文章编号：2096-1618(2021)02-0149-05

基于广义 logistic 混沌系统的快速图像加密方法

楚春阳[1,2]， 高瑜翔[1,2]， 谢建峰[1,2]

(1. 成都信息工程大学通信工程学院(微电子学院)，四川 成都 610225；2. 气象信息与信号处理四川省高校重点实验室，四川 成都 610225)

摘要：针对混沌加密系统的计算复杂与时耗高达1 s以上等问题，基于广义 logistic 混沌提出了一种快速的低复杂度的图像加密方法。该方法摒弃了复杂的多维混沌系统，利用广义 logistic 混沌序列进行图像的置乱、改进预处理操作，并应用特定的密钥方程代替烦琐的加密流程进行加密变换预处理后的图像。仿真实验表明，该算法降低了冗余度，提高了效率，实现了快速加密图像的目的。平均加、解密时间分别为0.231 s和0.022 s，是同等条件下 ElGamal 加密算法速率的5倍，能够满足加密的快速性、实时性要求，且能够抵抗多种攻击，具有安全性高、复杂性与时耗低等特点。

关 键 词：混沌加密系统；广义 logistic；低复杂度；实时性

中图分类号：TN911.73 **文献标志码**：A

doi：10.16836/j.cnki.jcuit.2021.02.004

0 引言

数据加密是保护数据免受威胁的有效方法。由于庞大的数据容量和图像文件中像素之间的高度相关性，传统技术不适用于图像加密[1]。如何保护这类信息成为一项迫在眉睫的挑战[2]。

在加密算法中，基于混沌的方法具有很强的加密特性，因其密钥空间大[3]、对初值与控制参数的敏感性与不易破解等特点，已出现了许多混沌图像加密算法[4-5]。混沌图像加密技术中，混沌系统主要有两种：一维(1D)和高维(HD)[6]。HD 混沌系统参数多、结构复杂，增加了其实现的难度和计算复杂度[7]。故一维混沌系统结构较为简单且易于实现。

由于大多数混沌图像加密[8]方案都具有很高的复杂度[9]，大大限制了时间效率，而低维混沌系统具有简单、高效，且易于实现[10]等优点，因此，本文使用了广义 logistic 混沌系统在提升了混沌区间范围和混沌行为等混沌特性的情形下，结合所提出的快速图像加密算法，用于实时处理图像加密。

该方法能够应用在医疗、军事、商业中，实时传输保密信息，保障其不被泄露、不易破解，保证了人们日常生活的安全。

仿真实验显示该算法显著降低了计算复杂度，在时间处理上优于大部分混沌图像加密算法，并保证了传输中加密图像的安全性，解决了图像传递中的攻击问题。通过仿真实验分析，证实了该算法的有效性。

1 广义 logistic 混沌

广义 logisitc 混沌方程如下：

$$f(x_k)=x_{k+1}=u_1 x_k^m(1-x_k)^n \tag{1}$$

根据文献[11]的推导，u_1 的变化范围为

$$\begin{cases} 1\le u_1\le \dfrac{(1+n)^{1+n}}{n^n}, & m=1 \\ \dfrac{(m+n-1)^{m+n-1}}{(m-1)^{m-1}n^n}\le u_1\le \dfrac{(m+n)^{m+n}}{m^m n^n}, & m>1 \end{cases} \tag{2}$$

确定在 $m=1, n=2$ 时(m、n 这里指的是方程的指数)，其混沌效应较好，混沌图如图1所示。

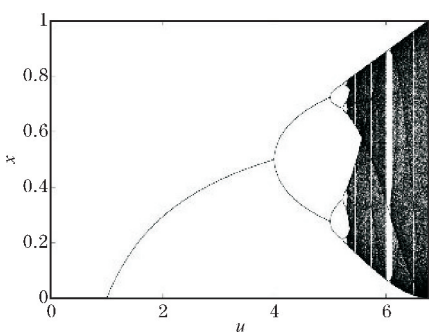


图1 广义 logisitc 混沌图

高维混沌系统具有复杂的结构和多个参数，它们增加了加密系统的安全性，但增加了算法实现的难度和计算复杂度，加大了算法的运行时间。相比之下，低维混沌系统结构简单，易于实现，设计和利用更好的一维混沌系统来加密图像对于加密系统的大规模实际应用很重要。而本文所提的广义 logistic 混沌系统的混沌区间足够大，在提高了自身混沌特性的情况下，结合快速图像加密算法，有效降低了时耗，实现了实时加密的特性。

