确保后续操作即使再次取到该行,在确定列索引值时不会重复选取到已访问过的位置.

步骤4　重复步骤2,步骤3操作,根据骑士巡游的位置,每确定1个新位置,便将当前位置的原始格子移动至新位置,逐步实现全局置乱.当某一行中所有格子均已被遍历时,需要更新所有格子的行坐标:行索引小于该行的格子坐标不变,行索引大于该行的格子行坐标减1.同时,由于模数current_rows的值表示当前剩余行数,所以其值相应减1,以确保后续模运算的正确性.

步骤5　当遍历至最后1个格子时,将该格子移动至骑士巡游的起始位置,完成对所有格子的遍历,从而实现对整个棋盘的骑士混沌巡游.

骑士混沌巡游流程如图4所示.

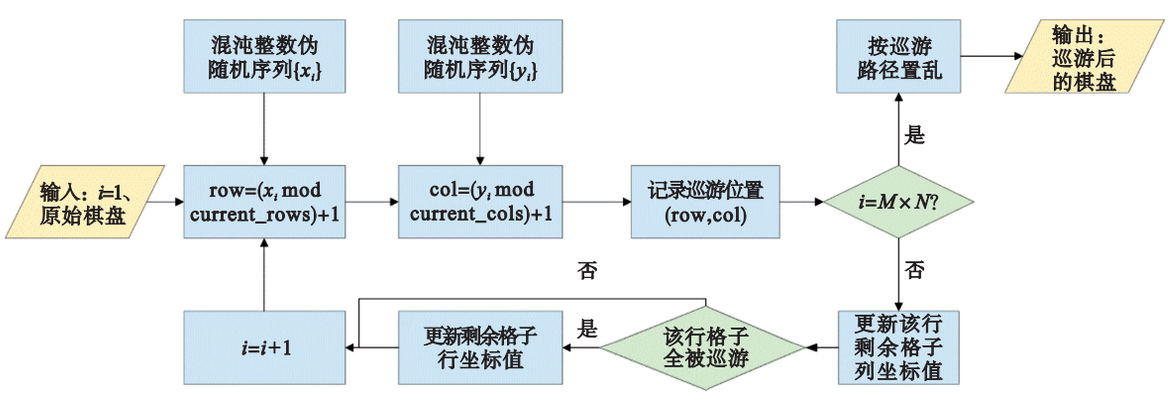


图4　骑士混沌巡游流程图

Fig. 4　Flowchart of knight's chaotic tour

为更加直观地阐述该置乱方法的原理与步骤,以5×5的棋盘为例,如图5所示.第1步,为棋盘中的每个格子按行和列的顺序分别从1到5设置1个二维坐标.第2步,将混沌整数伪随机序列$\{x_i\}$中的第i个元素x_i代入式(1),此时i的值为1,模数current_rows的值为5,假设得到的结果为3,则在此步中确定的行坐标值为3.同理,把混沌整数伪随机序列$\{y_i\}$中的第i个元素y_i代入式(2),此时i的值为1,模数current_cols的值为5,假设得到的结果为4,则在此步中确定的列坐标值为4.通过行和列的动态定位,确定选择坐标(3,4)所在的格子作为骑士巡游的第1个位置.第3步,将第3行格子的坐标值进行更新,在该行中位于(3,4)前的格子坐标保持不变,之后格子的列坐标值减1,这样即使下一次再取到该行,也不会重复选取已访问过的格子.第4步,重复进行选取位置与坐标更新两步操作,假设在某次循环后,某一行中所有格子都已经被遍历,则更新剩余格子的行坐标:位于该行之下的各行格子行坐标减1,列坐标不变,以此避免重复选取的可能.第5步,当遍历到最后1个格子时,下一步应移动至骑士巡游的起始位置,从而完成对5×5棋盘中所有格子的遍历,实现对整个棋盘的骑士混沌巡游.

