



基于单图像局部置乱和动态反馈扩散的混沌图像加密算法

崔业勤¹, 丁国超²

(1. 廊坊师范学院数学与信息科学学院, 河北 廊坊 065000;

2. 黑龙江八一农垦大学信息技术学院, 黑龙江 大庆 163319)

摘要: 提出一种基于单图像局部置乱和动态反馈的混沌图像加密算法。首先, 提出一种单图像局部置乱算法。其次, 在扩散阶段, 采用一种基于动态反馈的扩散策略来改变置乱后图像中的像素值, 通过动态反馈来改善图像的加密效果。最后, 实验结果表明, 与 3 种经典的算法相比, 提出的算法大大缩短了加密时间; 并且只通过一次加密, 其像素变化率和归一化平均变化强度值都可接近 99.6% 和 33.4%, 进一步证明了提出的算法具有良好的抵抗差分攻击的能力。

关键词: 混沌理论; 图像加密; 置乱; 动态反馈; 扩散

中图分类号: TP393

文献标识码: A

doi: 10.11959/j.issn.1000-0801.2016286

Chaotic image encryption algorithm based on single image local scrambling and dynamic feedback diffusion

CUI Yeqin¹, DING Guochao²

1. College of Mathematics and Information Science, Langfang Normal University, Langfang 065000, China

2. College of Information Technology, Heilongjiang Bayi Agricultural University, Daqing 163319, China

Abstract: A novel chaotic image encryption algorithm based on single image local scrambling and dynamic feedback diffusion was presented. Firstly, a single image local scrambling algorithm was proposed. Secondly, a novel dynamic feedback diffusion strategy was proposed to change the pixel values of the scrambled image in the phase of diffusion, by which improved the results of image encryption. Finally, the simulation results and performance analysis show that the number pixels change rate(NPCR) values and unified average changing intensity (UACI) values of the proposed algorithm can be close to 99.6% and 33.4%, showing that the proposed algorithm has better resistance to differential attacks and saves time compared with the other three classic algorithms.

Key words: chaotic theory, image encryption, scrambling, dynamic feedback, diffusion

收稿日期: 2016-10-11; 修回日期: 2016-11-13

通信作者: 丁国超, dgcer@163.com

基金项目: 国家自然科学基金资助项目 (No. 61500226); 黑龙江省自然科学基金资助项目 (No. F200804); 黑龙江省教育厅科技项目 (No. 11531056)

Foundation Items: The National Natural Science Foundation of China (No. 61500226), Natural Science Foundation of Heilongjiang Province of China (No. F200804), Science and Technology Project of Education Department of Heilongjiang Province of China (No. 11531056)



1 引言

图像信息生动、直观,是人们沟通交流的一种非常有效的手段,而全球性的互联网又是极不安全的,大量的图片信息通过类似 QQ 的聊天工具在互联网上传播,很可能会泄露个人信息,带来重大损失,甚至威胁到他人的人身安全,因而图像信息的安全问题变得越来越重要^[1]。在此背景下,图像加密技术的研究成为当今社会的一大热点。

数字图像信息不同于传统的文本信息,容量更大、相邻像素间相关性更强、数据冗余量更大^[2]。因此,加密图像信息不仅会大大降低加密速度,也导致传统的文本加密算法并不适合对数字图像进行加密^[3]。

混沌映射的许多内在特性如遍历性、伪随机性、不可预测性、对初始值和控制参数的极度敏感性等,都与密码学息息相关。于是,许多密码学家尝试将混沌理论引入密码学中,一些加密速度快、安全性高的图像加密算法陆续被提出。1989年,Matthews^[4]第一次将混沌学和密码学相结合,提出了一种基于变形的罗切斯特混沌的密码算法;赵亮等人^[5]设计了一种高维 Z 矩阵的混沌映射,并将其成功应用于图像加密中,提出了基于 Z 矩阵混沌映射和 PDP (plasma display panel) 模式的图像加密算法;董斌辉等人^[6]设计了一种确定性随机全排列的生成方法,用于构建一个随机置换模板,对明文进行置换加密。在此之后,通过一种替代变换置乱后图像的像素灰度值改变并产生互相依赖,使得加密算法具有置乱、替代、扩散等加密系统的基础要素;陆萍等人^[7]采用 Chebyshev 与 Logistic 混沌映射交替迭代生成混沌序列,在完成像素点重新散布后,根据其位置信息截取混沌二值序列实现对像素灰度值的加密。上述的加密算法都没有讨论置乱周期,因此安全性受到了很大的质疑;王静等人^[8]提出了一种超混沌图像加密算法,通过密文反馈方式控制算法中的密钥流,使得加密所需参数通过密文反馈与明文相关,将一个明文字节的影响扩散到更多的密文字节中。近年来,国外出现了一些新的方法,如 Zhou 等人^[9]创新性地提出了利用原图像的比特面作为安全密钥的全新图像加密算法,即 BPS 算法;Teng 等人^[10]提出了一种基于时空混沌系统的自适应比特级图像加密算法;Wang 等人^[11]用 Logistic 映射构造一个随机矩阵,去控制置乱后的图像中的像素点在比特级循环移位;韩凤英等人^[12]在改进算法像素值变换的过程中将像素值变换的扩