2 广义 logistic 快速图像加密算法

2.1 混沌系统的选用

多维混沌系统结构复杂，计算复杂度高，不利于加

收稿日期：2020-09-08
基金项目：四川省教育厅高校创新团队资助项目(15TD0022)

密算法的快速性,而一维混沌系统正好适用于这一点。因此,采用广义 logistic 混沌系统,一是降低混沌系统的复杂度;二是广义混沌系统混沌区间大,能够更好提升自身的混沌特性,继而保障混沌加密质量,提高安全性。

2.2 快速加密算法

现有的加密算法过于烦琐,冗余度较高,增加了算法的复杂性,导致加密时间更长,无法满足快速加密图像的要求,不利于实时处理。为了提高效率,快速加密图像,使用特定的密钥方程用于加密算法的具体实施。

步骤 1 使用循环处理像素的形式,将 $f(x_k)=x_{k+1}=u_1x_k^1(1-x_k)^2$ 产生混沌序列用于对图像像素的置乱排列。如下核心操作:

$T=I(m)$;T 为临时变量、I 为原始图像

$I(m)=I(in(m))$; $in(m)$ 为混沌序列排序后的值

$I(in(m))=T$。

步骤 2 利用循环移位函数对 $S_{i+1}=\sin[T\cdot\arcsin(S_i)]$ 产生的钥匙做乱序处理,$K=\text{circshift}(S,1)$;

最后将乱序后的密钥与原密钥异或得到最终密码钥匙。$\text{key}=\text{bitxor}(S,K)$。

步骤 3 使用 XOR 操作,完成对图像加密的整体实现。

加密的快速性在于加密密钥方程。主要使用相关密匙在密钥方程中产生一系列初始密钥,并扩大成整数值,通过进制转换和循环移位得到变换后的密钥,在将其异或于初始密钥形成最终密钥用于图像的加密。加密时通过倒置与异或操作成功完成加密功能。

其优势在于该密钥方程替代了繁杂的加密流程,实现快速加密却不降低加密的质量。并且由于加密密钥具有广泛的参数设置和统一分布的变异密度函数,可以增加密钥空间并增强加密安全性,尤其是密钥的处理,其更严密的密钥方案保障了加密的效果。

2.3 算法框架

提出的算法如图 2 所示。首先,将广义 logistic 混沌系统产生的混沌序列用于图像的置乱操作以及相应的预处理过程,保证加密算法的安全性。其次,使用给定的密钥方程 $S_{i+1}=\sin[T\cdot\arcsin(S_i)]$ 创建密钥,并对密钥做进制转换并循环移位,再与原密钥做异或处理得到加密所需的最终密钥。(广义 logistic 混沌是用于图像像素扰乱的预处理,密钥方程是用于制作加密钥匙对扰乱后的图像进行加密操作。)最后将预处理后的图像与最终密钥进行异或操作实现加密,达到低复杂性与低时耗的目的,实现快速性。