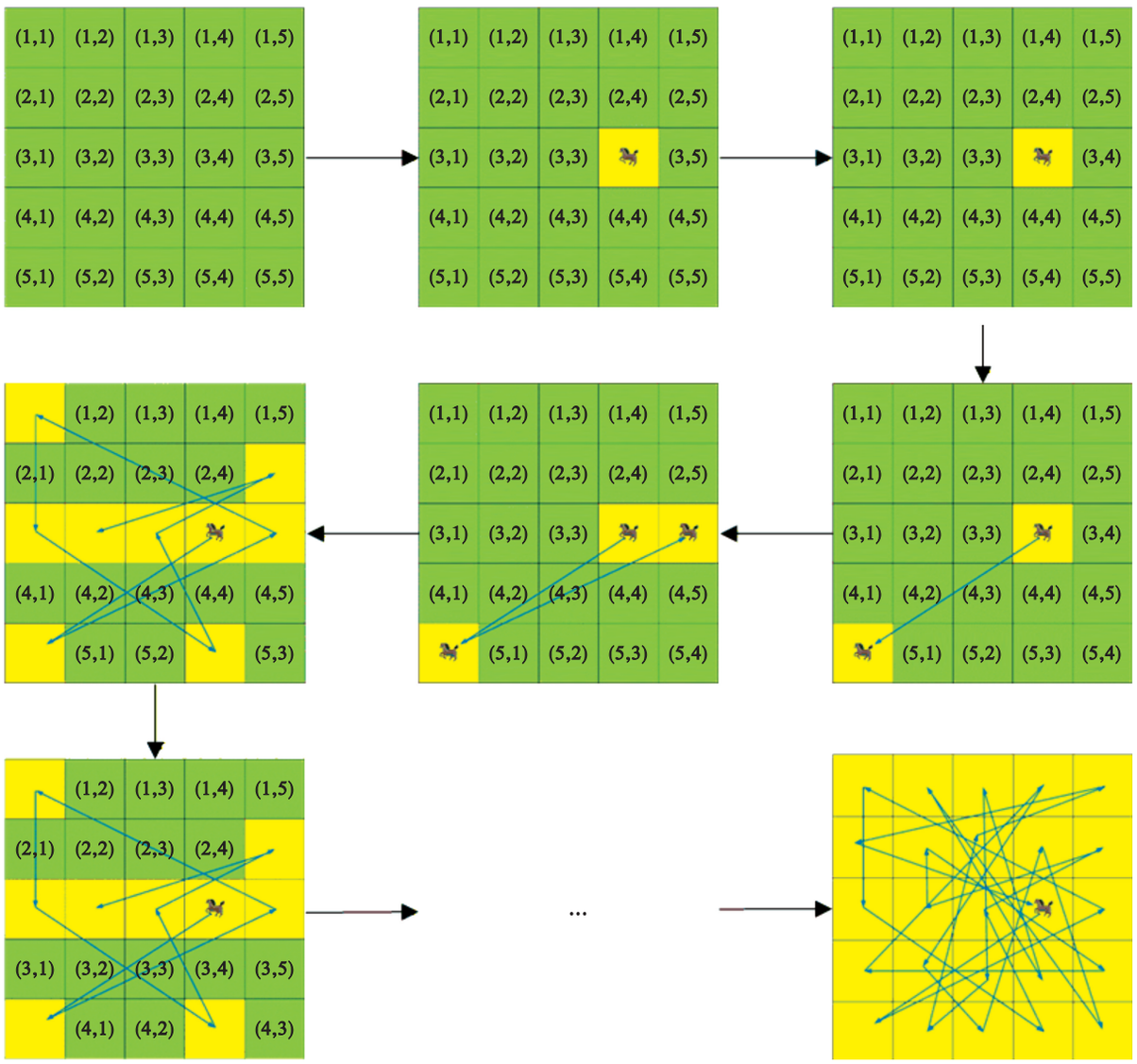


图5 骑士混沌巡游示例图

Fig. 5 Example diagram of knight's chaotic tour

从以上过程可以发现,本文提出的骑士混沌巡游方法的优点在于:该方法的巡游规则不再局限于日字形走法,下一步巡游的位置也不再局限于原位置附近,进行1次骑士混沌巡游便可以彻底打乱像素排列顺序,在增强置乱效果的同时提高了处理效率.此外,该方法适用于任意尺寸的棋盘,应用于图像加密时无需对图像进行补零或裁剪处理.

3 骑士混沌巡游方法在图像加密中的应用

3.1 三维Logistic混沌系统

三维Logistic混沌系统可表示为[22]

$$\left.\begin{aligned} x_{i+1}&=\alpha x_i(1-x_i)+\beta y_i^2 x_i+\gamma z_i^3,\\ y_{i+1}&=\alpha y_i(1-y_i)+\beta z_i^2 y_i+\gamma x_i^3,\\ z_{i+1}&=\alpha z_i(1-z_i)+\beta x_i^2 z_i+\gamma y_i^3. \end{aligned}\right\} \tag{3}$$

其中:(x,y,z)为系统的状态变量,每个变量的取值范围均为$[0,1]$;α,β,γ为系统参数.当参数取值为$3.68<\alpha<3.99$,$0<\beta<0.022$,$0<\gamma<0.015$时,该系统呈现出混沌特性[22].

如果系统参数及初始值$(\alpha,\beta,\gamma,X_0,Y_0,Z_0)=(3.80,0.010,0.005,0.1,0.2,0.3)$,可计算得到系统的3个Lyapunov指数(LE):$LE_1=0.442\ 3$,$LE_2=0.405\ 1$,$LE_3=-0.022\ 9$,其中2个为正,表明该系统为超混沌系统.图6为该三维Logistic映射的系统相图.

按16位有效数字(精度10^{-16})进行分析,系统的3个初始值取值范围长度均为1,每个初始值有10^{16}种取值可能.系统参数$\alpha\in(3.68,3.99)$,取值范围长度为3.99−3.68=0.31,其可能取值数量为$0.31/10^{-16}=3.1\times10^{15}$.同理,系统参数$\beta$的可能取值数量为$0.022/10^{-16}=2.2\times10^{14}$,系统参数$\gamma$的可能

取值数量为 $0.015/10^{-16}=1.5\times10^{14}$. 因此,该加密系统的总密钥空间 $S=(10^{16})^3\times(3.1\times10^{15})\times(2.2\times10^{14})\times(1.5\times10^{14})\approx2^{306}$,密钥空间庞大.

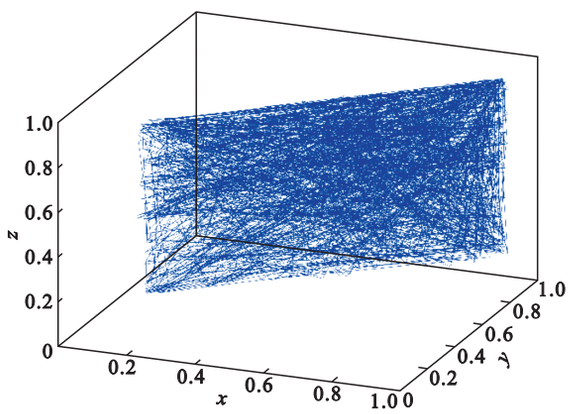


图 6　系统相图

Fig. 6　Phase diagram of system

图 7 展示了三维 Logistic 混沌系统在添加初始扰动下的密钥敏感性测试结果. 可以看出,该系统对初始值具有极强的敏感性,微小的密钥偏差会导致生成的伪随机序列完全不同.