散矢量与像素位置变换的置乱矢量相耦合,提出一种基于混沌的改进型置乱替代结构图像加密算法,从而有效地提高密钥矢量的破解难度。

此外,近几年国内也出现了一些新的相关方法,如陈河山等人^[13]设计了一种基于离散混沌动力系统和小波分解的数字图像加密算法;邓晓衡等人^[14]提出了一种利用 Kent 混沌映射的能抵抗选择明密文攻击的图像加密算法;Zhang 等人^[15]在猫映射的基础上又提出了两种混沌系统,即时空非相邻的耦合映射网格和时空混合线性与非线性的耦合映射网格,与 Logistic 映射和耦合映射网格相比,它们有更显著的动态密码学特性;王欣宇等人^[16]充分利用了云计算环境中多节点的特点,结合混沌加密和 MapReduce 并行框架,提出一种并行混合混沌加密的新方案;张永红等人^[17]提出了一种基于 Logistic 混沌系统的快速数字图像加密算法,通过给定的密钥序列生成混沌系统的初值,利用此混沌矩阵与原图像进行按位异或运算得到加密图像;葛滨等人^[18]提出了一种基于超混沌的图像加密算法,该算法通过优化像素置乱、像素替换和密文扩散过程,进一步混淆明文图像和密文图像以达到加密效果。然而,当前大多数的混沌加密采用的都是自然混沌系统,它们并不具有严格意义上密码学所要求的保密性,即它们容易被攻破。此外,众多研究还表明,低维混沌在计算机有限精度下实现的加密存在周期较短的缺陷,如 Mackey-Glass 方程^[19]、CML-map 混沌序列^[20]等都被成功预测,这也是制约混沌加密被广泛应用的主要原因。

在上述混沌密码研究成果的基础上,提出一种新的基于单图像局部置乱和动态反馈的混沌图像加密算法。在置乱阶段,分析了经典的双图像置乱算法,提出了一种单图像局部置乱算法,即将一幅图分块作为双图像来进行置乱加密处理,这种方法能克服计算机有限精度缺陷,实现对数字图像的有效加密;在扩散阶段,提出了一种基于动态反馈的扩散策略,以改变置乱后图像中的像素值,并结合提出的单图像局部置乱算法,设计出基于单图像局部置乱和动态反馈的图像加密算法。实验结果和性能分析表明,提出的算法加密后的像素变化率和归一化平均变化强度值接近 99.6% 和 33.4%,均优于经典的 BPS 算法、Wang 的算法和 Teng 的算法,证明了提出的算法具有良好的抵抗差分攻击的能力;并且在确保相同的安全性能下,提出的算法能大大节约加密时间,更加适用于对实时要求较高的加密系统。

2 混沌密码学

自然界中的现象多为非线性现象,混沌现象就是一种发生于稳定系统,却呈现出无法估测状态的非线性现象。混沌冲破了牛顿力学的教规,被认为是 20 世纪物理学第 3 次重大革命。在 1963 年,洛伦兹在研究大气流动问题时揭示出混沌现象具有不可预言性和对初始值的极端敏感依赖性的特点^[21]。之后,大批学者致力于混沌理论的研究,使得其飞速发展,应用前景广阔。近年来,混沌应用于图像加密备受关注。

2.1 混沌及其主要性质

1975 年,学者李天岩^[22]在文章《周期三意味着混沌》中第一次对混沌这两个字做了严格的定义,具体定义如下。

假设 f 定义在闭区间 I 上且是连续自映射,如果 f 周期点的周期无上界,当 f 在 I 上的不可数子集 S 同时满足以下 3 个条件时,则此系统具有混沌现象。

条件 1: $\forall x, y \in S$, 当 $x \neq y$ 时, 有 $\limsup_{n \rightarrow \infty} |f^n(x) - f^n(y)| > 0$;

条件 2: $\forall x, y \in S$, 有 $\liminf_{n \rightarrow \infty} |f^n(x) - f^n(y)| = 0$;

条件 3: $\forall x, y \in S$ 与 f 中的任意的周期点 Y , 有 $\limsup_{n \rightarrow \infty} |f^n(x) - f^n(y)| > 0$ 。

