

基于级联混沌映射与低位嵌入的图像隐写算法

穆俊

引用本文:

穆俊. 基于级联混沌映射与低位嵌入的图像隐写算法[J]. 液晶与显示, 2020, 35(4): 374–382.

MU Jun. Image steganography algorithm based on cascaded chaotic map and low bits embedding[J]. *Chinese Journal of Liquid Crystals and Displays*, 2020, 35(4): 374–382.

在线阅读 View online: <https://doi.org/10.3788/YJYXS20203504.0374>

您可能感兴趣的其他文章

Articles you may be interested in

基于二维串联调制耦合映射的图像加密–秘密分享算法

Image encryption–secret sharing algorithm based on two–dimensional cascade modulation coupling map

液晶与显示. 2019, 34(12): 1210–1217 <https://doi.org/10.3788/YJYXS20193412.1210>

结合图像边缘检测和最小误差替换的隐写方案

Steganography based on edge detection and minimum error replacement

液晶与显示. 2015, 30(1): 151–156 <https://doi.org/10.3788/YJYXS20153001.0151>

基于遗传–超混沌的数字图像加密算法设计

Digital image encryption algorithm design based on Genetic–hyperchaos

液晶与显示. 2017, 32(6): 474–481 <https://doi.org/10.3788/YJYXS20173206.0474>

基于特征排名的图像隐写分析算法

Image steganalysis algorithm based on feature ranking

液晶与显示. 2018, 33(6): 490–496 <https://doi.org/10.3788/YJYXS20183306.0490>

基于卷积神经网络的图像去雾算法

Image defogging algorithms based on multiscale convolution neural network

液晶与显示. 2019, 34(2): 220–227 <https://doi.org/10.3788/YJYXS20193402.0220>

文章编号:1007-2780(2020)04-0374-09

基于级联混沌映射与低位嵌入的图像隐写算法

穆 俊*

(滇西科技师范学院 信息工程学院, 云南 临沧 677000)

摘要:为保证部分具有重要价值的数字图像在不可信信道中传输的安全性,本文设计了一种基于级联混沌映射和伪装图低位嵌入的图像隐写算法。该算法为置乱-混淆-低位嵌入结构。在置乱步骤中,首先通过两个混沌映射的级联设计了一种新型的混沌映射并用其产生具有高度随机性的随机数序列,然后随机数序列被用于数字图像的置乱,生成置乱图。在混淆步骤中,通过用户随机选择的伪装图与置乱图的与或操作来实现置乱图中像素值的混淆。最后,在低位嵌入步骤中,混淆步骤生成的图像按照两个位平面一组的规则被拆分成 4 份子图像并嵌入到伪装图的最低两位。在多个混沌映射性能指标的测试中,本文所提出的级联混沌映射均表现优异。在图像安全性和性能分析实验中,本文所提出的图像隐写算法表现出高度的安全性和极高的执行效率。

关键词:混沌映射;图像隐写;低位嵌入

中图分类号:TP391.4; TH691.9 **文献标识码:**A **doi:**10.3788/YJYXS20203504.0374

Image steganography algorithm based on cascaded chaotic map and low bits embedding

MU Jun*

(School of Information Science & Engineering,
Dian Xi Science and Technology Normal University, Lincang 677000, China)

Abstract: In order to ensure the security of some digital images with important value in untrusted channels, an image steganography algorithm based on cascaded chaotic map and low-bits embedding is proposed. The algorithm has a permutation-confusion-low bits embedding structure. In the permutation step, a novel chaotic map is firstly designed by cascade of two chaotic maps and used to generate a highly random sequence of random numbers, and then the random number sequence is used for scrambling digital images. In the confusion step, the confusion of the pixel values in the scrambling image is achieved by the XOR operation of the randomly selected cover image and the scrambling image. Finally, in the low bits embedding step, the image generated by the confusion step is split into four sub-images and embedded in the lowest two bits of the cover image. In the test of several chaotic map performance indicators, the cascaded chaotic map proposed in this paper is excellent. In the image security and performance analysis experiments, the image steganography algorithm proposed in this paper also shows high security and high execution efficiency.

收稿日期:2019-08-30; **修订日期:**2019-11-22.

基金项目:云南省教育厅科学研究基金重点项目(No. 2014Z137)

Supported by Key Project of Scientific Research Foundation of Yunnan Provincial Department of Education

* 通信联系人, E-mail: Mujunmj0827@126.com

Key words: chaotic map; image steganography; low bits embedding

1 引言

数字图像在互联网中的传输越来越广泛和频繁,与之伴随而来的是不法分子在不可信信道中对一些具有重要价值图像的窃取和篡改。此类事件的大量发生不仅导致了一系列严重的经济损失,还可能导致国家利益被侵犯^[1-2]。针对重要数字图像在不可信信道中的安全传输问题,相关领域的学者们提出了一系列的解决方案,包括图像加密^[3-10]、图像隐写^[11-13]和图像水印^[14-18]。相比于图像水印方案,图像加密方案和图像隐写方案因为将图像中的全部可用信息进行了不可视处理,所以具有更高的安全性。

