

# 一种手指静脉特征图像加密方法的研究

王萌<sup>1</sup>, 魏韶锋<sup>2\*</sup>, 刘亚丽<sup>2</sup>, 钱磊<sup>2</sup>, 曹敏<sup>2</sup>, 高艺娟<sup>2</sup>, 陈暄<sup>3</sup>

<sup>1</sup>南昌医学院学科建设办公室, 江西 南昌

<sup>2</sup>南昌医学院药学院, 江西 南昌

<sup>3</sup>浙江工业职业技术学院, 设计与艺术分院, 浙江 绍兴

收稿日期: 2023年9月5日; 录用日期: 2023年10月12日; 发布日期: 2023年10月31日

## 摘要

针对当前手指静脉图像加密中存在信息丢失, 效果弱的缺点, 提出了一种新的加密策略。首先, 采用图像平滑器获得静脉图像大小以确定图像范围, 其次, 利用明暗区域的方法获取图像代表性的特征信息, 最后对图像的密钥信息和明文分别使用二次Logistic映射和Baker进行融合的加密, 提高了图像加密的安全性。仿真实验中该算法相关性分析三个指标均有明显的提升, 同时相比于一维混沌和均匀非退化离散混沌在统计分析方面平均提高了12.7%和5.6%, 验证了本文算法在图像加密方面的效果。

## 关键词

手指静脉, 图像加密, 混沌映射

# Research into Encryption Based on Finger Vein Feature Image

Meng Wang<sup>1</sup>, Shaofeng Wei<sup>2\*</sup>, Yali Liu<sup>2</sup>, Lei Qian<sup>2</sup>, Min Cao<sup>2</sup>, Yijuan Gao<sup>2</sup>, Xuan Chen<sup>3</sup>

<sup>1</sup>Discipline Construction Office of Nanchang Medical College, Nanchang Jiangxi

<sup>2</sup>Department of Pharmacy of Nanchang Medical College, Nanchang Jiangxi

<sup>3</sup>College of Design and Art of Zhejiang Industry Polytechnic College, Shaoxing Zhejiang

Received: Sep. 5<sup>th</sup>, 2023; accepted: Oct. 12<sup>th</sup>, 2023; published: Oct. 31<sup>st</sup>, 2023

## Abstract

Aiming at the shortcomings of information loss and weak effect in the current finger vein image encryption, a new encryption strategy is proposed. Firstly, an image smoother is used to obtain

\*通讯作者。

文章引用: 王萌, 魏韶锋, 刘亚丽, 钱磊, 曹敏, 高艺娟, 陈暄. 一种手指静脉特征图像加密方法的研究[J]. 软件工程与应用, 2023, 12(5): 714-721. DOI: 10.12677/sea.2023.125069

the size of the vein image to determine the image range, secondly, the method of bright and dark regions is used to obtain the representative feature information of the image, and finally, the key information and the plaintext of the image are encrypted by using the quadratic Logistic mapping and Baker fusion respectively, which improves the security of the image encryption. In the simulation experiments, the algorithm correlation analysis of the three indicators are significantly improved, while compared with the one Dimensional Chaotic and Uniform Non-Degeneracy Discrete Chaotic in the statistical analysis of an average of 12.7% and 5.6%, which verifies the effectiveness of this paper's algorithm in the image encryption.

## Keywords

Finger Vein, Image Encryption, Chaotic Mapping

Copyright © 2023 by author(s) and Hans Publishers Inc.

This work is licensed under the Creative Commons Attribution International License (CC BY 4.0).