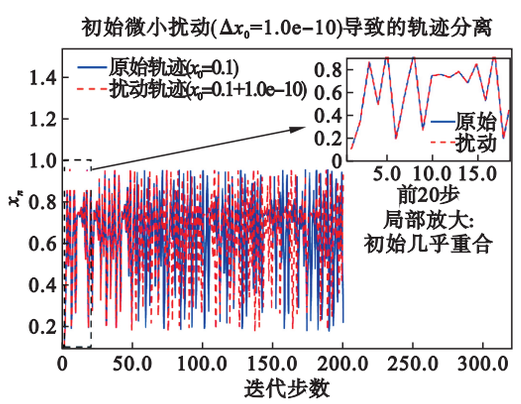


图 7　密钥敏感性测试图

Fig. 7　Test diagram for key sensitivity

3.2　基于骑士混沌巡游方法的图像加密算法

基于第 2 章提出的骑士混沌巡游方法,本节将其与上文介绍的三维 Logistic 混沌系统相结合,应用于图像加密,即将平面图像视为棋盘,棋盘格子对应图像像素点,由此提出 1 种基于骑士混沌巡游方法的图像加密算法. 其加密过程如下:

步骤 1　读取明文图像 P,然后进行预处理,将其分成 3 个通道(R,G,B),再将 3 个通道图像转换为尺寸为 $M\times N$ 的像素矩阵,并初始化所有行的编号为 1 到 M,每行中列编号为 1 到 N.

步骤 2　选取如下参数和初始值作为密钥 $K=(\alpha,\beta,\gamma,X_0^{\mathrm{R}},Y_0^{\mathrm{R}},Z_0^{\mathrm{R}},X_0^{\mathrm{G}},Y_0^{\mathrm{G}},Z_0^{\mathrm{G}},X_0^{\mathrm{B}},Y_0^{\mathrm{B}},Z_0^{\mathrm{B}})=(3.80,0.010,0.005,0.1,0.2,0.3,0.15,0.25,0.35,0.2,0.3,0.4)$,以 R 通道为例,代入式(4)中进行迭代:

$$\left.\begin{aligned}X_i&=\alpha X_{i-1}(1-X_{i-1})+\beta Y_{i-1}^2X_{i-1}+\gamma Z_{i-1}^3,\\Y_i&=\alpha Y_{i-1}(1-Y_{i-1})+\beta Z_{i-1}^2Y_{i-1}+\gamma X_{i-1}^3,\\Z_i&=\alpha Z_{i-1}(1-Z_{i-1})+\beta X_{i-1}^2Z_{i-1}+\gamma Y_{i-1}^3.\end{aligned}\right\}\tag{4}$$

去除前 1 000 次迭代结果以消除暂态效应,得到 3 个混沌伪随机序列 $\{X_i\}$,$\{Y_i\}$,$\{Z_i\}$.

步骤 3　对混沌伪随机序列 $\{X_i\}$,$\{Y_i\}$,$\{Z_i\}$ 按照式(5)乘以 10^{16} 进行整数化处理,得到 3 个混沌整数伪随机序列 $\{x_i\}$,$\{y_i\}$,$\{z_i\}$.

$$\left.\begin{aligned}x_i&=\mathrm{floor}\left(X_i\times10^{16}\right),\\y_i&=\mathrm{floor}\left(Y_i\times10^{16}\right),\\z_i&=\mathrm{floor}\left(Z_i\times10^{16}\right).\end{aligned}\right\}\tag{5}$$

其中:floor( )是向下取整函数.

步骤 4　对处理后得到的像素矩阵按照第 2 章介绍的骑士混沌巡游方法进行置乱,得到置乱后的像素矩阵 $\boldsymbol{A}$.

步骤 5　使用混沌整数伪随机序列 $\{z_i\}$ 对 256 取模,生成 1 个 $M\times N$ 的混沌矩阵 $\boldsymbol{L}$,将混沌矩阵 $\boldsymbol{L}$ 与上一步完成骑士混沌巡游后的置乱矩阵 $\boldsymbol{A}$ 进行异或运算,实现对置乱矩阵的扩散操作,得到密文矩阵.

步骤 6　同理,对另外 2 个通道分别进行步骤 2 到步骤 5 的操作,得到各通道的密文矩阵,再将 3 个通道的加密图像组合,得到彩色密文图像 C.

加密流程图如图 8 所示. 对于灰度明文图像,可将相同步骤直接应用于单通道像素矩阵,省去针对彩色图像的多通道分解和组合步骤.

基于骑士混沌巡游的图像解密过程为上述加密过程的逆过程,解密过程如图 9 所示.

3.3　仿真结果及性能分析

为验证所提图像加密算法的效果,本文选取 3 幅标准测试图像进行仿真实验,包括彩色图像 Female(256 像素×256 像素)、灰度图像 Baboon(512 像素×512 像素)和 Lena(512 像素×512 像素). 实验平台为 AMD Ryzen 7 5800H 处理器(3.20 GHz)、16.0 GB 内存、64 位 Windows 11 操作系统,使用 MATLAB R2023b 软件进行仿真.

在仿真中,基于 MATLAB GUI 编程设计并实现了 1 个用于图像加密、解密过程以及性能分析的可视化界面(如图 10 所示),对上述 3 幅图像进行加密与解密,仿真结果如图 11 所示. 从图 11 可以看出,生成的密文图像与对应的明文图像毫无关联,而解密后的图像与原始明文图像完全一致. 此外,使用错误密钥进行解密,得到的图像与

正确解密图像完全不同,这证实了本文提出的加解密方案的可行性与安全性.