其中, f^n 表示映射函数 f 的 n 阶导数。混沌主要具有以下性质。

- 有界性,混沌的轨迹局限在一个确定的区域内。
- 遍历性,混沌系统经过有限次叠代,其运动轨迹最终会遍历混沌吸引域内的所有点。
- 对初始条件和结构参数的敏感性,即混沌系统的初始条件和结构参数有极微小的改变都将导致混沌的运动轨迹截然不同。
- 长期不可预测性,混沌系统对初始条件和结构参数极度敏感,具有内随机特性,其结果是不可预测的。

2.2 混沌加密

随着信息技术的飞速发展,信息安全问题日益突出。国内外大批机构及学者专门从事此问题的研究工作,并催生了许多相关技术。密码技术就是其中的一种关键技术,为信息的安全传输提供了一种保障。密码学源于古希腊“斯巴达密码棒”,有两大研究方向,即研究加密技术的密

码编码学和研究破译技术的密码分析学。

密码学设计通常是基于两个基本原则^[24]:混乱(confusion)和扩散(diffusion)。其中,混乱亦被称为置乱(scrambling)。混沌与密码学具有紧密的联系,其伪随机性、对初始值的极度敏感性、遍历性能够很好地与密码学相结合。基于混沌的扩散和置乱与密码学的要求一致,能够对信息进行安全加密。大批学者投身于混沌理论与密码学的研究中,并已取得丰硕的研究成果,提出了大量基于混沌的加密算法。目前,混沌密码学已经成为密码学领域一个不可分割的研究方向。

3 基于单图像局部置乱和动态反馈的混沌图像加密算法

本节将给出基于单图像局部置乱和动态反馈的图像加密算法。图像加密主要分为两个步骤:置乱和扩散。鉴于此,首先在经典的双图像置乱算法基础上,提出一种单图像局部置乱算法,能有效地对单图像进行置乱;接着提出一种基于动态反馈的扩散策略,并结合先前提出的单图像局部置乱算法设计出一种基于单图像局部置乱和动态反馈的图像加密算法。

3.1 比特面分解

在参考文献[9]中,Zhou 等人介绍了一种比特面分解方法,即二进制比特面分解(binary bit-plane decomposition, BBD)。一个非负的十进制数 N 可被表示为一个二进制序列,如:

$$N = \sum_{i=0}^{n-1} b_i 2^i = b_0 2^0 + b_1 2^1 + \cdots + b_{n-1} 2^{n-1} \quad (1)$$

其中, n 取正整数。

在一幅灰度图像中,每个像素值的取值范围是 $[0, 255]$, 它可表示为一个 8 位的二进制序列。而 Zhou 等人^[9]提出的 BBD 比特面分解方法的主要思想就是将一幅灰度图像分解成 8 个二进制比特面,每个像素的二进制表示中的第 i 位共同组成了第 i 个比特面。这样一幅灰度图像可以由这 8 个 BBD 比特面所确定,并且图像中每个像素点值的信息都均匀地分布在这 8 个比特面中。

3.2 单图像局部置乱算法

提出的单图像局部置乱算法是受到经典的双图像置乱算法的启发,如用双图像置乱算法对图 1 的标准的大脑和房屋灰度图像进行置乱。

从图 1 可以看出,双图像置乱算法可以较好地

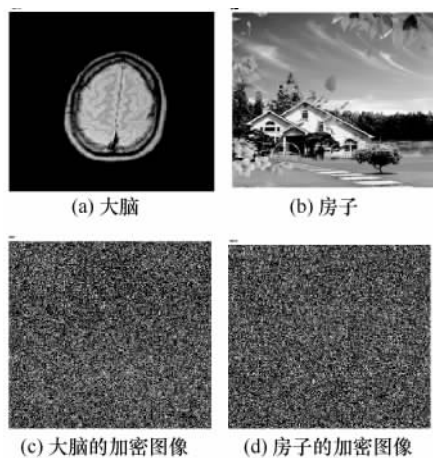


图 1 双图像置乱算法处理图例

大脑和房子图像进行加密；尽管原灰度图像差异很大，但加密后的密文图像却几乎一样，这意味着双图像置乱算法能够有效地让两幅图像中的像素均匀分布，从而达到极好的加密效果。

既然双图像置乱可以达到很好的加密效果，那么对于单图像来说，可以采用局部置乱的方法将单图像分成双图像，通过构造位置信息表来达到置乱的目的，这即是提出的基于局部置乱的单图像加密算法思想。算法将一幅图像按上下分成两块，如果图像为奇数行，可增加一行变为偶数行。然后按照双图像置乱方式对块图像进行置乱，最后合成单图像的加密图像，其流程如图 2 所示。