在图像加密领域,近年来研究者们提出了相当多种类的算法,这些算法使用的加密工具主要包括混沌映射^[3-7]、DNA计算^[10]、神经网络^[8]、波变换^[9]。由于混沌映射具有极端初值敏感性,同时其产生的随机数序列具有高度的随机性,与图像加密的安全性不谋而合,因此混沌映射在图像加密领域应用是最为广泛的一种工具。图像加密算法的结构一般为置乱-混淆结构,该结构为Fridrich^[3]首次提出,其高度的安全性已在实践中得到了反复验证。其中,置乱指对图像像素位置的规律性改变,混淆指对图像像素值的规律性改变。

部分学者认为图像加密生成的类似马赛克状的图像在信道中传输时,很容易引起窃密者的怀疑,因此提出了通过一些手段将重要图像隐藏到一些无价值图像中,以最大程度降低窃密者的兴趣,这种技术即为图像隐写。

本文提出了一种置乱-混淆-低位替换结构的图像隐写算法。该算法结合了传统置乱-混淆结构的图像加密方式和基于低位替换的图像隐写。通过图像加密和隐写的合并使用,算法的安全性得到了极大提高。在置乱步骤中,首先通过帐篷映射和Logistic映射的级联设计了一种新型的混沌映射并用其产生具有高度随机性的随机数序列,然后随机数序列被用于数字图像的置乱,生成置乱图。在混淆步骤中,加密方随机选择无价值的图像作为伪装图,通过伪装图与置乱图的与或操作实现置乱图中像素值的混淆。最后,在低位

替换步骤中,混淆步骤生成的图像按照两个位平面一组的规则被拆分成4份子图像并嵌入到伪装图的最低两位。在分叉图、李亚普诺夫指数(Lyapunov exponent, LE)这两个指标的测试中,本文所提出的级联混沌映射均表现优异。在图像安全性和性能分析实验中,本文所提出的图像隐写算法也表现出高度的安全性和极高的执行效率。

2 级联混沌映射

2.1 级联混沌映射架构

图1展示了一种新型级联混沌映射,称为帐篷-Logistic映射。在该映射中,帐篷映射的输出被作为Logistic映射的输入,Logistic映射的输出再反馈到帐篷映射的输入端。其中帐篷映射和Logistic映射的定义分别如公式(1)、(2)所示。通过图1所示架构生成的帐篷-Logistic映射的数学定义如公式(3)所示。

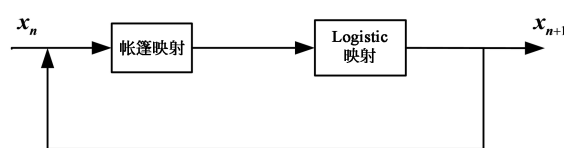


图1 帐篷-Logistic映射架构

Fig.1 Structure of tent-logistic map

$$x_{n+1} = \begin{cases} \mu x_n, & x_n < 0.5 \\ \mu(1 - x_n), & 0.5 \leq x_n \end{cases}, \quad (1)$$

$$x_{n+1} = r x_n (1 - x_n), \quad 3.5669 < r \leq 4, \quad (2)$$

μ 和 r 分别为帐篷映射和Logistic映射的系统参数。设定初始值 x_0 和系统参数,通过式(1)和(2)的持续迭代,可以生成混沌随机数序列 $\{x_0, x_1, x_2, \dots\}$ 。

$$x_{n+1} = \begin{cases} r\mu x_n(1 - \mu x_n), & x_n < 0.5 \\ r\mu(1 - x_n)[1 - \mu(1 - x_n)], & 0.5 \leq x_n \end{cases}. \quad (3)$$

