基于整数小波变换的图像加密算法及实验研究

李雪倩，王奕泽*
青海理工学院，青海 西宁 810000

DOI: 10.61369/TACS.2026080046

摘　　要： 研究了一种基于整数小波变换的快速图像加密实验算法。在该密码系统中，通过整数 S 变换分解原始图像，提取出低频系数和高频系数中的所有近似信息，并根据有符号补码表示原理压缩明文图像；在算法设计中，提出了基于分段线性映射的密码体制，采用了明文相关的一次置乱与两次扩散。

关 键 词： 图像加密；整数 S 变换；分段线性；置乱与扩散

A Image Encryption Scheme Based on Integer Wavelet

Li Xueqian, Wang Yize*
Qinghai Institute of Technology, Xining, Qinghai 810000

Abstract: This paper proposes a new image encryption scheme based on integer wavelet transform. The original image is decomposed by integer wavelet S transform, and the approximate information both in the low-frequency coefficients and high-frequency coefficients is extracted, then the plaintext image is compressed according to the principle of signed complement. In the design of the scheme, symmetrical key streams for encryption are generated by Piecewise linear map and S-box .The algorithm uses one-time scrambling related to the plaintext and two time diffusions.

Keywords: information security ; image encryption; integer s transform; piecewise linear map; scrambling and diffusion

随着信息技术的发展，图像加密已成为信息安全领域中一个热门的研究课题。由于混沌系统具有初值和参数极端敏感性等特性，借助于混沌系统生成加密图像的密码流取得了大量可喜的研究成果[1-4]。在现有的整数小波算法设计中，置乱和扩散模块仅仅作用于分解后的低频系数，完全忽略了高频系数中的近似信息。同时，置乱操作都与明文无关，易受选择 / 已知明文攻击[5-9]。一些加密算中，仍然存在混沌序列简单、密钥空间小的问题。在典型混沌图像密码系统上，我们尝试探索了一个新的图像加密系统，其中伪随机密码流仍由混沌系统产生，加密图像为整数 S 变换后压缩图像，加密过程不需要循环操作。

一、基础理论

（一）PWLCM

采用分段线性映射产生混沌序列，映射方程表达为下式（1）所示。

$$F(x)=\begin{cases}x/p, & x\in[0,p)\\(1-x)/(1-p), & x\in(p,1]\end{cases} \tag{1}$$

其中，$x_i\in(0,1)$，$p\in(0,0.5)$。分段线性映射能生成具有良好统计特性的伪随机序列，因此，很多读者的加密方法中都应用了 PWLCM，并且都达到了很好的加密效果[3,7]。

（二）整数 S 变换

Sweldens 学者在 1994 年已经证明在提升方案的基础上可以进行整数集到整数集的小波变换[6,9]。一个整数集合通过小波变换得到的仍然是整数集合，并且这种变换完全可逆，能实现无失真重构数据[9]。整数 S 变换有如下 3 个步骤：

（1）分裂

将原始信号 $s_j=\{s_{j,k}\}$ 分为两个互不相交的子集和，每个子集长度为原子集的一半。通常将该信号序列分为偶数序列 e_{j-1} 和奇数序列 o_{j-1}，即：$Split(s_j)=(e_{j-1},o_{j-1})$。其中，$e_{j-1}=\{e_{j-1,k}=s_{j,2k}\}, o_{j-1}=\{o_{j-1,k}=s_{j,2k+1}\}$。

（2）预测

以其中一个序列（一般是偶数序列 e_{j-1}）来预测另一个序列（一般是奇数序列 o_{j-1}）来反映两序列之间的逼近程度。预测的过如下：$d_{j-1}=o_{j-1}-P(e_{j-1})$。其中，预测算子 P 可用预测函数 Pk 表示，预测函数为 $Pk(e_{j-1})\Rightarrow(e_{j-1,k}+e_{j-1,k+1}=s_{j,2k}+s_{j,2k+1})/2$。

（3）更新

为保持原始数据整体特征，整数 S 变换的更新的过程如下：$s_{j-1}=e_{j-1}+U(d_{j-1})$ 其中，s_{j-1} 为 s_j 的低频部分。更新函数为 $Uk(d_{j-1})=d_{j-1,k}/2$。

第一作者：李雪倩，女，硕士研究生，研究方向：信息安全、密码学。
通讯作者：王奕泽，男，硕士研究生，研究方向：数字思政与教育数字化建设。

 Copyright © This Work is Licensed under A Commons Attribution-Non Commercial 4.0 International License.