<http://creativecommons.org/licenses/by/4.0/>



Open Access

## 1. 引言

随着 5G 网络应用范围越来越广泛,人们使用网络进行信息传递的频率越来越高。如何更加安全的在网络中传输图像信息是目前研究的重点[1]。

文献[2]提出基于单通道加扰、扩散混沌系统的多图像加密算法,仿真实验的性能说明该算法既具有出色的加密速度和安全性能;文献[3]提出新的混沌加密图像策略,它是由正弦图、正切函数和第一类切比雪夫多项式派生出来的,仿真实验表明该算法在加密性能和算法复杂性方面具有不错的效果;文献[4]提出使用块扰乱和混沌的彩色图像加密策略,该策略将子图像和区块中的像素排列改变并在子图像中进行加扰,扰乱的图像利用逻辑图进行扩散得到加密的图像,实验结果表明提出的算法在加密彩色图像方面具有良好的性能;文献[5]提出具有大混沌空间的分数一维混沌图,该图结合了替换和置换阶段来同时修改像素的位置和值,仿真和实验分析证明了该方案具有很高的加密性能;文献[6]提出混沌系统生成算法,实验结果表明该算法在加密的图像在密钥敏感性、明文敏感性、鲁棒性、相关性和信息熵方面具有良好的加密特性。文献[7]提出基于混沌系统的快速、高效的多图像加密方法,它将合并后的图像的子块是通过应用组合混沌系统产生的混沌序列进行替换,结果表明能够有效地抵御各种攻击;文献[8]提出基于 PWLCM 混沌图和哈希算法的图像加密算法,仿真实验说明该算法在加密和解密时间很短;文献[9]提出了一种基于位平面和混沌的多图像加密算法,该算法具有加密效果好、加密效率高、密钥空间大、密钥敏感、抗统计攻击、暴力攻击能力强等优点;文献[10]提出了一种将小波变换与改进的二维 Logistic 混沌映射相结合的图像加密算法。仿真结果表明该加密方式使密文敏感度高,能够有效抵御统计分析攻击、穷举攻击和差分攻击。

以上学者对于图像加密的研究取得了不同程度的成果,总结以上这些算法,我们发现这些算法加密过程需要消耗大量的实际时间,同时都是直接对图像进行加密处理,并没有选取主要的图像加密信息,造成了加密过程的冗余,本文在现有的图像加密成果的基础上,通过对手指静脉图像构建图像平滑器获得图像大小,并通过明亮区域的特征获取,最后采用 Logistic 映射和 Baker 变换的混合加密方式,仿真实验验证了算法的有效性。

## 2. 手指静脉图像的获取和处理

### 2.1. 构建图像平滑器

常见的手指静脉图像中固有的单一结构是无法适应于网络进行传输的，因此，我们通过构建图像平滑器来完成有关图像的处理，我们选择了4个4×4的结构单元并将其进行合并，从而形成了8×8的图像平滑器结果。其结构如图1所示。

0	1	0	0	1	0	1	1
1	1	1	1	0	1	0	0
1	0	1	1	0	0	1	0
0	0	0	1	0	0	0	1
0	0	0	1	0	0	1	0
1	1	1	0	0	1	1	0
0	1	0	0	0	0	1	0
1	0	0	0	0	1	1	1

Figure 1. 8×8 image smoother

图 1. 8×8 的图像平滑器

在图 1 中，我们发现通过图像平滑器能够对手指静脉的图像  $f$  进行扩充运算并获得 4 个子图像  $f_a, f_b, f_c, f_d$  将其通过一定的加权方式进行图像的重构获得最终的图像特征，而使用  $\alpha, \beta, \kappa, \rho$  表达上述 4 个子图像的权重数值并且它们的和为 1。因此表达式如(1)所示。

$$f = \alpha \times f_1 + \beta \times f_2 + \kappa \times f_3 + \rho \times f_4 \quad (1)$$

### 2.2. 图像明暗区域特征提取

本文采用白变换和黑变换进行图像方面的特征提取，设计一种尺寸递增的结构序列  $\{\varepsilon_1, \varepsilon_2, \dots, \varepsilon_i\}$ 。