对帐篷-Logistic映射而言,由于包含了更多的参数,因此相比于原来的两个混沌映射,其初值敏感性更高,混沌范围更广泛。

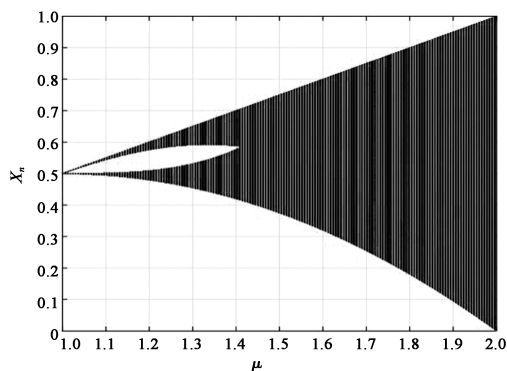
2.2 混沌性能测试

将本文所提出的帐篷-Logistic映射与帐篷映

射、Logistic 映射分别进行了定性比较和定量比较。定性比较通过比较各自分叉图的分叉范围完成。定量比较通过比较李亚普诺夫指数谱完成。

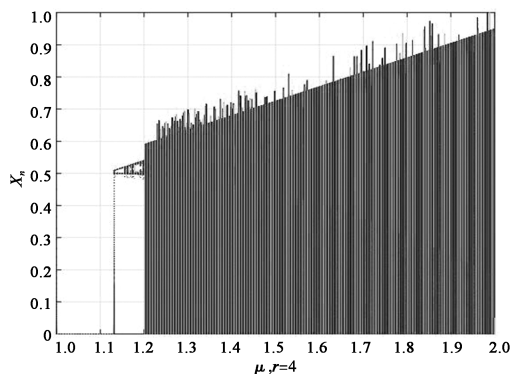
2.2.1 分叉图比较

当系统参数 μ 的变化范围为 $[1, 2]$ 时, 帐篷映射的分叉图如图 2(a) 所示。固定系统参数 $r = 4$, 帐篷-Logistic 映射的分叉图如图 2(b) 所示。当系统参数 r 的变化范围为 $[1, 4]$ 时, Logistic 映射的分叉图如图 3(a) 所示。固定系统参数 $\mu = 2$, 帐篷-Logistic 映射的分叉图如图 3(b) 所示。



(a) 帐篷映射的分叉图

(a) Bifurcation of tent map



(b) 帐篷-Logistic 映射的分叉图

(b) Bifurcation of tent-logistic map

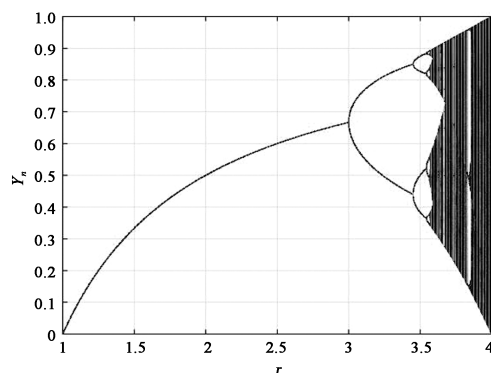
图 2 帐篷映射和帐篷-Logistic 映射的分叉图

Fig.2 Bifurcation of tent map and tent-logistic map

通过图 2 和图 3 可以看出, 本文所提出的新型映射的混沌范围要远大于两个原来的子映射的混沌范围。更大的分叉图范围意味着混沌映射生成的随机数序列的随机性更高, 这样的混沌映射可以保证加密方案具有更高的安全性。

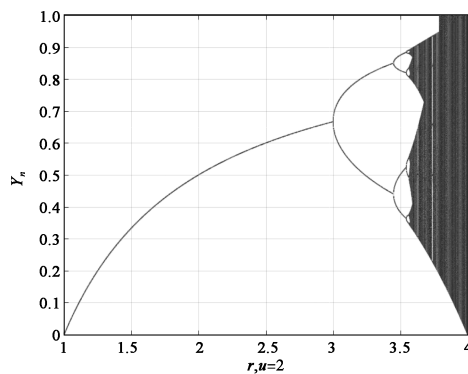
2.2.2 李亚普诺夫指数谱比较

李亚普诺夫指数谱的横轴为系统参数变化范



(a) Logistic 映射的分叉图

(a) Bifurcation of logistic map



(b) 帐篷-Logistic 映射的分叉图

(b) Bifurcation of tent-logistic map

图 3 Logistic 映射和帐篷-Logistic 映射的分叉图

Fig.3 Bifurcation of logistic map and tent-logistic map

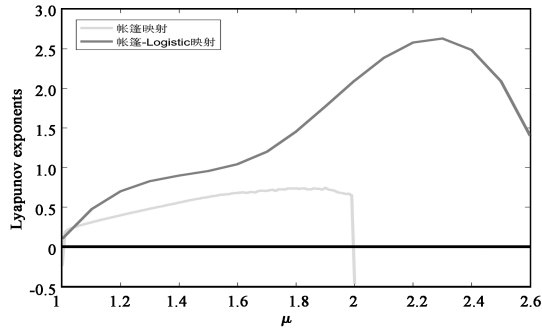
围, 纵轴为李亚普诺夫指数值。大于 0 的李亚普诺夫指数值表示此系统参数下的混沌映射处于混沌状态, 小于 0 的李亚普诺夫指数值表示此系统参数下的混沌映射处于周期震荡状态^[19]。为了定量分析所提出的混沌映射的性能, 本文展示了 3 种映射的李亚普诺夫指数谱, 如图 4 所示。

通过图 4 可以直观地发现本文所提出的帐篷-Logistic 映射相比于参与比较的其他两个映射, 其混沌系统参数的设置范围要宽松许多, 说明系统更容易进入混沌状态, 而这种特性正是图像加密所需的。

