

引用格式:李振汕. 基于混沌算法及压缩感知的图像压缩加密算法研究[J]. 微电子学与计算机, 2020, 37(2): 87-90. [LI Z S. Research on image compression encryption algorithm based on chaos algorithm and compression perception [J]. Microelectronics & Computer, 2020, 37(2): 87-90]

基于混沌算法及压缩感知的图像压缩加密算法研究

李振汕

(广西警察学院 信息技术学院, 广西 南宁 530200)

摘 要: 文章根据三个一维映射通过串联及并联构造了一维复合混沌系统, 并提出结合压缩感知理论进行优化改进. 利用两幅图像灰度级为 256 对改进后的算法进行仿真实验, 仿真实验结果表明, 改进后的算法具有良好的抗干扰能力, 通过原图像和加密处理后的加密图像在直方图、相邻像素相关系数等对比分析可以看出, 此次提出的加密算法具有非常好的效果.

关键词: 混沌算法; 压缩感知; 图像加密; 复合混沌映射

中图分类号: TP3

文献标识码: A

文章编号: 1000—7180(2020)02—0087—04

Research on image compression encryption algorithm based on chaos algorithm and compression perception

LI Zhen-shan

(School of Information Technology, Guangxi Police College, Nanning 530200, China)

Abstract: In this paper, a one-dimensional composite hybrid system is constructed in series and in parallel according to three one-dimensional mapping, and the optimization and improvement are put forward in combination with the compression-aware theory. The improved algorithm is simulated with two image gray levels of 256. The experimental and simulation results show that the improved algorithm has good anti-interference ability. Through the comparison and analysis of the original image and the encrypted image in histogram, the correlation coefficient of adjacent pixels and so on, it can be seen that the proposed encryption algorithm has a very good effect.

Key words: chaos algorithm; compression perception; image encryption; composite chaotic mapping

1 引言

互联网技术的发展给人们的生产生活带来了极大的便利,但是在信息的交换和传输过程,存在着越来越严重的信息安全问题,其中最为显著的就是图像数据.相较于声音和文本信息,图像更为形象直观,包含的信息更加丰富,目前在多个领域中都有着非常广泛的应用,因而图像数据的传输安全越来越受到人们的关注和重视.^[1]因此必须要加强互联网信息安全,采取加密措施来避免信息的泄露.常用的安全防御技术主要有身份认证、入侵检测、加密技术

等,其中的加密技术是十分关键和基础的环节.^[2]

混沌理论最早诞生于上世纪六十年代,由于其混沌典型特征、敏感性、混合特性等,经过几十年的发展,目前广泛应用于生物、经济、通信等各个科技领域之中.^[3]由于混沌所具有的各种典型特征和加密系统特性有着非常好的对应关系,因而混沌系统适用于进行图像的加密应用之中.随着科学技术和理论水平的不断发展,各类攻击手段层出不穷,攻击水平也快速提升,原本安全性不错的加密算法也逐渐被破译.当前,关于图像加密算法还未行程统一的通用标准,图像加密技术在不断发展和完善.将混沌

理论应用于图像加密之中,有助于完善图像加密理论和技术的应用^[4-9].

2 基于压缩感知的混沌系统改进

2.1 混沌系统改进优化

为了取得良好的图像加密效果,此次设计了一维复合混沌系统,包含了 3 个一维映射进行并联后串联,系统结构图如图 1 中所示.不同于传统的单向扩散,此次采用了双向扩散策略,可以有效减少整体论述,进而有效减少时间消耗.