1) 白变换公式：

$$\text{White hat}_i = f \times (1 - \varepsilon_i) \quad (2)$$

公式(2)中  $\text{White hat}_i$  表示通过  $\varepsilon_i$  尺寸对手指静脉图像  $f$  在第  $i$  维度进行白变换。 $\text{White hat}_{i(i-1)}$  表示在手指静脉图像  $f$  在两个相邻区域尺寸上的明区域的变换，表达式如(3)所示，提取手指静脉图像中的明区域  $f_w$  如公式(4)所示，其中， $k$  表示维度

$$\text{White hat}_{i(i-1)} = \text{White hat}_i \cap \text{White hat}_{i-1} \quad (3)$$

$$f_w = \sum_{i=1}^k \frac{\text{White hat}_{i(i-1)}}{k(k-1)} \quad (4)$$

2) 黑变换公式：

$$\text{Black hat}_i = f \times (\varepsilon_i - 1), \quad (5)$$

公式(5)中的  $\text{Black hat}_i$  表示通过  $\varepsilon_i$  对手指静脉图像  $f$  在第  $i$  维度上进行黑变换。 $\text{Black hat}_{i(i-1)}$  表示在手指静脉图像  $f$  在两个相邻区域尺寸上的暗区域的变换，公式如(6)所示，提取手指静脉图像中的暗区域  $f_w$  如公式(7)所示，其中， $k$  表示维度。

$$\text{Black hat}_{i(i-1)} = \text{Black hat}_i \cap \text{Black hat}_{i-1} \quad (6)$$

$$f_B = \sum_{i=1}^k \frac{\text{Black hat}_{i(i-1)}}{k(k-1)} \quad (7)$$

### 3. 基于混沌手指静脉图像加密设计

为了更好地获得手指静脉图像的加密效果，我们在本文中采用了混沌映射和 Baker 变换方式进行融合处理，融合后从而获得较好的效果。在密钥方面采用混沌映射进行加密，原始手指静脉图像通过 Baker 进行置换。

#### 3.1. 二维 Logistic 映射

二维 Logistic 映射是一种非线性动力系统，以混沌理论和非线性动力学的研究为基础，表达式如下所示：

$$\begin{cases} x_{n+1} = x_n + h(x_n + y_n - x_n^2) \\ y_{n+1} = y_n + h(y_n + x_n - y_n^2) \end{cases} \quad (8)$$

$x_n$  和  $y_n$  是第  $n$  个迭代步骤中的  $x$  和  $y$  值。 $h$  为混沌系数，当  $h \in [0.653, 0.686]$  的时候，Logistic 处于二维混沌状态。

#### 3.2. Baker 变换

Baker 变换基本思想是将二维平面分成小方块，并按照一定的规则进行重排或混合。它是数据置乱的一种方式。二维连续的 Baker 变换的表达式如(9)。

$$\begin{cases} B(x_{n+1}, y_{n+1}) = k\left(2x_n, \frac{y_n}{2}\right), & x_n \in [0, 1/2] \\ B(x_{n+1}, y_{n+1}) = k\left(2x_n - 1, \frac{y_n + 1}{2}\right), & x_n \in [1/2, 1] \end{cases} \quad (9)$$

其中  $(x_n, y_n)$  记录着原始数据的位置， $(x_{n+1}, y_{n+1})$  记录着置乱后的数据位置。 $k(x, y)$  表示变换函数。

因此，上述混合加密序列如图 2 所示。

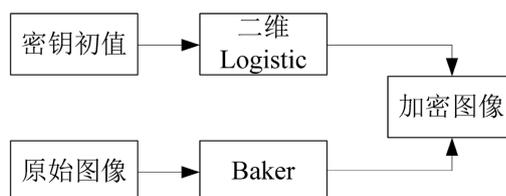


Figure 2. Hybrid encryption sequence of both  
图 2. 二者混合加密序列

### 4. 仿真实验

为了更好的进一步验证本文算法在加密过程中的效果，我们在硬件环节中选择了 CPU 为酷睿 I5，内存为 16GDDR3，硬盘容量为 2T，仿真软件为 Matlab2010，操作系统选择 Windows10。从相关系分析和统计分析两个方面进行分析。