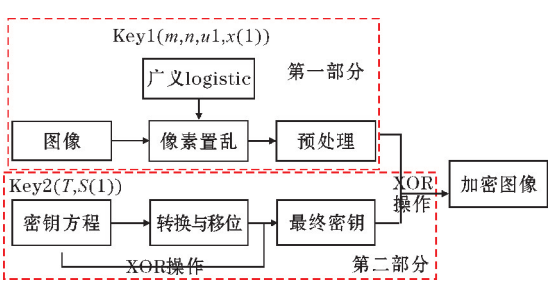


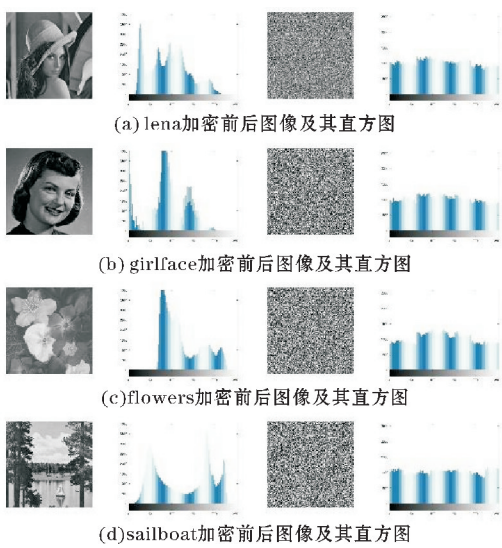
图 2 广义 logistic 快速图像加密系统

传统的经典算法会导致大量密文和极高的时间消耗,但本文算法在提高加密效率的前提下,降低了算法实现的难度与计算复杂度,提高了加密的速度,缩短了加密时间。

3 仿真实验结果

3.1 密钥空间、直方图与像素分析

若每个参数的长度和初始值都设置为 14 位小数,则该算法的 6 个控制参数[$m,n,u_1,x(1),p,k(1)$](m、n 与式(2)中指数对应)的密钥空间大小为10^{84},可见密钥空间足够大,能够抵抗蛮力攻击。且加密后的图像直方图及图像的相邻像素都是均匀分布的,证明能够抵抗统计攻击。如图 3、4 所示。



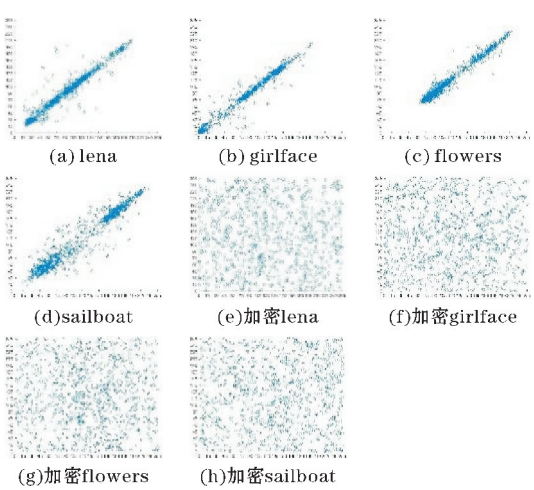
(a) lena加密前后图像及其直方图

(b) girlface加密前后图像及其直方图

(c)flowers加密前后图像及其直方图

(d)sailboat加密前后图像及其直方图

图 3 不同加密前后图像及其直方图



(a) lena (b) girlface (c) flowers

(d)sailboat (e)加密lena (f)加密girlface

(g)加密flowers (h)加密sailboat

图 4 原图像与加密图像在对角方向上的相邻像素分布图

3.2 相关性分析

优质的加密算法会破坏像素的相关性,在加密后图像相邻像素相关性会变低。这是加密性能的一个重要指标。分别对水平、垂直、对角进行分析,如表 1 所

示。公式如下:

$$E(x)=\frac{1}{N}\sum_{i=1}^{N}x_i \tag{3}$$

$$D(x)=\frac{1}{N}\sum_{i=1}^{N}[x_i-E(x_i)]^2 \tag{4}$$

$$\mathrm{cov}(x,y)=\frac{1}{N}\sum_{i=1}^{N}[x_i-E(x_i)][y_i-E(y_i)] \tag{5}$$

$$r_{xy}=\frac{\mathrm{cov}(x,y)}{\sqrt{D(x)D(y)}} \tag{6}$$

表 1　相关性分析

图像	原始图像			加密图像		
	水平方向	垂直方向	对角方向	水平方向	垂直方向	对角方向
lena	0.9757	0.9911	0.9634	0.0005	-0.0036	-0.0034
girlface	0.9879	0.9894	0.9818	0.0035	0.0219	-0.0085
flowers	0.9918	0.9929	0.9851	0.0037	-0.0798	-0.0019
sailboat	0.9722	0.9709	0.9576	-0.0019	0.0211	0.0079