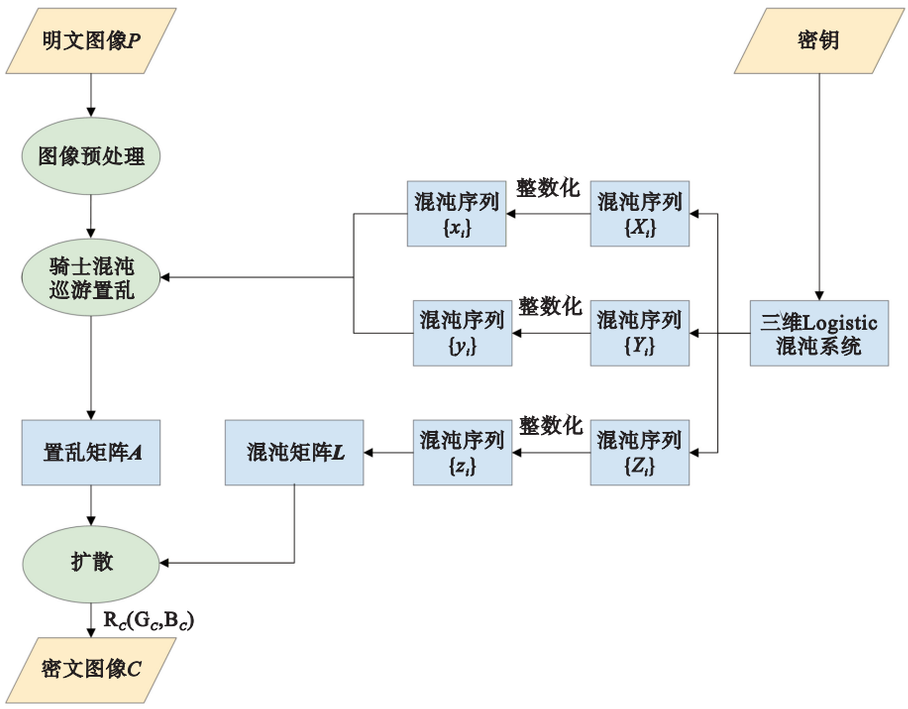


图 8 明文图像的加密流程图

Fig. 8 Encryption flowchart for plaintext image

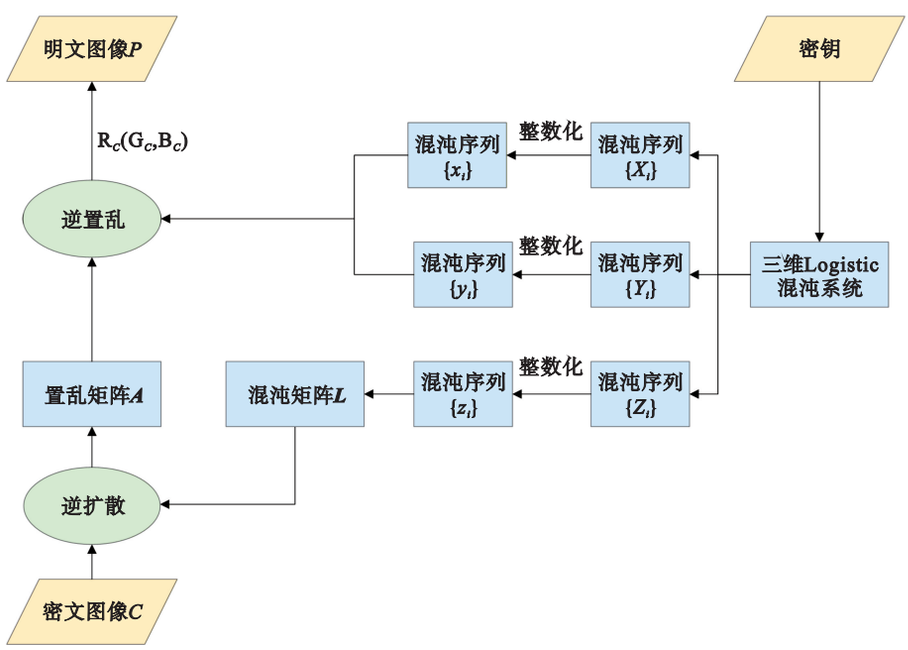


图 9 密文图像的解密流程图

Fig. 9 Decryption flowchart for encrypted image

3.3.1 密钥敏感性分析

密钥敏感性是衡量图像加密算法安全性的重要指标之一.为测试本文所提加密算法对密钥变化的敏感程度,计算像素变化率(NPCR)和统一平均变化强度(UACI),所得结果如表 1 所示,可知本文加密算法对密钥变化的敏感性很高,可有效防御差分攻击.

3.3.2 密钥空间分析

为有效抵抗暴力破解,加密算法的密钥空间至少大于 2^{100}.本文在加解密过程中将彩图分解为 3 个通道(R,G,B)分别进行操作,为了进一步增大该算法的密钥空间并提高加解密安全性,3 个通道选取 3 组不同的初始值.故本文算法使用的密钥 K 包含 9 个初始值以及 3 个系统参数,共 12

个独立的密钥分量,总密钥空间 $S=(10^{16})^9\times(3.1\times10^{15})\times(2.2\times10^{14})\times(1.5\times10^{14})\approx2^{625}$. 该值远大于 2^{100},说明本文提出的算法具有足够大的密钥空间.表2比较了本文所提的加密算法与其他文献提出的加密算法的密钥空间.



图 10　基于 MATLAB GUI 的可视化界面

Fig. 10　Visual interface based on MATLAB GUI



图 11　明文图像与加解密图像

Fig. 11　Plain, encrypted and decrypted images

表 1　密钥敏感性对比

Table 1　Comparison of key sensitivity

图像	NPCR/%	UACI/%
Female	99. 606 1	33. 446 8
Lena	99. 608 7	33. 454 1
Baboon	99. 613 4	33. 419 0
理想值	99. 609 4	33. 463 5

表 2　密钥空间对比

Table 2　Comparison of key space

算法	密钥空间
本文	2^{625}
文献[10]	2^{75}
文献[18]	2^{256}
文献[23]	2^{80}

3. 3. 3　直方图分析

灰度直方图可用于展示图像中各像素值对应的分布情况,其横坐标表示像素值,纵坐标为对应像素值在图像中出现的频数.对 Female 明文图像和密文图像进行分析,从图 12 可以看出,明文图像的像素值分布极不均匀,存在多个明显峰值,而密文图像的灰度直方图分布相对均匀,各像素值频数差异较小.这表明本文算法有效打乱了明文图像的像素值分布规律,使攻击者难以通过像素值统计特征获取明文图像信息.