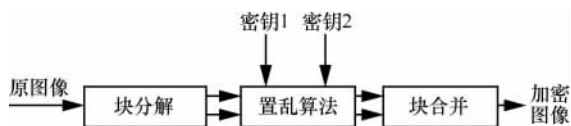


图 2 单图像局部置乱算法流程

提出的单图像局部置乱算法的主要步骤如下。

步骤 1 先用混沌系统产生两个二进制序列密钥流，即用密钥 $key_1(x_0, \mu_1)$ 产生两个混沌序列 a_1 和 a_2 ，其中 x_0, μ_1 为混沌系统的初始值和控制参数。将序列通过式(2)量化后，再对其进行矩阵填充，得到这两个量化后的混沌矩阵 A_1 和 A_2 ，其尺寸大小均为 $M \times N$ 。

$$a_i = \text{mod}(\text{floor}(a_i \times 10^{14}), M) + 1 \quad (2)$$

步骤 2 利用这两个量化后的混沌矩阵 A_1 和 A_2 ，根据式(3)~式(5)分别构造 X 坐标信息表 XT 、 Y 坐标信息表 YT 和交换控制表 CT ：

$$CT(i,j) = \begin{cases} 1, & \text{abs}(A_1(i,j)-i) < M/4 \text{ 或 } \text{abs}(A_2(i,j)-i) < N/40 \\ 0, & \text{其他} \end{cases} \quad (3)$$

$$XT(i,j) = \begin{cases} \text{mod}(A_1(i,j) + M/4, M) + 1, & \text{abs}(A_1(i,j)-i) < M/4 \\ A_1(i,j), & \text{其他} \end{cases} \quad (4)$$

$$YT(i,j) = \begin{cases} \text{mod}(A_2(i,j) + N/4, N) + 1, & \text{abs}(A_2(i,j)-i) < N/4 \\ A_2(i,j), & \text{其他} \end{cases} \quad (5)$$

步骤 3 根据表 XT 、 YT 和 CT ，从左上角开始，按照从左到右、从上到下的方向顺序交换块图像中的元素。将第一块图像表示为 image1 ，第二块表示为 image2 。具体地，在 image1 中若 $CT(i,j)=0$ ，则交换元素 $\text{image1}(i,j)$ 与 $\text{image1}(XT(i,j), YT(i,j))$ ；否则交换元素 $\text{image1}(i,j)$ 与 $\text{image2}(XT(i,j), YT(i,j))$ 。同理，在 image2 中如果 $CT(i,j)=0$ ，则交换元素 $\text{image2}(i,j)$ 与 $\text{image2}(XT(i,j), YT(i,j))$ ；否则交换元素 $\text{image2}(i,j)$ 与 $\text{image1}(XT(i,j), YT(i,j))$ 。

下面采用提出的单图像局部置乱算法来对标准的 256 dpi×256 dpi 的灰度 Lena 图像做加密。加密效果如图 3 所示，可以看到，算法起到了很好的置乱加密效果。

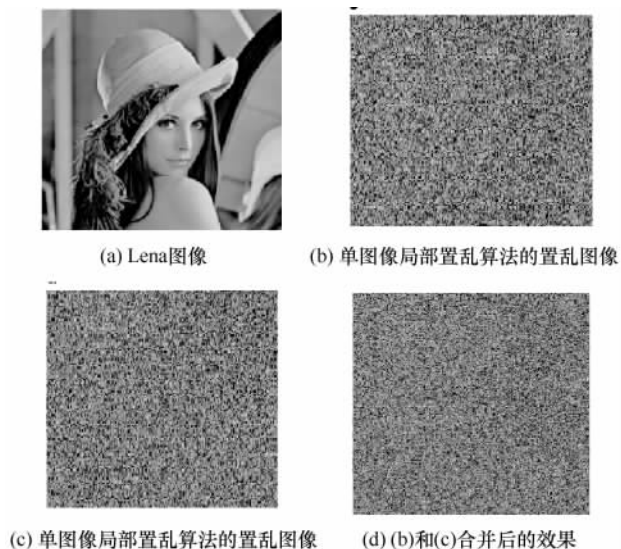


图 3 单图像局部置乱算法处理图例

3.3 所提图像加密算法流程

在第 3.2 节的基础上，采用动态反馈的扩散策略，通过反馈循环来改善图像的加密效果。为此，提出了基于单图像局部置乱和动态反馈扩散的图像加密算法。其主要流程如图 4 所示。

具体步骤如下。

第一阶段：对即将加密的图像实施单图像局部置乱算法(见第 3.2 节)

步骤 1 将待加密图像按上下分为两块；

步骤 2 根据混沌矩阵分别构造 X 坐标表 XT 、 Y 坐

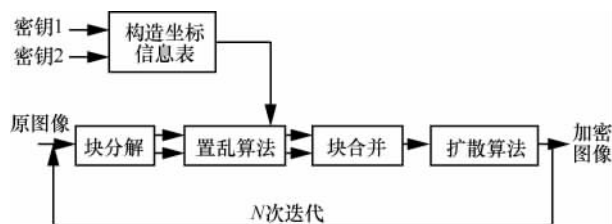


图4 提出算法的整体流程

标表 YT 和交换控制表 CT ;