3 图像隐写方案设计

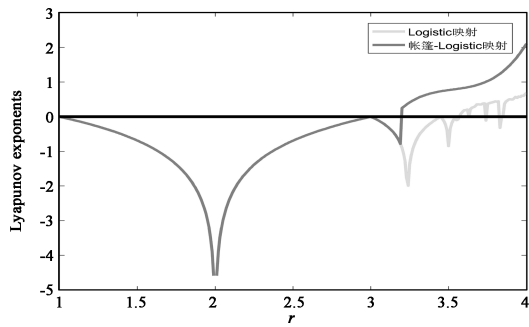
3.1 隐写模块方案设计

将待隐藏的原始秘密图像隐藏到伪装图像的过程分为 3 步: 置乱、混淆和低位嵌入。整体流程



(a) 帐篷-Logistic 映射与帐篷映射

(a) Tent-logistic map and tent map



(b) 帐篷-Logistic 映射与 Logistic 映射

(b) Tent-logistic map and logistic map

图4 帐篷-Logistic 映射与两种原始映射的李亚普诺夫指数谱比较

Fig.4 Comparison of tent-logistic map and two original maps in Lyapunov exponent spectra

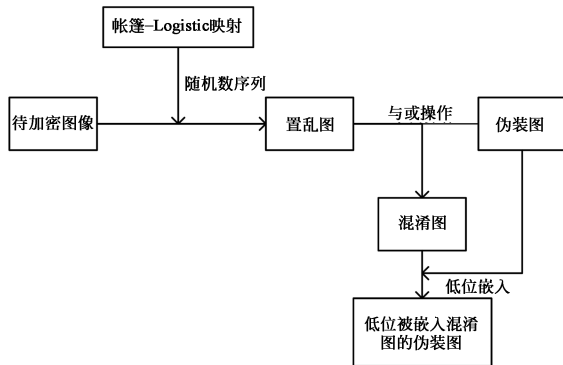


图5 隐写模块运行流程图

Fig.5 Flow chart of steganographic module operation

如图5所示。设原始秘密图像为 O ,其大小为 $M \times N$,图像隐写的详细步骤叙述如下,其中置乱为步骤1~3,混淆为步骤4,低位嵌入为步骤5。

步骤1:设定帐篷-Logistic映射的系统参数 μ, r 及初始值 x_0 ,驱动帐篷-Logistic映射产生混

沌随机数序列 $C = \{x_1, x_2, \dots, x_{M+N}\}$;

步骤2:将 C 拆分为 $C_1 = \{x_1, x_2, \dots, x_M\}$, $C_2 = \{x_{M+1}, x_{M+2}, \dots, x_{M+N}\}$ 。分别将 C_1 和 C_2 按照降序排列,得到 C_1 和 C_2 的排序矢量 $a = \{a_1, a_2, \dots, a_M\}$ 和 $b = \{b_1, b_2, \dots, b_N\}$;

步骤3:按照公式(4)对原始秘密图像进行置乱,生成置乱图;

$$O(a_i, b_j) = O(i, j), \begin{cases} i=1, 2, \dots, M \\ j=1, 2, \dots, N \end{cases}, \quad (4)$$

步骤4:加密方随机选择一幅与置乱图相同大小的无价值图像作为伪装图。将伪装图的前6个位平面与步骤3生成的置乱图的前6个位平面进行与或操作,生成混淆图;

步骤5:将步骤4生成的混淆图按照相邻两个位平面一组的顺序进行拆分,得到4幅子图像。将伪装图复制4份,每份伪装图的最低两个位平面使用一幅子图像进行替换,生成新的伪装图 C_1, C_2, C_3, C_4 。

3.2 秘密图像提取方案设计

从低位被嵌入混淆图的伪装图 $C_i, i=1, 2, 3, 4$ 中提取出原始秘密图像 O 的整体流程框图如图6所示。

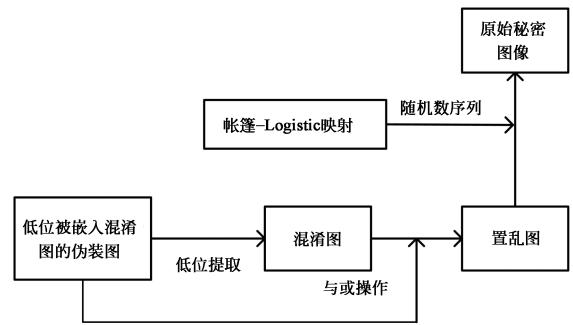


图6 秘密图像提取模块运行流程图

Fig. 6 Flow chart of secret image extraction module operation

其详细步骤如下所述:

步骤1:收集所有的 $C_i, i=1, 2, 3, 4$,通过提取最低两个位平面然后重组的方式生成混淆图;

步骤2:通过混淆图与伪装图的与或操作生成置乱图;

步骤3:设定帐篷-Logistic映射的系统参数 μ, r 及初始值 x_0 ,驱动帐篷-Logistic映射产生混沌随机数序列 $C = \{x_1, x_2, \dots, x_{M+N}\}$;

步骤4:将 C 拆分为 $C_1 = \{x_1, x_2, \dots, x_M\}$,

$C_2 = \{x_{M+1}, x_{M+2}, \dots, x_{M+N}\}$ 。然后分别将 C_1 和 C_2 按照降序排列, 得到 C_1 和 C_2 的排序矢量 $\mathbf{a} = \{a_1, a_2, \dots, a_M\}$ 和 $\mathbf{b} = \{b_1, b_2, \dots, b_N\}$;