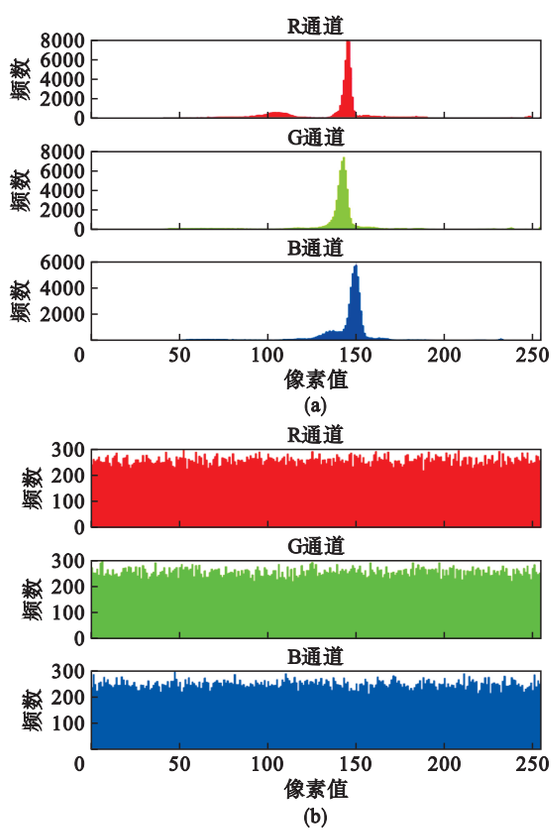


图 12　明文图像直方图与密文图像直方图对比

Fig. 12　Comparison between plain image histograms and encrypted image histograms

(a)—明文图像直方图;(b)—密文图像直方图.

3. 3. 4　相邻像素相关性分析

相邻像素相关性用于衡量图像中相邻像素间的关联程度.在明文图像中,相邻像素往往具有较高相关性.理想的加密算法应能大幅降低这

种相关性,使加密图像像素间呈现随机性.对Female明文图像和密文图像相邻像素相关性分析如图13所示,明文图像的散点沿对角线聚集,而密文图像的相邻像素相关性非常小,呈现出均匀分布的特性,说明所提算法很好地打破了明文图像像素之间的相关性.