仿真实验分析证实该算法加密性能较好,具有抵抗相关性的统计攻击的能力。

3.3　信息熵、敏感性与峰值信噪比(PSNR)分析

信息熵计算公式如下:

$$H(s)=-\sum_{i=0}^{2^n-1}P(s_i)\lg[P(s_i)] \tag{7}$$

对于[0,255]的灰度图像,信息熵值最大为 8。越接近最大的熵值,说明加密的效果越好。

敏感性分析主要用来衡量加密算法是否能够抵抗差分攻击。由以下两个因素度量:

像素变化率(NPCR)。

$$\mathrm{NPCR}=\frac{1}{N\times M}\sum_{i=1}^{M}\sum_{j=1}^{N}E(i,j)\times 100\% \tag{8}$$

统一平均变化强度(UACI)。

$$\mathrm{UACI}=\frac{1}{N\times M}\sum_{i=1}^{M}\sum_{j=1}^{N}\frac{|I(i,j)-R(i,j)|}{255}\times 100\% \tag{9}$$

NPCR 表示输入图像相同的两个密码图像在微小变化前和后的变化率。UACI 表示两个密码图像之间相应强度值的平均变化强度。$M\times N$ 是原图像大小,$I(i,j)$是原始图像,$R(i,j)$是加密图像。如果 $I(i,j)=R(i,j)$,那么$E(i,j)=0$;如果 $I(i,j)\neq R(i,j)$,那么 $E(i,j)=1$。

PSNR 分别将原始图像与加密图像作为信号和噪声客观地评估加密算法[12]。公式如下:

$$\mathrm{MSE}=\frac{1}{M\times N}\sum_{i=1}^{M}\sum_{j=1}^{N}[D(i,j)-P(i,j)]^2 \tag{10}$$

$$\mathrm{PSNR}=10\times\lg\left(\frac{L^2}{\mathrm{MSE}}\right) \tag{11}$$

其中,D 是加密图像,P 是原始图像,$M\times N$ 是原图像的大小,本文中灰度值 $L=255$。其综合分析如表 2 所示。

表 2　信息熵值和敏感性分析

图像	加密信息熵	NPCR/%	UACI/%	PSNR/dB
lena	7.9931	99.5761	29.2079	8.9367
girlface	7.9934	99.6089	31.0556	8.3610
flowers	7.9844	99.5594	27.0655	9.6859
sailboat	7.9972	99.6013	31.8148	8.2082

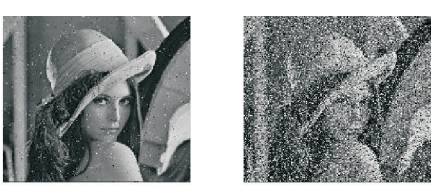
从表 2 分析得出,NPCR 和 UACI 的值逼近于理想值 99.61% 和 33.46%[13],且每个图像的 PSNR 值小于 10 dB[14],证实该算法具有抗差分攻击的能力,加密质量较好。

3.4　噪声与裁剪攻击

实验通过结构相似性(SSIM)与 PSNR 来分析视觉差异。加密效果好的密码系统能够在一定程度上抵制不同类型的噪声[15],实验分析如表 3 所示。图 5 显示了该算法抵抗椒盐噪声攻击的能力,图 6 是本文算法与文献[16]在 75% 裁剪攻击下的图像复原效果比较,证明本文算法的性能良好。

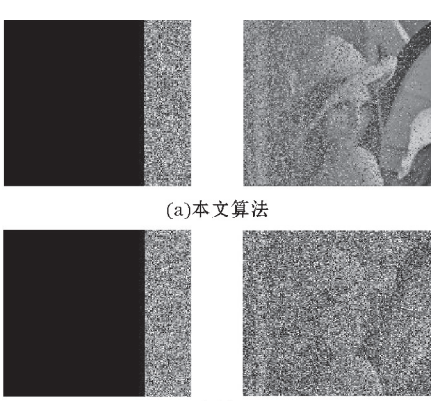
表 3　lena 图像在椒盐噪声影响下的 PSNR 与 SSIM

方案	椒盐噪声概率			
	0.005	0.05	0.1	0.5
本文 PSNR	30.4180	28.1087	24.7867	12.0749
文献[17]PSNR	29.7712	19.6544	16.6706	10.9036
本文 SSIM	0.9031	0.8223	0.6565	0.0611