步骤 5: 按照公式(5)对置乱图进行还原, 生成原始秘密图像;

$$O(i, j) = O(a_i, b_j), \begin{cases} i = 1, 2, \dots, M \\ j = 1, 2, \dots, N \end{cases} \quad (5)$$

4 算法安全性和执行效率测试

本文所提出的算法对图 7 所示的 4 张灰度图各进行了一轮隐写-提取, 生成的 4 幅类似于马赛克图像的加密图像展示于图 8。4 次加密所用的伪装图原图和被嵌入了加密图像的伪装图展示于图 9。

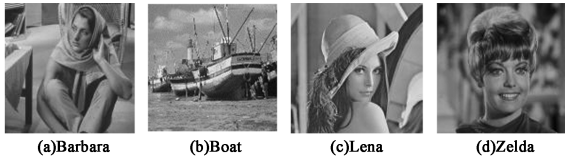


图 7 原始秘密图像

Fig.7 Original secret images

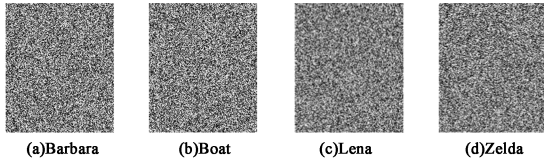


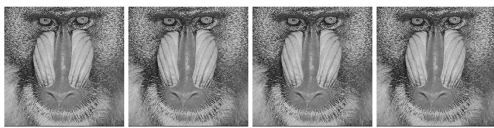
图 8 通过置乱-混淆环节生成的 4 幅加密图像

Fig.8 Ciphertext images



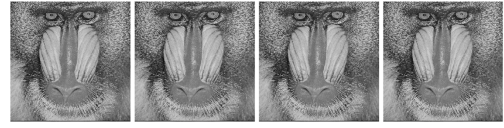
(a) 原始伪装图

(a) Original cover image



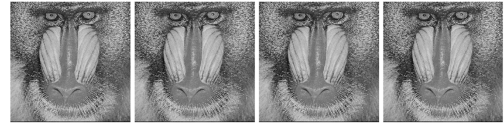
(b) 最低 2 位嵌入图 8(a) 的隐写图像

(b) Steganographic images of lowest 2 bits embedding Fig.8(a)



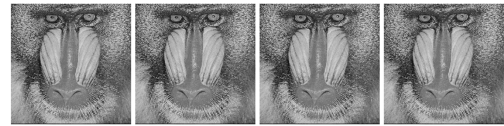
(c) 最低 2 位嵌入图 8(b) 的隐写图像

(c) Steganographic images of lowest 2 bits embedding Fig.8(b)



(d) 最低 2 位嵌入图 8(c) 的隐写图像

(d) Steganographic images of lowest 2 bits embedding Fig.8(c)



(e) 最低 2 位嵌入图 8(d) 的隐写图像

(e) Steganographic images of lowest 2 bits embedding Fig.8(d)

图 9 原始伪装图和隐写图像

Fig.9 Cover image and steganographic images

为了测试本文所提出算法的高度安全性和执行效率, 本文所提出算法进行了 3 种测试, 分别是密钥敏感性测试、抗统计攻击测试和隐写-提取用时测试。

4.1 密钥敏感性分析

本文所提出的算法使用的密钥对 $k = \{\mu, r, x_0\}$ 主要用于驱动帐篷-Logistic 映射产生随机数序列。一个优良的加密算法对于密钥应该是极端敏感的, 这样才能有效对抗密钥穷举攻击。密钥敏感性分析的目的在于衡量密钥的有效性, 当密钥发生微小变化时, 若加密同一个明文图像所得到的两幅密文图像有显著差异, 则该加密方案的密钥敏感性强。

本小节测试中, 以 Barbara 为样例, 以得到图 8(a) 中加密图像的密钥对 $\{k = \{\mu, r, x_0\}\}$ 为初值, 以 10^{-4} 为改变量, 任意改变其中一个密钥, 得到 3 个新的密钥对。以 3 个新密钥对加密 Barbara, 得到新的 3 幅加密图示于图 10。3 幅新的加密图与图 8(a) 进行同位置像素相减操作, 得到的差值图示于图 11。