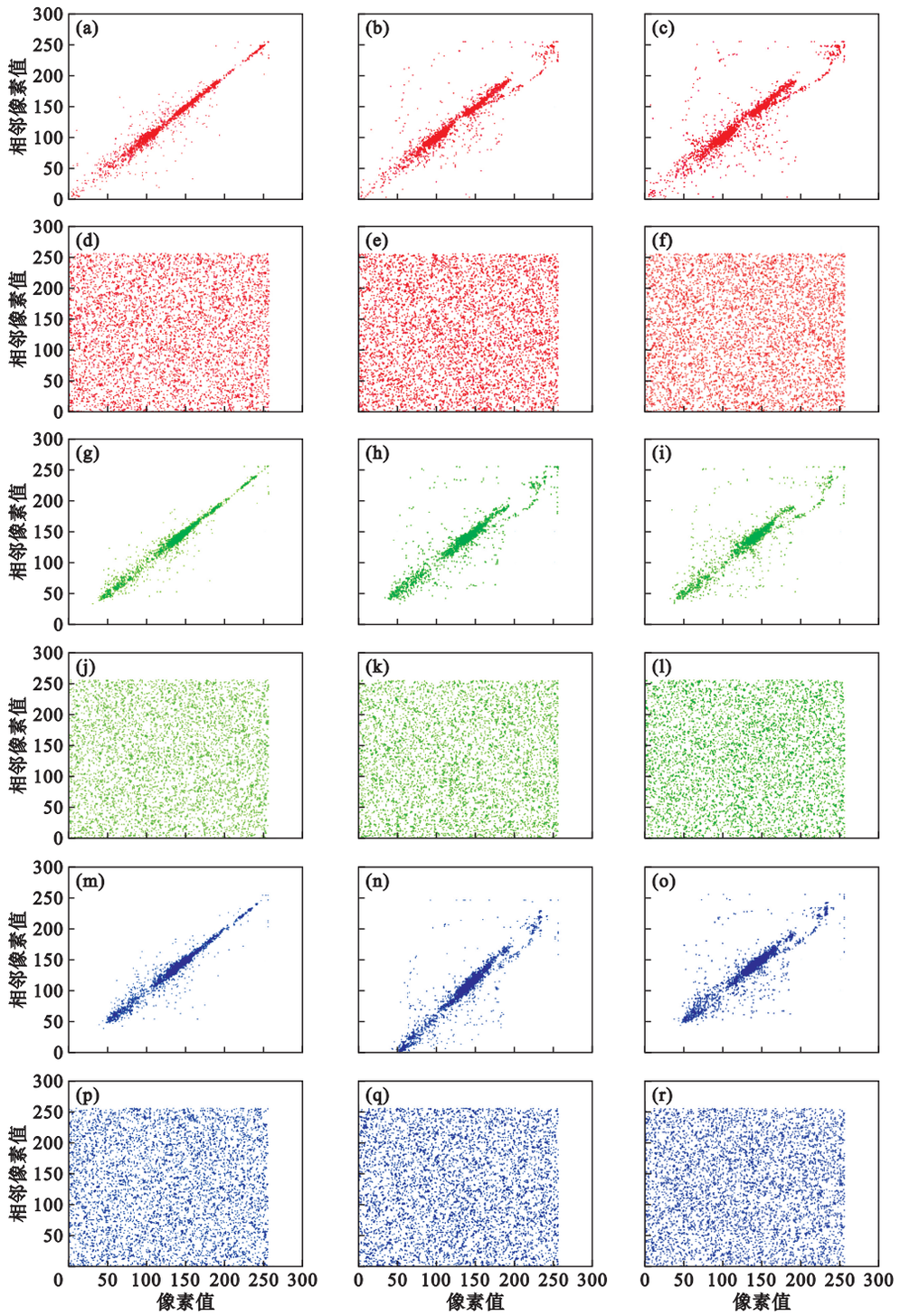


图13 明文图像和密文图像的相邻像素相关性对比

Fig. 13 Comparison of adjacent pixel correlation between plain image and encrypted image

(a)—明文图像R通道水平方向;(b)—明文图像R通道垂直方向;(c)—明文图像R通道对角线方向;(d)—密文图像R通道水平方向;(e)—密文图像R通道垂直方向;(f)—密文图像R通道对角线方向;(g)—明文图像G通道水平方向;(h)—明文图像G通道垂直方向;(i)—明文图像G通道对角线方向;(j)—密文图像G通道水平方向;(k)—密文图像G通道垂直方向;(l)—密文图像G通道对角线方向;(m)—明文图像B通道水平方向;(n)—明文图像B通道垂直方向;(o)—明文图像B通道对角线方向;(p)—密文图像B通道水平方向;(q)—密文图像B通道垂直方向;(r)—密文图像B通道对角线方向.

为了进一步检验本文算法对相邻像素点的置乱程度,分别计算了Female,Lena和Baboon的密文图像在3个方向上的相邻像素相关系数,并与其他算法进行了比较,结果如表3所示.从表中可以看出,相较于其他算法,本文算法加密得到的密文图像的相邻像素相关系数更接近于0,这说明本文采用的骑士混沌巡游方法,通过混沌伪随机序列控制每一步的行、列步长,突破了传统骑士日字形走法的限制,增强了置乱效果.

表3　各加密算法关于相邻像素相关系数对比

Table 3　Comparison of adjacent pixel correlation coefficients among different encryption algorithms

图像	算法	相关系数		
		水平方向	垂直方向	对角线方向
Female	文献[7]	−0. 015 6	−0. 000 3	−0. 012 4
	本文	−0. 001 05	0. 001 14	−0. 001 02
Lena	文献[23]	0. 003 0	0. 021 2	0. 121 2
	本文	0. 000 36	−0. 000 09	0. 002 07
Baboon	文献[16]	0. 003 1	0. 002 2	0. 003 1
	文献[17]	0. 002 0	0. 002 1	−0. 005 5
	文献[18]	0. 001 613	0. 001 149	−0. 004 630
	本文	0. 000 742	−0. 000 458	0. 002 814

3.3.5　信息熵分析

信息熵是对不确定性的度量.在加密领域,加密图像的信息熵越接近于8,说明加密后的图像越接近均匀分布,攻击者从加密图像中获取原始信息的难度就越大.由表4可以看出,使用本算法得到的加密图像相较于其他文献算法,其信息熵的值更高.

3.3.6　置乱效率分析

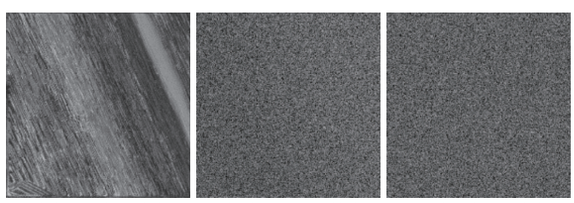
为了对比传统骑士巡游方法和本文提出的骑士混沌巡游方法在图像加密时的置乱效率,本文以Lena图像为例进行了仿真验证.其中,分别采用传统方法进行1轮和10轮置乱,以及使用本文的骑士混沌巡游方法进行1轮置乱,所得到的置乱图像如图14所示;并从时间和相邻像素相关系数两方面对置乱效率进行对比分析,结果如表5所示.可以看出,本文设计的骑士混沌巡游方法,仅需进行1轮置乱,便可以实现对图像像素点的全局置乱,克服了传统骑士巡游方法单轮置乱不彻底,需要进行多轮置乱才能保证效果的局限性.

表4　信息熵对比

Table 4　Comparison of information entropy

图像	算法	信息熵
Female	文献[7]	7. 999 2
	本文	7. 999 2
Lena	文献[23]	
	本文	7. 999 2
Baboon	文献[16]	7. 997 2
	文献[17]	7. 996 8
	文献[18]	7. 997 6
	本文	7. 999 3

注:文献[23]未给出Lena密文图像的信息熵指标.



1轮传统骑士巡游　10轮传统骑士巡游　1轮骑士混沌巡游

图14　置乱图像对比

Fig. 14　Comparison of scrambled images

表5　置乱效率对比

Table 5　Comparison of scrambling efficiency

变量	1轮骑士混沌巡游	1轮传统骑士巡游	10轮传统骑士巡游
时间/s	0. 785 6	1. 144 5	12. 542 8
相邻像素相关系数水平方向	0. 004 153	0. 295 079	0. 010 196
相邻像素相关系数垂直方向	−0. 004 222	0. 313 469	0. 006 403
相邻像素相关系数对角线方向	−0. 001 468	0. 311 955	0. 010 974

3.3.7　抗攻击能力分析

为全面评估本文提出的加密算法在实际场景下的安全性,本节按照噪声攻击、裁剪攻击、选择明文攻击与已知明文攻击4个部分,以Female图像为对象进行实验分析.