二、加密方案

加密算法中，密码流不仅与密钥有关，而且与明文相关。同时，为加快图像加密速度并充分确保图像信息完整性，通过整数S变换分解压缩原始输入图像，并运用了“扩散－置乱－扩散”的图像加密结构[3-5]。其中，扩散操作明文无关，而置乱操作与明文相关。

（一）压缩图像I

另明文图像为 P，大小为 $M\times N$（M 和 N 分别代表图像的宽度和高度），同时确保 N 必须为偶数。若 N 不是偶数，则将一个长度为 M 的零列向量加入到图像 P 的最后一列，使其成为大小为 $M\times(N+1)$ 的矩阵。

首先，对原始输入图像（如图1 (a-c) 所示，分别为 Lena，Pepper，Baboon）进行一级整数S变换分解，得到四个大小为 $(M/2)\times(N/2)$ 的不重复多分辨率系数集。接着，充分利用水平分量系数 (LH) 和垂直分量系数 (HL) 中所包含的低频信息，再次通过整数S变换提取出相应分量系数中的低频系数，与一级分解后的低频分量合并压缩为大小为 $(M/2+M/4)\times N/2$ 的图像 I。在图像 I 中，水平分量系数 (LH) 和垂直分量系数 (HL) 的低频系数中出现了不符合像素值的负值，通过有符号补码表示原理，得到符合0-255的所有像素值。不失一般性，以 Lena，Pepper，Baboon 图像为列，它们的压缩图像分别如图1(d-f) 所示。则压缩后的图像 I，I 的大小为 $m\times n$，即 $n=N/2$，$m=M/2+M/4$。以下所有 m 和 n 均为此大小。



(a) (b) (c) (d) (e) (f)

图1 原始图像和压缩图像：(a)Lena; (b)Pepper; (c)Baboon; (d-f) 分别为 (a-c) 的压缩图像

（二）密码矩阵

利用分段线性混沌映射进行迭代运算，以设定的初始值与控制参数为驱动，生成满足长度需求的一维混沌序列，为后续密码矩阵构造提供伪随机数据源[3-4,7,10]。

对生成的混沌序列进行归一化映射处理，将浮点型混沌值转换至 [0,255] 整数区间，使其符合图像像素的数值范围与加密运算要求。

将归一化后的混沌序列按照加密图像的高度与宽度进行维度重构，构造出与 $m\times n$ 尺寸一致的二维密码矩阵，用于后续加密过程。

（三）加密过程

(1)前向扩散

通过密码矩阵Y，将压缩图像I扩散为新图像矩阵A，该过程的具体步骤实现如下：

步骤1：令 $j=1,j=1$：

$$j=1,j=1,A(1,1)=I(1,1)\oplus Y(1,1) \tag{2}$$

步骤2：令 $i=1,j=j+1$，由 $I(1,j)$ 得到 $A(1,j)$，$j=2,3...n$：

$$A(1,j)=I(1,j)\oplus Y(1,j)\oplus A(1,j-1) \tag{3}$$

步骤3：令 $i=i+1,j=1$，由 $I(i,1)$ 得到 $A(i,1)$，$i=2,3...m$：

$$A(i,1)=I(i,1)\oplus Y(i,1)\oplus A(i-1,1)\oplus A(i-1,n) \tag{4}$$

步骤4：令 $i=2,3...m$，$j=2,3...n$：

$$A(i,j)=I(i,j)\oplus Y(i,j)\oplus A(i-1,j)\oplus A(i,j-1) \tag{5}$$

(2)置乱

步骤1：对于矩阵B的每个坐标点 $(i,j),i=1,2,...m,j=1,2,...n$，计算矩阵B的所有行和与列和，分别记为 R_i 和 C_j。之后，用如下的方法计算新的坐标值 (y,z)：

如果 $j \bmod 2=1$，则：

$$\begin{aligned} y&=[C_j-B(i,j)+Z(i,j)+Z(M+1-i,N+1-i)]\bmod M+1\\ z&=[R_i-B(i,j)+Z(i,N+1-j)+Z(M+1-i,\ j)]\bmod N+1 \end{aligned} \tag{6}$$

如果 $j \bmod 2=0$，则：

$$\begin{aligned} y&=M-[C_j-B(i,j)+Z(i,j)+Z(M+1-i,N+1-i)]\bmod M\\ z&=N-[R_i-B(i,j)+Z(i,N+1-j)+Z(M+1-i,j)]\bmod N \end{aligned} \tag{7}$$