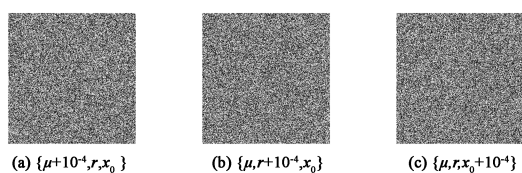


图10 新密钥对得到的加密图

Fig. 10 Ciphertext images generated from new secret key pairs

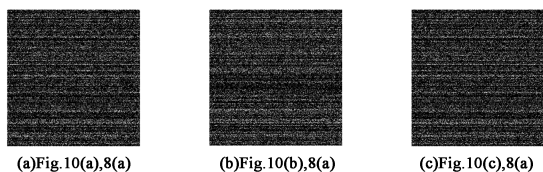


图11 新加密图与原加密图之间的差值图

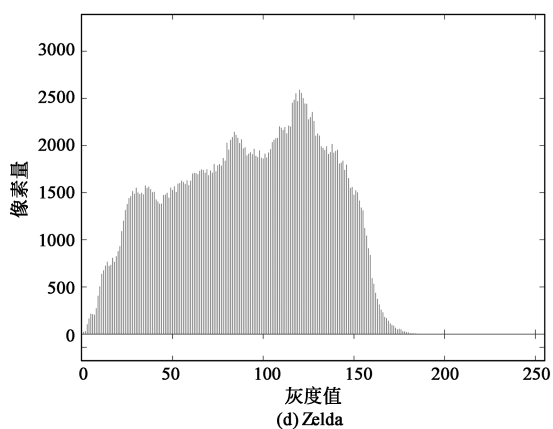
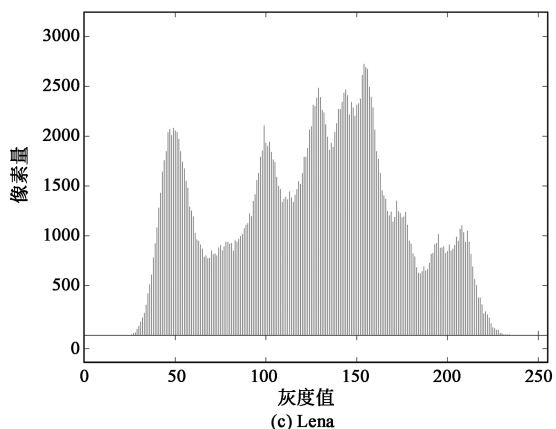
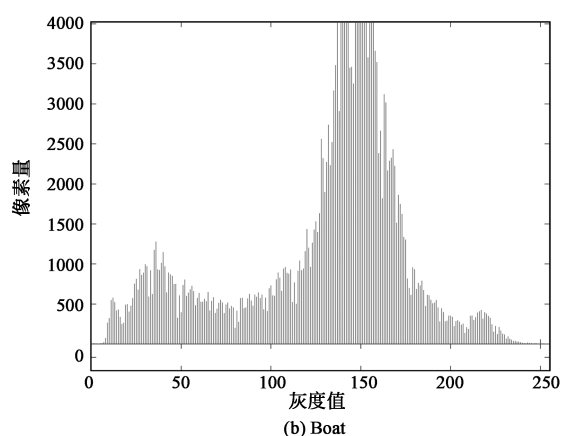
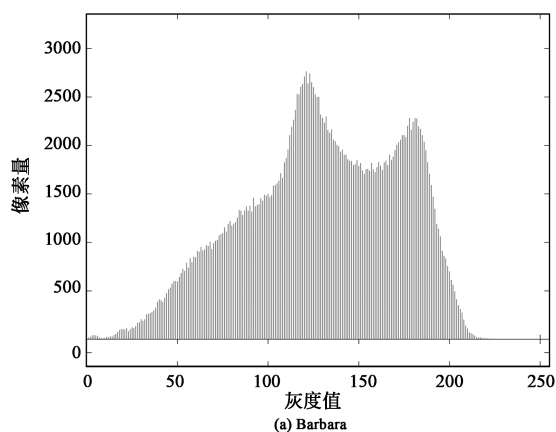
Fig. 11 Difference images between new ciphertext images and original images

从图 11 可以看出,3 幅差值图均呈现噪声形式,说明密钥值的微小改变造成了密文图像的显著差异性,这一点证实了本文所提出的算法具有高度的密钥敏感性。

4.2 抗统计攻击能力分析

窃密者通过获取大量加密图像便可以通过统计学知识来获取密文图像中包含的原始秘密图像信息,这种攻击方式称为统计攻击。具有强抗统计攻击能力的图像安全算法应当使得通过加密生成的图像类似于均匀分布的噪声。

图 12 展示了图 7 中的 4 幅原始秘密图像和图 8 中 4 幅加密图像的直方图。根据图 12 可以直观看出,明文图像的直方图有很大起伏,而加密图像则很平坦。因此可以认为加密图中像素为服从均匀分布的噪声点,本文所提出算法具有很强的对抗统计攻击的能力。