#### 4.1. 像素相关性分析

像素相关性是衡量加密效果的重要组成部分，这是因为很多图像都会包括一些冗余的信息，这些信息存在一定的相关性，因此为了验证本文算法的加密效果，我们选择 100 组(每一组包括手指静脉图像和加密后的图像)验证加密后的图像在水平、垂直和对角线方向的像素相关性结果。公式如(10)~(13)所示。其中  $x_k$  表示像素个体， $E(x)$  表示变量期望值， $Cov$  表示为协方差， $(x, y)$  表示手指静脉图像中的相邻像素点的灰度值， $N$  为挑选的像素个数。

$$E(x) = \frac{1}{N} \sum_{k=1}^N x_k \quad (10)$$

$$D(x) = \frac{1}{N} \sum_{k=1}^N (x_k - E(x))^2 \quad (11)$$

$$Cov(x, y) = \frac{1}{N} \sum_{k=1}^N (x_k - E(x))(y_k - E(y)) \quad (12)$$

$$r(x, y) = \frac{|Cov(x, y)|}{\sqrt{D(x)}\sqrt{D(y)}} \quad (13)$$

表 1 展示了加密前后的两种图像的相关系数，从表中的数值结果来看，相比于采集的时候接近 1 的像素值对比，加密图在三个方向的数值都接近 0，说明了手指静脉特征通过加密已经扩散到随机加密中，同时从数据数值的对比来看，加密后的像素相关性的效果具有明显的改进，进一步说明了本文算法的效果。表 2 显示了两种图像算法在时间复杂度的对比情况，从表中的数据结果来看，加密后的时间复杂度相比于原始手指静脉采集平均降低 32.18%，这说明了本文算法的加密效果是显著的。图 3~6 进一步显示了本文算法的灰度值的对比情况。从图中的结果来看，本文算法在三个方向的加密效果中呈现的像素点都比较分散，说明了通过本文算法的处理后，图像的加密效果得到了进一步提高，能够有效的处理好图像的加密效果。