1)噪声攻击测试.分别对密文图像添加不同强度的椒盐噪声与高斯噪声后解密,得到的解密图像如图15所示.可以看出:当椒盐噪声密度为0.01时,解密图像仅出现少量黑白噪点,图像内容完整可辨,椒盐噪声密度增至0.05时,噪点增多,但图像主要轮廓与结构依然清晰.对于高斯噪声方差为0.001及0.01时,解密图像出现一定程度的模糊,但主体信息如人物面部、衣物纹理等仍可识别.

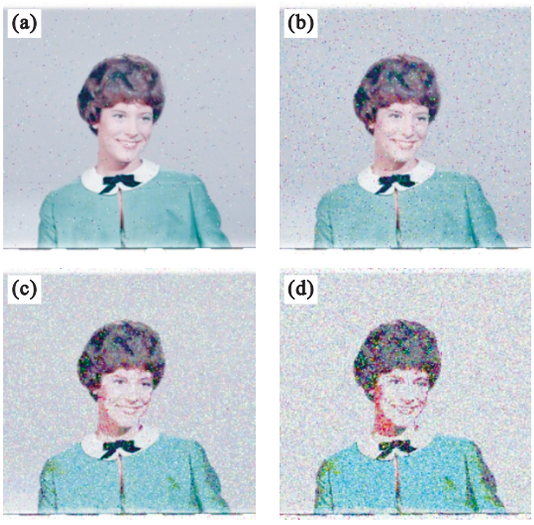


图 15 受不同噪声攻击后的解密图像

Fig. 15 Decrypted images under different noise attacks

(a)—椒盐噪声密度 0.01;(b)—椒盐噪声密度 0.05;(c)—高斯噪声方差 0.001;(d)—高斯噪声方差 0.01.

结果表明,本文提出的方法对椒盐噪声具有较好的抗攻击能力,对高斯噪声也具备一定的抵抗能力.

2) 裁剪攻击测试.为验证算法对数据丢失的鲁棒性,分别对密文图像进行左上角 12.5%、中心 25%、右侧 50% 以及随机 30 像素×30 像素块的裁剪,然后解密,结果如图 16 所示.图中从上至下依次为原始密文裁剪后图像和对应解密图像.可以看出,对于局部裁剪,解密后的图像仍能保留主要视觉信息.即使密文丢失比例达 50%,本文提出的骑士混沌巡游方法也能确保图像核心内容不被完全破坏,具有较强的抗裁剪攻击能力.

3) 选择明文攻击测试.选择明文攻击通常通过观察明文微小变化对密文的影响来评估,采用 2 个标准指标 NPCR 和 UACI 进行分析,在 Female 图像上测试得到 NPCR 和 UACI 的值分别为 99.606 1%,33.446 8%,两者均非常接近理论理想值.这说明加密方法对明文具有极高的敏感性,能够有效抵抗选择明文攻击.

4) 已知明文攻击分析.已知明文攻击是假设攻击者获得若干明密文对,以此破解密钥或加密机制.在本文提出的方法中,混沌系统的初值和控制参数由用户密钥决定,骑士巡游的起始点及移动路径高度依赖于混沌序列,而混沌序列依赖于混沌系统与密钥的复杂迭代.即使攻击者掌握一对或多对明密文对,由于混沌系统的强非线性和庞大的密钥空间(2^{625}),也难以反推出密钥.此外,上述 NPCR 和 UACI 结果也间接证明了明文与密文之间不存在可线性拟合的映射关系,因此该方法具备抵抗已知明文攻击的能力.

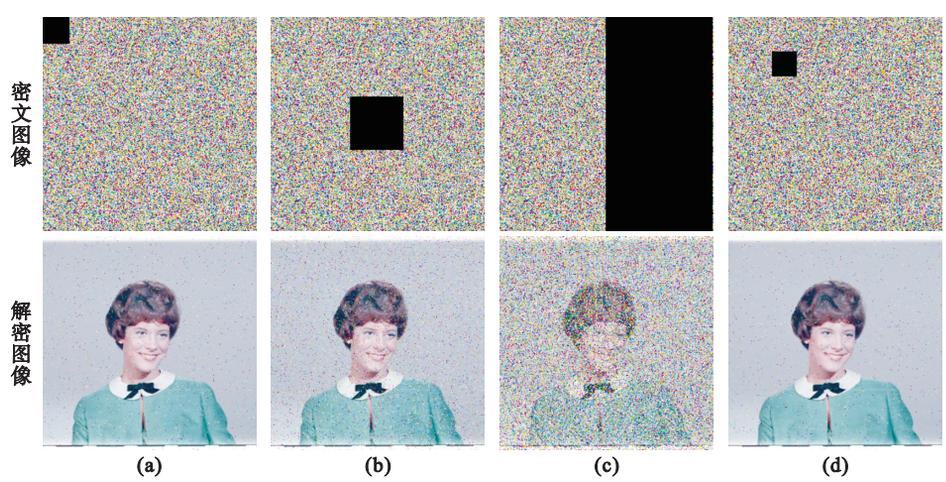


图 16 受不同比例裁剪攻击后的解密图像

Fig. 16 Decrypted images under cropping attacks with different proportions

(a)—裁剪左上角 12.5%;(b)—裁剪中心 25%;(c)—裁剪右侧 50%;(d)—裁剪 30 像素×30 像素块.

4 结 论

1) 本文研究了 1 种可用于图像加密的骑士混沌巡游方法,旨在解决传统骑士巡游因日字形移动规则限制而导致的图像置乱程度不高的问题.该方法将混沌伪随机序列引入巡游过程,利用生成的混沌整数伪随机序列动态控制骑士在行与列方向上的移动步长,实现不规则巡游.