(a) 0.1　　(b) 0.5

图 5　lena 在 0.1 与 0.5 椒盐噪声密度下的复原图像



(a)本文算法　　(b)文献[16]

图 6　75% 裁剪比例下的复原图像

3.5 时耗分析

本文所提出的算法将置乱与预处理和特殊加密密钥结合在一起,且每次加密时只需对图像进行一次扫描,并且每个加密步骤中的时间消耗非常低[18]。计算复杂度主要取决于设计的算法流程中的两部分,并对其做测试分析,如表 4 所示。

表 4 部分图像加解密实验均值分析 单位:s

图像	加密		解密
	第一部分	第二部分	
girlface	0.0412	0.1550	0.0078
sailboat	0.0529	0.1842	0.0091
lena	0.0445	0.1753	0.0099
flowers	0.0487	0.1490	0.0081

在加密过程中,采用了一些整数运算符(例如 XOR,模数等)来减少浮点整数的乘法和转换等耗时的运算数量[19]。本文基于 Win10, 1.80GHz Intel CPU,3.90 GBRAM, Matlab2016a,大小为 512×512 的图像进行加密和解密实验,分析如表 5 所示。

表 5 不同方法的时耗 单位:s

加密方案	平均加密时间	平均解密时间
ElGamal	1.201	1.554
文献[18]	0.270	0.269
文献[21]	9.590	6.538
文献[22]	4.031	3.624
本文方案	0.231	0.022

本文提出的算法无需多次置换、扩散以及循环加密等操作,只需要进行一次加密即可达到满意的加密效果,且该算法执行时间和像素移动操作的迭代次数更少[20]。提出的方案中广义 logistic 混沌这一一维混沌对前期的像素扰乱与后续的密钥方程处理加密,这两部分完成了整体的加密流程,相比现有的加密算法(对图像像素的对角变化、混合置乱,循坏扩散等方式过程烦琐、耗时长、计算复杂度高)大大地提高了效率。仿真实验结果显示,该方案平均运行时间优于现阶段大部分图像加密算法,具有实时性的优点,且能够高效完成混沌图像加密,抵抗各种攻击,满足加密需要。由此看出,本文算法加密性能较好。

4 结束语

本文的加密方法大大降低了加密所需的时耗,能够满足实时加密的特点,具有快速性,高效性。即使受到各种攻击,甚至在 75% 裁剪下的图像也可以成功解密并且能较为清晰地辨识出来,有效保证了图像加密的性能,不但提高了加密效率,也保障了其安全性与可靠性。可见,基于广义 logistic 混沌系统的快速图像加密方法具有很好的优越性。

参考文献:

[1] Zhang G, Liu Q. A novel image encryption method based on total shuffling scheme[J]. optics communications, 2011, 284(12): 2775-2780.

[2] Volos CK, Kyprianidis I M, Stouboulos I N. Image encryption process based on chaotic synchronization phenomena[J]. Signal processing, 2013, 93(5): 1328-1340.

[3] ZHU H G, ZHAO C, ZHANG X D. A novel image encryption-compression scheme using hyper-chaos and Chinese remainder theorem[J]. Signal processing: image communication, 2013, 28(6): 670-680.

[4] Kumar G A, Bagan K B, Sriraam N, et al. IMAGE ENCRYPTION BASED ON DIFFUSION AND MULTIPLE CHAOTIC MAPS[J]. International Journal of Network Security & Its Applications, 2011, 3(2): 181-194.

[5] Ellatif A A, Li L, Wang N, et al. Image Encryption Scheme of Pixel Bit Based on Combination of Chaotic Systems[C]. intelligent information hiding and multimedia signal processing, 2011: 369-373.

[6] Hua Z, Zhou Y, Pun C M, et al. 2D Sine Logistic modulation map for image encryption[J]. Information Sciences, 2015, 297: 80-94.

[7] Ye G. Image scrambling encryption algorithm of pixel bit based on chaos map[J]. Pattern recognition letters, 2010, 31(5): 347-354.