步骤3 根据表 XT 、 YT 和 CT , 从左上角开始, 按照从左到右、从上到下的方向顺序交换块图像中的元素。

第二阶段: 基于动态反馈的扩散策略

步骤1 将置乱后的图像从上到下拉成一个一维向量 P , 即向量的长度为 $M \times N$;

步骤2 对扩散策略的 $k(z_0, \mu_3)$ 加以控制来产生一个密钥流, 其中元素的范围均取 1 到 M 之间, 其中, z_0 、 μ_3 分别表示密钥流的初始化值和初始化参数。并对序列进行量化处理, 即:

$$k = \text{mod}(\text{floor}(k_1 \times 10^{14}), 256) \quad (6)$$

步骤3 计算向量中除第一个元素之外的所有元素和, 记为 S ;

步骤4 用 $s_0 = \text{mod}(S, 256)$ 计算 s_0 的值, 用来加密第一个元素, 即:

$$p(1) = s_0 \oplus p(1) \oplus k(1) \quad (7)$$

步骤5 设置 $i=2$, 根据式 (8) 和式 (9) 计算动态索引 kt_1 和 kt_2 的值。用第 kt_1 和 kt_2 个元素来加密第 i 个元素。

$$kt_1 = \text{floor}(\text{mod}(p(i-1) + k(i)), 256) / 256 \times (i-1) + 1 \quad (8)$$

$$kt_2 = \text{floor}(\text{mod}(p(i-1) + k(i)), 256) / 255 \times (L' - i - 1) + i + 1 \quad (9)$$

步骤6 利用式 (10) 加密第 i 个元素, 即:

$$p(i) = p(i) \oplus k(i) \oplus p(kt_1) \oplus p(kt_2) \quad (10)$$

步骤7 设置 $i=i+1$, 跳回到步骤 5, 直到 $i=L-1$ 停止迭代。

步骤8 将加密后的向量 P 转换成 $M \times N$ 的密文图像。从上述的详细步骤可以看出, 该算法包括一种图像局部置乱方法和一种基于动态反馈的扩散策略。首先将原图像对称分为两块, 若按行分块且行数为奇数则随意增加一行。同理, 若按列分块且列数为奇数则随意增加一列。然后, 根据混沌矩阵分别构造 X 坐标表、 Y 坐标表和交换控制表。在构造表的过程中, 保证像素的位置始终在一个确定的约束范围内。通过查找 X 坐标表、 Y 坐标表得到待置乱像素的交换位置, 交换控制表用来控制像素是与当前图

像中像素交换还是与另一块图像中的像素交换。最后, 用基于动态反馈的扩散策略改变置乱后的图像中的像素值完成对图像的最终加密。其中, 步骤 5 中的两个动态索引分别用来确定已加密序列和待加密序列中的像素位置。确定的两个像素用来加密当前待加密像素。

需要说明的是, 单图像置乱算法能够有效地置乱两幅图像, 置乱后的两幅图像在视觉上具有一致性。并将此算法延伸, 从而提出了一种基于动态反馈的扩散策略, 该策略与单图像局部置乱算法结合组成一个非常安全可靠的加密系统。在第 4 节的实验仿真也将证明该系统具有很好的安全性能。

4 仿真测试

在实验部分, 对提出的加密算法的性能进行仿真实验, 分别从直方图分析、差分攻击分析和算法复杂度分析 3 个角度来评价算法的加密效果。为了控制变量以及准确对比各个算法的优劣, 在实验过程中, 选取的测试图像均是尺寸为 256 dpi × 256 dpi 为标准的 8 bit 灰度图像。用于实验的电脑配置为 2.66 GHz CPU, 内存 2 GB, 操作系统为 Windows XP SP3 32 bit, 仿真环境为 MATLAB 7.8.0 (R2009a)。

4.1 直方图分析

图像的直方图展示了像素强度值的分布。而一个安全的加密算法应该能使加密后的图像有相同的分布。因此, 分别采用 Lena、Brain、Cameraman、Barbara 和 Couple 等多组标准图像进行直方图分析实验, 采用提出的算法分别对其进行加密, 并观察其原始图像即其加密图像的直方图, 如图 5 和图 6 所示。

在图 5(b) 中, 密文图像的所有灰度值在区间 $[0, 255]$ 上具有一致的分布。这与图 5(a) 中明文图像 Lena 的分布有明显的不同。而图 5(c) 中恢复图像的直方图与图 5(a) 中原图像的直方图一致。从图 6 中对不同图像横向加密对比可以看出, 尽管加密的原图像差异性很大, 但所有的加密图像都具有一致的分布。这表明该算法能够很好地抵抗统计攻击, 并能通过解密算法有效恢复。