**Table 1.** Correlation of two neighboring pixels of captured vein map and encrypted map

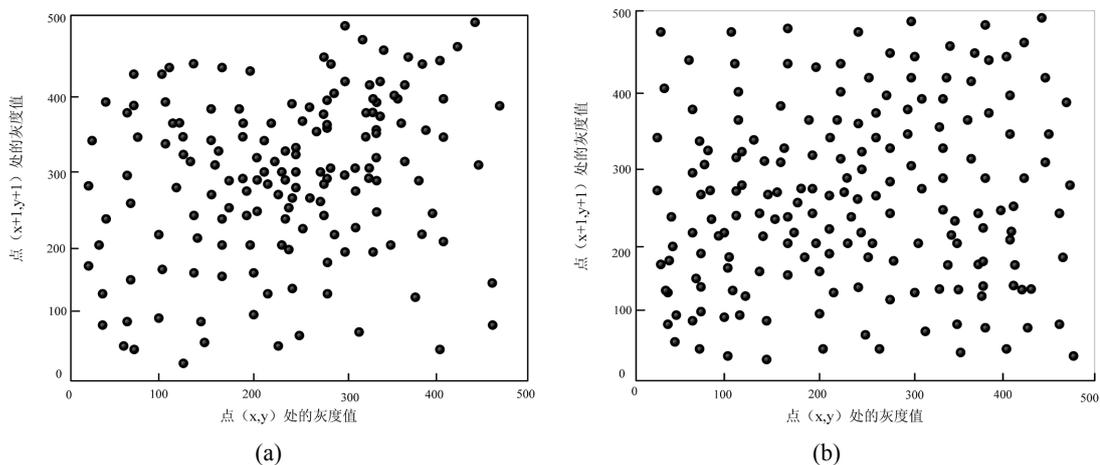
**表 1.** 采集静脉图与加密图的两相邻像素相关性

方向	手指静脉采集图	加密图
水平方向	0.9132	0.0034
垂直方向	0.8915	0.0029
对角方向	0.9275	0.0023

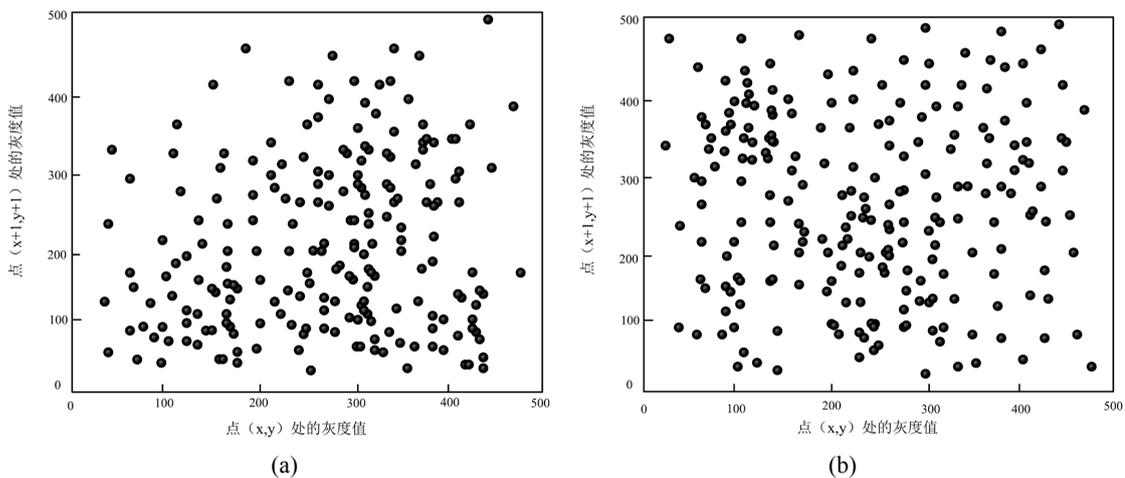
**Table 2.** Comparison of time complexity of capturing vein maps and encrypted maps

**表 2.** 采集静脉图与加密图的时间复杂度比较

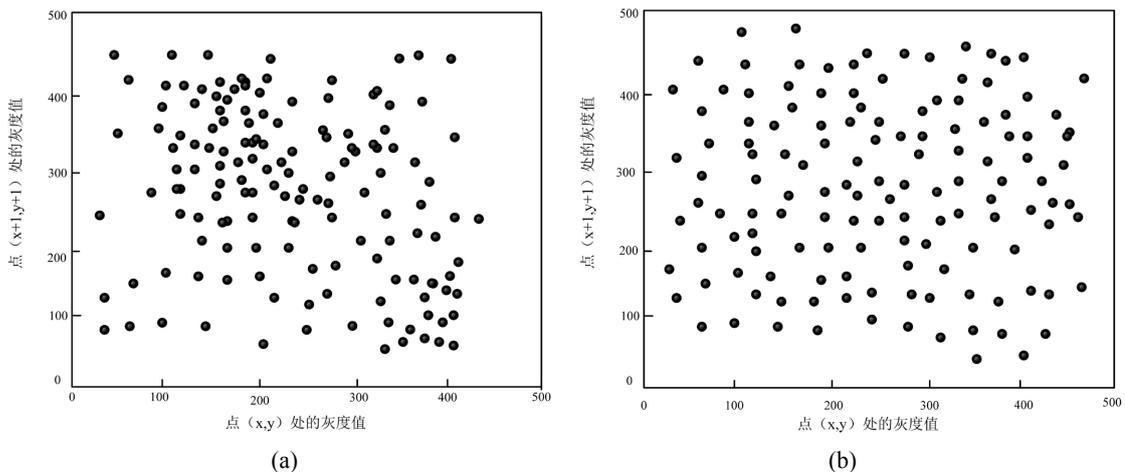
方向	手指静脉采集图(%)	加密图(%)
水平方向	75.25	38.15
垂直方向	66.45	36.35
对角方向	91.37	64.74