[8] Wang X, Wei N, Zhang D, et al. A novel image encryption algorithm based on chaotic system and improved GravityModel[J]. Optics Communications, 2015, 338: 209-217.

[9] Lin Z, Liu J, Lian J, et al. A novel fast image encryption algorithm for embedded systems[J]. Multimedia Tools & Applications, 2019, 78(14).

[10] Bhatnagar G, Wu Q M. Selective image encryption based on pixels of interest and singular value decomposition[J]. Digital Signal Processing, 2012,

22(4):648-663.
[11] 郭凤鸣,涂立. 混沌理论在密码学中的应用[M]. 北京:北京理工大学出版社,2015.
[12] Hanchinamani G, Kulkarni L. An Efficient Image Encryption Scheme Based on a Peter De Jong Chaotic Map and a RC4 Stream Cipher[J]. 3d Research, 2015, 6(3).
[13] Li Y,Wang C,Chen H,et al. A hyper-chaos-based image encryption algorithm using pixel-level permutation and bit-levelpermutation[J]. Optics and Lasers in Engineering,2017,90:238-246.
[14] Sheela S J,Suresh K V,Tandur D. Image encryption based on modified Henon map using hybrid chaotic shift transform[J]. Multimedia Tools and Applications,2018,77(19):25223-25251.
[15] A Saaidi,A Saaidi,M L Benmaati. A Novel Image Encryption Algorithm Based on the Two-Dimensional Logistic Map and the Latin Square Image Cipher [M]. Springer-Verlag New York,Inc. 2015.
[16] Zhan K,Wei D,Shi J,et al. Cross-utilizinghyperchaotic and DNA sequences for image encryption [J]. Journal of Electronic Imaging,2017,26(1): 13021.
[17] Xiangjun Wu,Haibin Kan. A new color image encryption scheme based on DNA sequences and multiple improved 1D chaotic maps[M]. Elsevier Science Publishers B. V,2015.
[18] Li F,Wu H,Zhou G,et al. Robust real-time image encryption with aperiodic chaotic map and random-cycling bitshift[J]. Journal of Real-time Image Processing,2019,16(3):775-790.
[19] Wang Y, Wong K, Liao X, et al. A new chaos-based fast image encryptionalgorithm[J]. Applied Soft Computing,2011,11(1):514-522.
[20] Liu W,Sun K,Zhu C,et al. A fast image encryption algorithm based on chaoticmap[J]. Optics and Lasers in Engineering,2016,84:26-36.
[21] Yi S,Zhou Y. Binary-block embedding for reversible data hiding in encryptedimages[J]. Signal Processing,2017,133:40-51.
[22] WANG K, ZHANG H W, LI X H. Image block encryption algorithm based on DNA code operation and chaotic system[J]. Video engineering, 2017,41(3):6-10.

A Fast Image Encryption Method based on Generalized logistic Chaotic System

CHU Chunyang[1,2], GAO Yuxiang[1,2], XIE Jianfeng[1,2]

(1. College of Communication Engineering (College of Microelectronics), Chengdu University of Information Technology, Chengdu 610225, China; 2. Meteorological Information and Signal Processing Key Laboratory of Sichuan Education Institutes, Chengdu 610225, China)

Abstract: To solve the problems of chaotic encryption system, such as high computational complexity and time consumption up to more than 1s, a fast and low-complexity image encryption method based on generalized logistic chaos was proposed. In this method, the complex multidimensional chaotic system is abandoned, and the image is scrambled and preprocessed with the generalized logistic chaotic sequence, and the specific key equation is used instead of the cumbersome encryption process to encrypt and transform the preprocessed image. Simulation results show that the algorithm reduces redundancy, improves efficiency and achieves fast image encryption. The average encryption and decryption time are 0.231 s and 0.022 s respectively, which is 5 times of the speed of ElGamal encryption algorithm under the same conditions. It can meet the requirements of fast and real-time encryption, and can resist a variety of attacks, and is with high security, complexity and low time consumption.

Keywords: chaotic encryption system; the generalized logistic; low complexity; real-time