4.2 差分攻击分析

如果一个像素值的改变引起密文图像的完全变化就说明该算法能够较好地抵御差分攻击。像素变化率 (number pixels change rate, NPCR)^[22] 和归一化平均变化强度 (unified average changing intensity, UACI)^[23] 是衡量图像加密算法抵抗差分攻击能力的重要指标。选取 Brain、

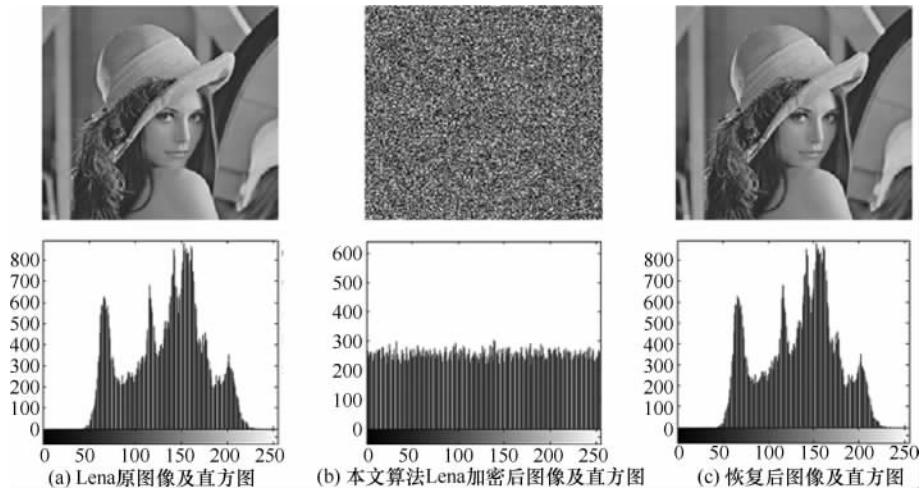


图 5 Lena 图像直方图分析

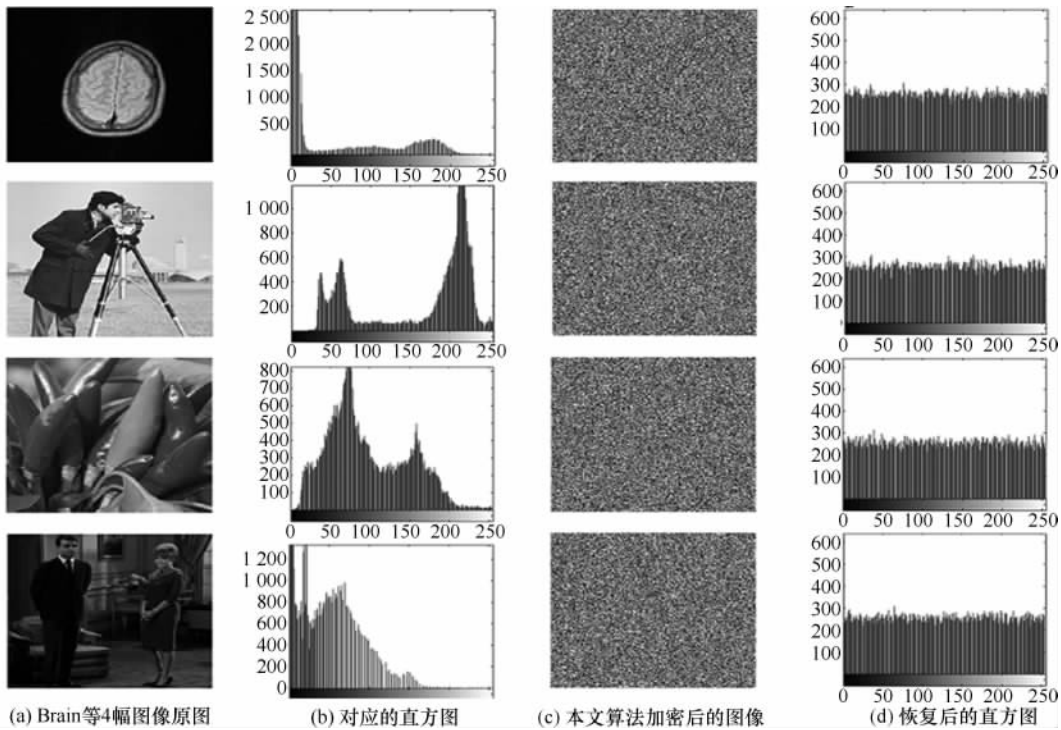


图 6 多组标准图像直方图分析

Couple 和 Cameraman 作为实验图像,并分别计算其 NPCR 和 UACI 值,结果见表 1。

表 1 3 种图像的 NPCR 和 UACI 值

测试图像	NPCR	UACI
Brain	0.995 635 9%	0.334 410%
Couple	0.996 163 2%	0.335 536%
Cameraman	0.996 195 3%	0.336 124%

而如果用经典的 BPS 加密算法^[9]、Teng 的算法^[10]和 Wang 的算法^[11]对上述 3 个标准图像分别进行加密,相应的 NPCR 与 UACI 值分别见表 2~表 4。