**Figure 3.** (a) Acquisition of image diagonal; (b) Encrypted image diagonally  
**图 3.** (a) 采集图像对角; (b) 加密图像对角



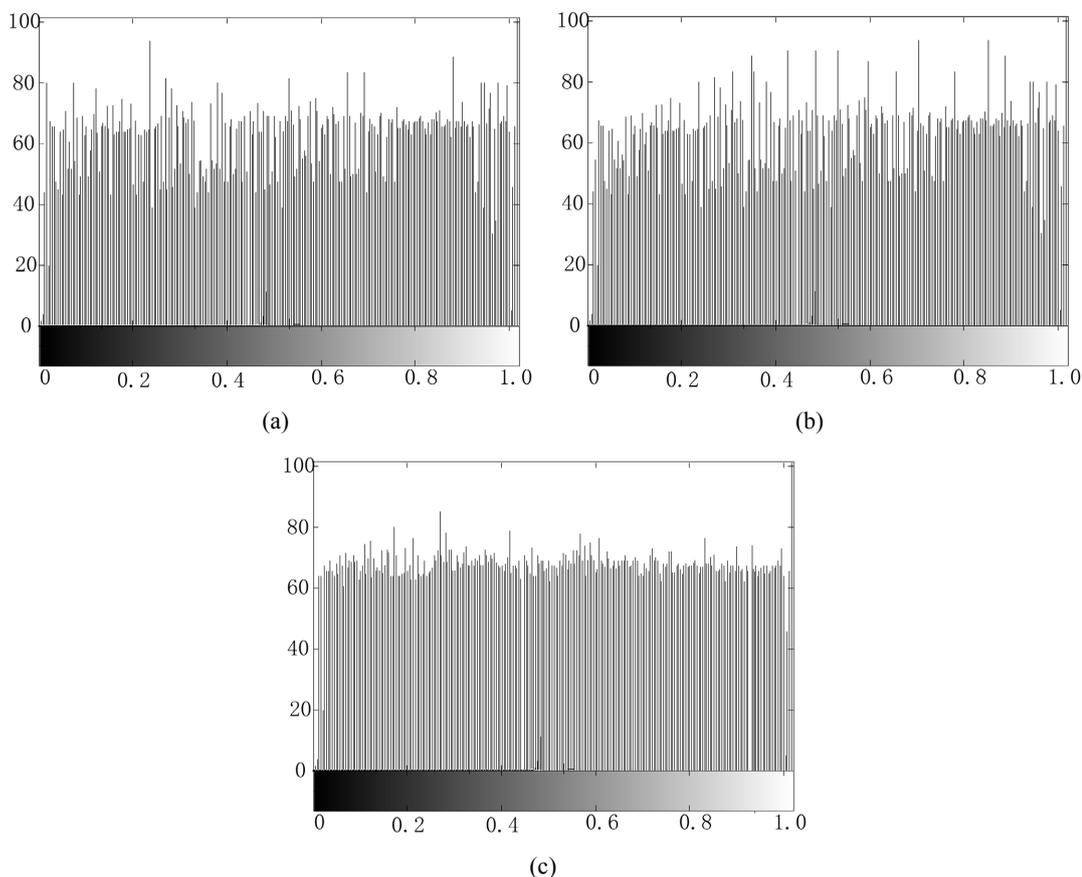
**Figure 4.** (a) Acquisition of image level; (b) Encrypted image level  
**图 4.** (a) 采集图像水平; (b) 加密图像水平



**Figure 5.** (a) Acquisition of images vertical; (b) Encrypted image vertically  
**图 5.** (a) 采集图像垂直; (b) 加密图像垂直

## 4.2. 统计分析

在统计分析中,我们选择了文献[5]和文献[6]两种较新的算法作为对比算法进行验证,比较结果如图6所示,从图中的对比结果发现文献[5]的统计分析数值结果多次出现不同的振幅,文献[6]的统计分析结果也同样出现了震荡的情况,说明了这两种算法在加密方面还存在不稳定的因素,说明了加密效果有待进一步提高,而本文算法的灰度值结果具有稳定的效果,说明了该算法通过明暗区域的特征提取和采用混沌映射进行密钥加密和原始手指静脉图像通过 Baker 进行置换的效果是明显。总体来看,本文算法相比于文献[5]和文献[6]在统计分析方面平均提高了 12.7%和 5.6%。