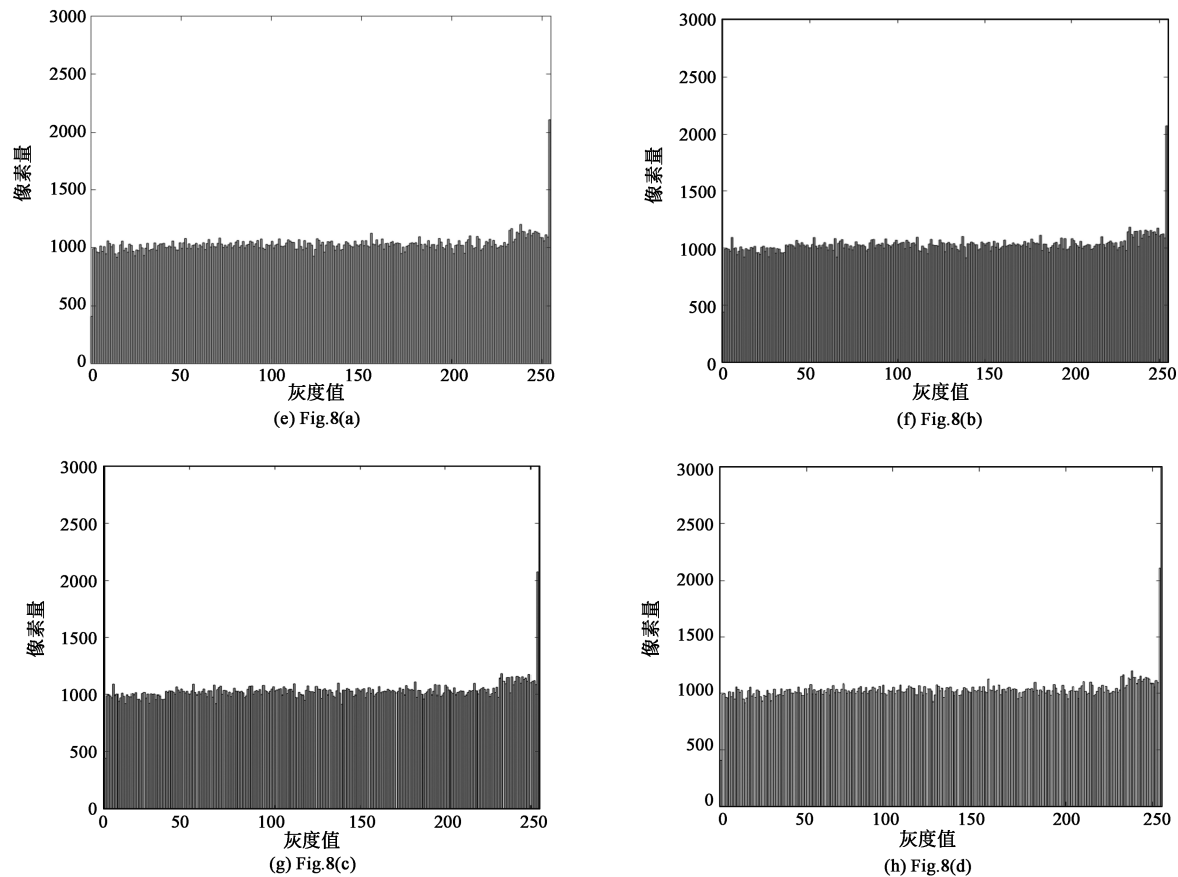


图 12 原始秘密图像的直方图(a~d)和图 8 中 4 幅加密图像的直方图(e~h)

Fig.12 Histogram of the original secret images (a~d) and histogram of the four encrypted images in Fig. 8 (e~h)

4.3 算法执行效率分析

为了满足大批量图片的实时性隐写要求,图像隐写算法的隐写-提取时间必须尽可能短。以图 7 所示的 4 幅图像作为测试样例,为证实本算法的高

执行效率,本算法的 100 次隐写-提取平均消耗时间与其他两种常用算法^[3-4]的执行耗时列于表 1。

通过表 1 可以看出,本文所提出的算法能够满足大批量图片实时隐写的要求。

表 1 算法隐写-提取平均耗时
Tab.1 Average steganography-extracting time consuming

隐写-提取平均耗时/s (100 次)			
	本文算法	文献[3]	文献[4]
Barbara	0.71	2.54	1.01
Boat	0.73	2.41	0.95
Lena	0.68	2.53	0.99
Zelda	0.65	2.53	0.93

5 结 论

针对重要数字图像的不可信信道安全传输问

题,本文基于帐篷映射和 Logistic 映射的级联设计了一种帐篷-Logistic 映射,在此基础上设计了一种基于帐篷-Logistic 映射和伪装图低位嵌入的图像隐写算法。该算法为置乱-混淆-低位嵌入结

构,通过结合传统置乱-混淆结构的图像加密方式和基于低位嵌入的图像隐写,极大地提高了算法的安全性。在分叉图和李亚普诺夫指数的测试中,本文所提出的帐篷-Logistic 映射均表现优异。

在密钥敏感性测试、抗统计攻击测试和隐写-提取用时测试实验中,本文所提出的图像隐写算法也表现出高度的安全性和极高的执行效率。因此,本文所提出算法具有一定实用性。

参 考 文 献:

- [1] 黄晓生.数字图像安全技术研究进展[J].华东交通大学学报,2006,23(1):82-86.
HUANG X S. A brief review on security of digital image [J]. *Journal of East China Jiaotong University*, 2006, 23(1): 82-86. (in Chinese)
- [2] 于琛.图像隐藏技术在信息安全中的应用研究[D].青岛:中国海洋大学,2006.
YU C. The application of image hiding technique in information security [D]. Qingdao: Ocean University of China, 2006. (in Chinese)
- [3] FRIDRICH J. Symmetric ciphers based on two-dimensional chaotic maps [J]. *International Journal of Bifurcation and Chaos*, 1998, 8(6): 1259-1284.
- [4] WANG X Y, YANG L, LIU R, *et al.* A chaotic image encryption algorithm based on perceptron model [J]. *Non-linear Dynamics*, 2010, 62(3): 615-621.
- [5] KANSO A, GHEBLEH M. A novel image encryption algorithm based on a 3D chaotic map [J]. *Communications in Nonlinear Science and Numerical Simulation*, 2012, 17(7): 2943-2959.
- [6] CHEN G R, MAO Y B, CHUI C K. A symmetric image encryption scheme based on 3D chaotic cat maps [J]. *Chaos, Solitons & Fractals*, 2004, 21(3): 749-761.
- [7] LIU L, ZHANG Q, WEI X P, *et al.* Image encryption algorithm based on chaotic modulation of Arnold dual scrambling and DNA computing [J]. *Journal of Computational and Theoretical Nanoscience*, 2011, 4(11/12): 3537-3542.
- [8] LAFE O. Data compression and encryption using cellular automata transforms [J]. *Engineering Applications of Artificial Intelligence*, 1997, 10(6): 581-591.
- [9] KEKRE H B, SARODE T, HALARNKAR P N. Partial image scrambling using Walsh sequency in sinusoidal wavelet transform domain [M]//BERRETTI S, THAMPI S M, SRIVASTAVA P R. *Intelligent Systems Technologies and Applications*. Cham: Springer, 2015: 471-484.
- [10] SONG C Y S, QIAO Y L. A novel image encryption algorithm based on DNA encoding and spatiotemporal chaos [J]. *Entropy*, 2015, 17(12): 6954-6968.
- [11] 雷正桥,肖迪.基于空域可恢复信息隐藏的图像安全人工退化算法[J].计算机科学,2015,42(3):162-166.
LEI Z Q, XIAO D. Artificial image security degradation algorithm based on invertible information hiding in spatial domain [J]. *Computer Science*, 2015, 42(3): 162-166. (in Chinese)
- [12] 穆晓芳,邓红霞,李晓宾,等.基于人工蜂群算法的两阶段图像隐写分析算法[J].计算机科学,2019,46(6):174-179.
MU X F, DENG H X, LI X B, *et al.* Two-phase Image Steganalysis algorithm based on artificial bee colony algorithm [J]. *Computer Science*, 2019, 46(6): 174-179. (in Chinese)
- [13] 陈嘉勇,王超,张卫明,等.安全的密文域图像隐写术[J].电子与信息学报,2012,34(7):1721-1726.
CHEN J Y, WANG C, ZHANG W M, *et al.* A secure image Steganographic method in encrypted domain [J]. *Journal of Electronics & Information Technology*, 2012, 34(7): 1721-1726. (in Chinese)
- [14] GUL E, OZTURK S. A novel hash function based fragile watermarking method for image integrity [J]. *Multimedia Tools and Applications*, 2019, 78(13): 17701-17718.
- [15] YAO X M, DU W C, HUANG M, *et al.* Pattern-based blind spatial image watermarking [C]//*Proceedings of the 2010 Third International Symposium on Intelligent Information Technology and Security Informatics*. Jing-gangshan, China: IEEE, 2010.
- [16] SU Q T, NIU Y G, WANG Q J, *et al.* A blind color image watermarking based on DC component in the spatial

- domain [J]. *Optik*, 2013, 124(23): 6255-6260.
- [17] 吴佳楠, 王世刚, 张迪, 等. 融合量子密钥真随机性的二值图像水印 [J]. 光学 精密工程, 2017, 25(11): 2968-2974. WU J N, WANG S G, ZHANG D, *et al.* Binary image watermark fusionbased on quantum key true randomness [J]. *Optics and Precision Engineering*, 2017, 25(11): 2968-2974. (in Chinese)
- [18] 王玉海, 朱长青, 苏守宝, 等. 结合感知哈希与数字水印的遥感影像认证方法 [J]. 光学 精密工程, 2016, 24(10s): 640-648. WANG Y H, ZHU C Q, SU S B, *et al.* An authentication method based on perceptual hashing and watermarking for remote sensing image [J]. *Optics and Precision Engineering*, 2016, 24(10s): 640-648. (in Chinese)
- [19] CARDOSO V, MIRANDA A S, BERTI E, *et al.* Geodesic stability, Lyapunov exponents, and quasinormal modes [J]. *Physical Review D*, 2009, 79(6): 064016.

作者简介:



穆 俊(1979—),男,云南临沧人,硕士,副教授,2008 年于云南大学获得硕士学位,主要从事计算机应用、计算机软件与理论、数据挖掘方面的研究。E-mail: Mujunmj0827@126.com