从表 1~表 4 中可以看出,采用提出的算法加密后,NPCR 和 UACI 值接近 99.6%和 33.4%,比经典的 BPS 加密算法、Teng 的算法和 Wang 的算法高,从而证明了提出的算法相对具有良好的抵抗差分攻击的能力。再有,本文在单图像分块局部置乱的基础上,用基于动态索引的扩散

表 2 BPS 算法加密图像的 NPCR 和 UACI 值

测试图像	NPCR	UACI
Brain	0.794 764%	0.300 988%
Couple	0.802 012%	0.311 952%
Cameraman	0.816 521%	0.353 322%

表 3 Teng 的算法加密图像的 NPCR 和 UACI 值

测试图像	NPCR	UACI
Brain	0.895 665%	0.315 616%
Couple	0.884 551%	0.309 879%
Cameraman	0.831 964%	0.299 461%

表 4 Wang 的算法加密图像的 NPCR 和 UACI 值

测试图像	NPCR	UACI
Brain	0.854 971%	0.298 324%
Couple	0.825 987%	0.308 481%
Cameraman	0.836 544%	0.315 564%

算法改变置乱后的图像中的像素值以达到二次置乱的效果,因此加密效果得到了大大的加强,从而能很好地抵抗差分攻击。

4.3 算法复杂度分析

本次实验仍然选择与经典的 BPS 算法、Teng 的算法和王 Wang 的算法作对比实验,主要针对算法复杂度和耗时方面进行对比。在提出的算法中,主要耗时的算法步骤在于控制表的构造、计算动态索引值,像素交换等操作;在 BPS 和 Teng 的算法中,主要耗时的步骤在于大量的排序与查找操作;而 Wang 的算法需要将明文图像分成多组,然后构造多个动态 S-box 去置换像素。

采用提出的算法及对对比算法将 256 dpi×256 dpi 的 Lena、Couple 和 Babara 灰度图像加密,多次试验取平均统计其算法耗时情况,结果见表 5。

表 5 4 种加密算法的耗时对比 (单位:s)

加密算法	Lena	Couple	Barbara
提出的算法	0.62	0.67	0.63
BPS	2.52	2.43	2.50
Wang 的算法	1.23	1.09	1.10
Teng 的算法	2.83	2.10	2.84

从表 5 中可以看出,加密 Lena 图像所提出的算法耗时 0.62 s。而用 BPS、Wang 的算法和 Teng 的算法则分别需要 2.52 s、1.23 s 和 2.83 s。本文的算法加密时间要远远小于其他 3 种算法,由此证明了提出的加密算法复杂度更

低,比上述的这 3 种常用的加密算法要快得多。

5 结束语

提出一种基于单图像局部置乱和动态反馈的混沌图像加密算法。该算法包括一种图像局部置乱算法和一种基于动态反馈的扩散算法。受到双图像置乱加密算法的启发,局部置乱可以很好地将单图像进行有效的加密;而两个反馈扩散则分别用来确定已加密序列和待加密序列中的像素位置。确定的两个像素用来加密当前待加密像素。实验结果和性能分析表明,本文提出的基于单图像局部置乱和动态反馈的数字图像加密算法只通过一次迭代就能达到很好的安全性能。然而,图像数据容量越来越大,已有的算法加密速度过慢,并行计算处理数据已是趋势,因此后续的研究将从解决该问题出发,旨在设计有效可行的并行加密算法。

参考文献:

[1] JAY ANTHI V E, RAJAMANI V, KARTHIKAYEN P. Performance analysis for geometrical attack on digital image watermarking [J]. International Journal of Electronics, 2011, 98(11): 1565-1580.

[2] WANG Y, WONG K W, LIAO X, et al. A chaos-based image encryption algorithm with variable control parameters[J]. Chaos, Solitons & Fractals, 2009, 41(4): 1773-1783.

[3] YOON J W, KIM H. An image encryption scheme with a pseudorandom permutation based on chaotic maps [J]. Communications in Nonlinear Science and Numerical Simulation, 2010, 15(12): 3998-4006.

[4] MATTHEWS R. On the derivation of a “chaotic” encryption algorithm[J]. Cryptologia, 1989, 13(1): 29-42.

[5] 赵亮. 数字混沌图像加密算法的分析与设计 [D]. 重庆: 重庆大学, 2009.

ZHAO L. Analysis and design of digital chaotic image encryption algorithms [D]. Chongqing: Chongqing University, 2009.

[6] 董斌辉, 周健勇. 混沌随机全排列置换加密算法及应用[J]. 计算机工程与应用, 2011, 47(8): 59-61.

DONG B H, ZHOU J Y. Transposition encryption algorithm based on chaotic random permutation and its application [J]. Computer Engineering and Applications, 2011, 47(8): 59-61.