若 $y=i$ 或 $z=j$，则 $B(i,j)$ 位置不变；否则交换 $B(i,j)$ 和 $B(y,z)$。

步骤2：通过从左到右、从上到下按步骤1的方式扫描B中每个像素得到一个新的置乱矩阵D。置乱矩阵D为后向扩散的输入矩阵。

(3)后向扩散

借助于伪随机密码矩阵Y，后向扩散将置乱后的矩阵D转换为新矩阵C，后向扩散的具体步骤如下：

步骤1：令 $j=1,j=1$：

$$C(1,1)=D(1,1)\oplus Y(1,1) \tag{8}$$

步骤2：令 $i=1,j=j+1$，由 $D(1,j)$ 得到 $C(1,j)$，$j=2,3,...n$：

$$C(1,j)=D(1,j)\oplus Y(1,j)\oplus D(1,j-1) \tag{9}$$

步骤3：令 $i=i+1,j=1$，由 $D(i,1)$ 得到 $C(i,1)$，$i=2,3,...m$：

$$C(i,1)=D(i,1)\oplus Y(i,1)\oplus D(i-1,1)\oplus D(i-1,N) \tag{10}$$

步骤4：令 $j=2,3,...n$，$i=2,3,...m$：

$$C(i,j)=D(i,j)\oplus Y(i,j)\oplus D(i-1,j)\oplus D(i,j-1) \tag{11}$$

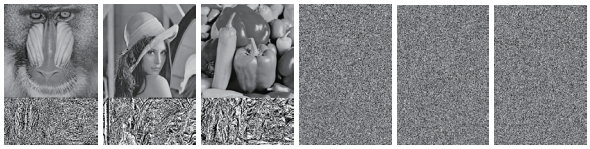
在加密过程中，后向扩散的输出C为最终的密文图像。

三、仿真结果

测试仿真使用的计算机配置为 Intel(R) Core(TM) i7-4720HQ CPU@2.60GHz，8GB RAM，Windows 7(64-bit)。不失一般性，算法使用密钥为 K={250 ,30,215,133,116, 122,

30,53,98,7,251,214,192,231,203,209,45,17,158,83,152,53,49,29,99,237,44,194,42,188,239,255,234,66,44,30,64,242,28,7,19,183,44,38,171,123,49,211,249,187,181,215,179,120,116,130,131,32,171,125,16,172,89,152}（十进制形式）。采用标准测试图像 Lena、pepper、Baboon（原图大小为 512×512，压缩后的图像大小为 384×256，压缩图像如图2(a-c) 所示），进行仿真测试分析，仿真加密图为下图2(d-f) 所示。

Copyright © This Work is Licensed under A Commons Attribution-Non Commercial 4.0 International License.



(a) (b) (c) (d) (e) (f)

图2仿真结果图：(a-c)Lena,Pepper,Baboon 的压缩图像；(d-f) Lena,Pepper,Baboon 的密文图像

四、结束语

本文提出了一种基于整数 S 变换的快速图像加密算法。该设计方法包括明文相关的一次置乱与两次扩散。仿真结果表明，密文图像呈现噪声样式，没有任何可视信息泄漏，且还原后的图像与原始的图像压缩前的图像完全一致，说明提出的图像密码系统可正常工作。

参考文献

[1] 赵耿，李文健，马英杰 . 基于变参数的 logistie 混沌系统图像加密算法 [J]. 计算机应用与软件，2023，40 (12):325-331.DOI:10.3969/j.issn.1000-386x.2023.12.048.

[2] 张翔 . 基于 Logistic 映射生成动态 S 盒的 Cat 混沌图像加密 [J]. 信息技术时代 ,2025 (13):75-77.

[3] 常举越，刘欢 . 基于四维超混沌系统的图像加密算法 [J]. 周口师范学院学报 ,2025,42(2):7-14.

[4] 唐成伟 . 基于改进混沌系统的数字图像加密算法设计与分析 [D]. 阜阳师范大学 ,2023.

[5] 徐冬冬，于欣，杜丽敏，等 . 基于混沌与快速小波变换的多光谱图像压缩加密算法 [J]. 光谱学与光谱分析 ,2022(009):042.DOI:10.3964/jissn.1000-0593(2022)09-2976-07.

[6] 谭晓东，赵奇，文明珠，等 . 基于 BEMD,DCT 和 SVD 的混合图像水印算法 [J]. 浙江大学学报：理学版 ,2023,50(4):442-454.

[7] 徐冬冬，于欣，杜丽敏，等 . 基于混沌与快速小波变换的多光谱图像压缩加密算法 [刀] 光谱学与光谱分析 ,2022(009):042.DOI:10.3964/j.issm.1000-0593(2022)09-2976-07.

[8] 高媛 . 基于离散小波变换和奇异值分解的数字水印改进算法研究 [D]. 安徽建筑大学 ,2021.

[9 沈子懿 . 王卫亚，荣宪伟，等 . 基于整数小波变换和二维混沌系统的多图像加密算法 [J]. 计算机工程与设计 ,2022,43(3):8

[10] 汪飞 . 基于双向防御的网络大数据无损加密算法仿真 [J]. 计算机仿真 ,2021.DOI:10.3969/j.issn.1006-9348.2021.10.063.

 Copyright © This Work is Licensed under A Commons Attribution-Non Commercial 4.0 International License.