**Figure 6.** (a) Gray scale image of finger vein from literature [5]; (b) Gray scale image of finger vein from literature [6]; (c) Gray scale image of finger vein for this paper's algorithm

**图 6.** (a) 文献[5]的手指静脉图像灰度图; (b) 文献[6]的手指静脉图像灰度图; (c) 本文算法的手指静脉图像灰度图

## 5. 结束语

针对手指静脉图像加密存在的加密效果弱的问题,我们对手指静脉图像亮暗区域特征进行提取,其次,使用 Logistic 映射和 Baker 变换的混合加密方式对密钥和原始图像进行不同程度的加密。实验说明了本文算法在相关系分析和统计分析等方面结果具有较好的加密效果。

## 课题来源

江西省教育厅科学技术研究项目资助(GJJ2203513); 江西省教育厅科学技术研究项目资助(GJJ2203522)。

## 参考文献

- [1] Singh, M. and Singh, K.A. (2022) A Comprehensive Survey on Encryption Techniques for Digital Images. *Multimedia Tools and Applications*, **82**, 11155-11187. <https://doi.org/10.1007/s11042-022-12791-6>
- [2] Gao, X., Mou, J., Xiong, L., et al. (2022) A Fast and Efficient Multiple Images Encryption Based on Single-Channel Encryption and Chaotic System. *Nonlinear Dynamics*, **108**, 613-636. <https://doi.org/10.1007/s11071-021-07192-7>
- [3] Belazi, A., Kharbech, S., Aslam, M.N., et al. (2022) Improved Sine-Tangent Chaotic Map with Application in Medical Images Encryption. *Journal of Information Security and Applications*, **66**, Article ID: 103131. <https://doi.org/10.1016/j.jisa.2022.103131>
- [4] Hosny, K.M., Kamal, S.T. and Darwish, M.M. (2022) A Color Image Encryption Technique Using Block Scrambling and Chaos. *Multimedia Tools and Applications*, **81**, 505-525. <https://doi.org/10.1007/s11042-021-11384-z>
- [5] Talhaoui, M.Z. and Wang, X. (2021) A New Fractional One Dimensional Chaotic Map and Its Application in High-Speed Image Encryption. *Information Sciences*, **550**, 13-26. <https://doi.org/10.1016/j.ins.2020.10.048>
- [6] Liu, X., Tong, X., Wang, Z., et al. (2022) Uniform Non-Degeneracy Discrete Chaotic System and Its Application in Image Encryption. *Nonlinear Dynamics*, **108**, 653-682. <https://doi.org/10.1007/s11071-021-07198-1>
- [7] Zarebnia, M., Pakmanesh, H. and Parvaz, R. (2019) A Fast Multiple-Image Encryption Algorithm Based on Hybrid Chaotic Systems for Gray Scale Images. *Optik*, **179**, 761-773. <https://doi.org/10.1016/j.ijleo.2018.10.025>
- [8] Bisht, A., Dua, M. and Dua, S. (2019) A Novel Approach to Encrypt Multiple Images Using Multiple Chaotic Maps and Chaotic Discrete Fractional Random Transform. *Journal of Ambient Intelligence and Humanized Computing*, **10**, 3519-3531. <https://doi.org/10.1007/s12652-018-1072-0>
- [9] Zhang, L. and Zhang, X. (2020) Multiple-Image Encryption Algorithm Based on Bit Planes and Chaos. *Multimedia Tools and Applications*, **79**, 20753-20771. <https://doi.org/10.1007/s11042-020-08835-4>
- [10] 李立, 向菲. 基于小波变换的混沌图像加密算法[J]. 计算机仿真, 2023, 40(7): 200-204.