2) 设计了 1 种基于骑士混沌巡游的图像加密算法:利用三维 Logistic 混沌映射生成 3 个混沌整数伪随机序列,其中 2 个序列用于控制巡游路

径生成以实现像素置乱,另 1 个序列用于扩散操作以改变像素值.

3）通过 MATLAB 仿真,验证了该算法具有更优的性能指标,并通过分析相邻像素相关系数、信息熵、抗攻击能力等,对比 1 轮骑士混沌巡游与不同轮传统骑士巡游在置乱后的效果,证实了本文提出的骑士混沌巡游方法可增强置乱效果和安全性,提高加密效率.

参考文献:

[1] Li W F, Ge B, Xia C X, et al. Image encryption algorithm for 3D-hyperchaotic systems driven by nonlinear feedback mechanism [J]. *Signal, Image and Video Processing*, 2025, 19(12): 984.

[2] Alnabhan M, Alsaraireh S, AbuHour Y, et al. Lightweight and hybrid image encryption approach: dynamic anchor blocks selection [J]. *Cluster Computing*, 2025, 28(16): 1050.

[3] Wang J Q, Zhang M, Tong X J, et al. An image compression encryption scheme based on chaos and SPECK-DCT hybrid coding [J]. *Nonlinear Dynamics*, 2024, 112(11): 9581-9602.

[4] Nan Y, Wo Y. RIE-GAN: a retrievable image encryption method based on GAN [J]. *Digital Signal Processing*, 2025, 163: 105202.

[5] Jiang D L, Bai S, Dong W M. An image encryption algorithm based on knight's tour and slip encryption-filter [C]//2008 International Conference on Computer Science and Software Engineering. Wuhan: IEEE, 2008: 251-255.

[6] Singh M, Kakkar A, Singh M. Image encryption scheme based on knight's tour problem [J]. *Procedia Computer Science*, 2015, 70: 245-250.

[7] Kumar J, Nirmala S. A novel and efficient method based on knight moves for securing the information contents of images: a parallel approach [J]. *Journal of Information Security and Applications*, 2016, 30: 105-117.

[8] Mahmood A S, Rahim M S M. Novel method for image security system based on improved SCAN method and pixel rotation technique [J]. *Journal of Information Security and Applications*, 2018, 42: 57-70.

[9] Bisht K, Deshmukh M. Encryption algorithm based on knight's tour and n-neighbourhood addition [C]//2020 7th International Conference on Signal Processing and Integrated Networks (SPIN). Noida: IEEE, 2020: 31-36.

[10] 兰红, 方毅. 基于Arnold变换的改进骑士巡游图像加密算法[J]. 通信技术, 2018, 51(7): 1663-1670.
(Lan Hong, Fang Yi. Modified knight's tour image encryption algorithm based on Arnold transform [J]. *Communications Technology*, 2018, 51(7): 1663-1670.)

[11] Gao X Y, Mou J, Banerjee S, et al. Color-gray multi-image hybrid compression-encryption scheme based on BP neural network and knight tour [J]. *IEEE Transactions on Cybernetics*, 2023, 53(8): 5037-5047.

[12] Fridrich J. Image encryption based on chaotic maps [C]// 1997 IEEE International Conference on Systems, Man and Cybernetics. Orlando: IEEE, 1997: 1105-1110.

[13] Geng S T, Li J H, Zhang X C, et al. An image encryption algorithm based on improved Hilbert curve scrambling and dynamic DNA coding[J]. *Entropy*, 2023, 25(8): 1178.

[14] El Ghouate N, Tahiri M A, Bencherqui A, et al. A high-entropy image encryption scheme using optimized chaotic maps with Josephus permutation strategy [J]. *Scientific Reports*, 2025, 15: 29439.

[15] Ning X Y, Dong Q, Zhou S H, et al. Construction of new 5D Hamiltonian conservative hyperchaotic system and its application in image encryption [J]. *Nonlinear Dynamics*, 2023, 111(21): 20425-20446.

[16] He C C, Chen Z, Wang L J, et al. An algorithm based on 6D fractional order hyperchaotic system and knight tour algorithm to encrypt image [J]. *Physica Scripta*, 2024, 99(5): 055205.

[17] Ullah S, Liu X G, Waheed A, et al. Novel grayscale image encryption based on 4D fractional-order hyperchaotic system, 2D Henon map and knight tour algorithm [J]. *Physica Scripta*, 2024, 99(9): 095248.

[18] Deng X, Chen Z, Long B F, et al. An image encryption algorithm based on a novel 4D hyperchaotic system and improved knight's tour scrambling algorithm [J]. *Physica Scripta*, 2025, 100(4): 045208.

[19] Ghosh D, Bhaduri U. A simple recursive backtracking algorithm for knight's tours puzzle on standard 8×8 chessboard [C]//2017 International Conference on Advances in Computing, Communications and Informatics (ICACCI). Udupi: IEEE, 2017: 1195-1200.

[20] Parberry I. An efficient algorithm for the knight's tour problem [J]. *Discrete Applied Mathematics*, 1997, 73(3): 251-260.

[21] Chia G L, Ong S H. Generalized knight's tours on rectangular chessboards [J]. *Discrete Applied Mathematics*, 2005, 150(1/2/3): 80-98.

[22] Ye G D, Jiao K X, Pan C, et al. An effective framework for chaotic image encryption based on 3D logistic map [J]. *Security and Communication Networks*, 2018(1): 8402578.

[23] 潘营利, 何冰, 王英. 基于骑士巡游的改进图像加密算法[J]. 计算机与数字工程, 2016, 44(1): 136-140.
(Pan Ying-li, He Bing, Wang Ying. Image encryption algorithm based on improved knight tour [J]. *Computer & Digital Engineering*, 2016, 44(1): 136-140.)