[7] 陆萍, 董虎胜, 马小虎. 基于混合混沌与位分解的图像置乱改进算法[J]. 计算机工程与应用, 2011, 47(21): 191-194.

LU P, DONG H S, MA X H. Image scrambling optimization algorithm based on mixed chaos system and bit decomposition[J]. Computer Engineering and Applications, 2011, 47(21): 191-194.



- [8] 王静, 蒋国平. 一种超混沌图像加密算法的安全性分析及改进[J]. 物理学报, 2011, 60(6): 83-93.
WANG J, JIANG G P. Cryptanalysis of a hyper-chaotic image encryption algorithm and its improved version [J]. Acta Physica Sinica, 2011, 60(6): 83-93.
- [9] ZHOU Y C, CAO W J, CHEN C L P. Image encryption using binary bitplane[J]. Signal Processing, 2014, 100(7): 197-207.
- [10] TENG L, WANG X. A bit-level image encryption algorithm based on spatiotemporal chaotic system and self-adaptive [J]. Optics Communications, 2012, 285(20): 4048-4054.
- [11] WANG X, WANG Q. A novel image encryption algorithm based on dynamic s-boxes constructed by chaos [J]. Nonlinear Dynamics, 2014, 75(3): 567-576.
- [12] 韩凤英, 朱从旭. 新型置换和替代结构的图像混沌加密算法[J]. 武汉大学学报: 理学版, 2014, 60(5): 447-452.
HAN F Y, ZHU C X. New permutation-substitution image encryption scheme based on chaos [J]. Journal of Wuhan University(Natural Science Edition), 2014, 60(5): 447-452.
- [13] 陈河山, 吕珍珍, 罗伟. 一个基于离散混沌加密的数字水印算法[J]. 计算机科学, 2014, 41(12): 48-52.
CHEN H S, LV Z Z, LUO W. Digital image watermarking algorithm based on dispersed chaotic mapping system [J]. Computer Science, 2014, 41(12): 48-52.
- [14] 邓晓衡, 廖春龙, 朱从旭, 等. 像素位置与比特双重置乱的图像混沌加密算法[J]. 通信学报, 2014(3): 216-223.
DENG X H, LIAO C L, ZHU C X, et al. Image chaotic encryption algorithm based on dual scrambling of pixel position and bits[J]. Journal on Communications, 2014(3): 216-223.
- [15] ZHANG Y Q, WANG X Y. A new image encryption algorithm based on non-adjacent coupled map lattices [J]. Applied Soft Computing, 2015(26): 10-20.
- [16] 王欣宇, 杨庚, 闵兆娥. 基于 MapReduce 的并行混合混沌加密方案[J]. 计算机应用研究, 2015, 32(6): 1757-1760.
WANG X Y, YANG G, MIN Z E. Parallel mixed chaotic encryption scheme on MapReduce [J]. Application Research of Computers, 2015, 32(6): 1757-1760.
- [17] 张永红, 张博. 基于 Logistic 混沌系统的图像加密算法研究[J]. 计算机应用研究, 2015, 32(6): 1770-1773.
ZHANG Y H, ZHANG B. Algorithm of image encrypting based on Logistic chaotic system [J]. Application Research of Computers, 2015, 32(6): 1770-1773.
- [18] 葛滨, 鲁华祥, 陈旭, 等. 基于超混沌的快速图像加密算法[J]. 系统工程与电子技术, 2016, 38(3): 699-705.
GE B, LU H X, CHEN X, et al. Fast image encryption algorithm based on hyper-chaos [J]. Journal of Systems Engineering and Electronics, 2016, 38(3): 699-705.
- [19] NAMAJUNAS A, PYRAGAS K, TAMASEVICIUS A. An electronic analog of the mackey-glass system[J]. Physics Letters, 1995, 201(1): 42-46.
- [20] SIK D, SANDBERG A A. Chromosomes and causation of human cancer and leukemia: XXXIX. usual and unusual findings in Ph1-positive CML[J]. Cancer, 1980, 46(10): 2227-2237.
- [21] LORENZ E N. Deterministic non-periodic flow[J]. Journal of the Atmospheric Sciences, 1963, 20(2): 130-141.
- [22] LI T Y, YORKE J A. Period three implies chaos [M]. Berlin: Springer, 2004, 82(82): 985-992.
- [23] CARLET C. On the confusion and diffusion properties of Maiorana-McFarland's and extended Maiorana-McFarland's functions[J]. Journal of Complexity, 2004, 20(2, 3): 182-204.

[作者简介]



崔业勤(1973-),女,廊坊师范学院副教授、系主任,主要研究方向为图形图像处理、计算机视觉等。



丁国超(1980-),男,博士,黑龙江八一农垦大学副教授、研究生处学科建设科科长,主要研究方向为生物信息检测、机器学习等。