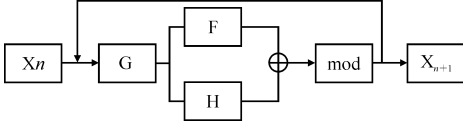


图 1 一维复合混沌系统结构图

该一维混沌系统结构中, G 、 F 和 H 都采用的是—维映射,其中的 mod 表示的是对 1 取模操作. 三种映射的定义具体如下:

$$\begin{cases} x_{n+1} = b \cos(\pi x_n / 2) \\ x_{n+1} = \gamma x_n (1 - x_n) \\ x_{n+1} = a \sin(\pi x_n) \end{cases} \quad (1)$$

式中, a, b, γ 是对应的控制参数,其取值区间分别在 $(0, 1]$, $(0, 4]$, $(0, 1]$. 由于是由三种映射所组合的,因此存在 3 种组合并对应产生 3 种不同的一维复合混沌映射,利用正弦、余弦以及逻辑斯的映射所共同构建的混沌系统,其最大的不足就是序列分布显著不均匀,如果要将其应用于要求较高的图像加密中时,就必须对该系统方法进行完善改进. 通过仿真实验,将原正弦映射替换成为帐篷映射有:

$$\begin{cases} x_{n+1} = \begin{cases} \text{mod}(a \sin(\pi \mu x_n) + \gamma \mu x_n (1 - \mu x_n), 1) \\ 0 \leq x_n \leq 0.5 \\ \text{mod}(a \sin(\pi \mu (1 - x_n)) + \gamma \mu (1 - x_n) (1 - \mu (1 - x_n)), 1) \\ 0.5 < x_n \leq 1 \end{cases} \end{cases} \quad (2)$$

随后可以利用二维分叉图、一维分叉图、二维李雅普诺夫指数图来刻画它对应的力学特性. 式(2)所表示的,是在一个较大的参数空间之中,一维复合混沌映射能够输出为分布较为均匀的混沌序列,由此可以满足于图像加密对混沌映射的要求,也便于构造出压缩感知过程中测量矩阵.

2.2 压缩感知

信号的稀疏性就是可压缩性,设长度为 N 的待重构可压缩信号为 $x \in R^N$,紧框架稀疏变换基为

Ψ ,那么就可以得到关于 x 的 K 稀疏公式为:

$a = \Psi x$ s. t. $\|a\|_0 = K$ ($K \ll N$),从该式中可以看出,进一步从相对较少的随机线性测量值重构精确信号,用 $y = \Phi x$ 来表示测量过程,用 Φ 来表示和稀疏变换基没有关系的测量矩阵,于是可以进行测量构成,信号重构问题实际上就是求解最优化问题,利用非线性方法数值求解公式

$$\arg \min_{x, a} \|\hat{a}\|_1 \text{ s. t. } \Phi \Psi^{-1} \hat{a} = y \text{ 即可完成.}$$

3 基于改进算法的图像加密过程

改进后图像加密算法的加密流程具体包含了采样、置乱以及扩散这三个步骤. 经由 SHA256 方法生成明文图像的密钥,该密钥具体包含了混沌系统中的扩散初始值、变换次数等,明文图像首先是经过 CS 加密得到采样图像数据分块,其次利用 FLT 变换对这些分块进行置乱后线性调整至 $[0, 255]$ 的范围,最后完成扩散操作. 假设钥值 K ,设混沌系统的初始值分别为 x_{01}, x_{02} ,扩散初始值为 c_0 ,FLT 变换次数为 num ,由此可以得到各参数的计算公式为:

$$\begin{cases} x_{01} = (k_1 \oplus k_2 \oplus \dots \oplus k_{10}) / 256 \\ x_{02} = (k_{11} \oplus k_{12} \oplus \dots \oplus k_{20}) / 256 \\ c_0 = k_{21} \oplus k_{22} \oplus \dots \oplus k_{30} \\ num = 3 + \text{mod}(k_{31} \oplus k_{32}, 3) \end{cases} \quad (3)$$

进行迭代计算,迭代次数为 $N + 1000$ 次,并对序列进行排序,剔除前 1000 个序列得到序列 X (长度为 N),使用序列 X 生成 $M \times N$ 的随机循环测量矩阵为减小该矩阵相干性,将矩阵中的首个元素进行调整,随后利用小波变换将原图像表示为稀疏图像数据 A ,使用随机循环测量矩阵 Φ 对其测量后获得数据 Y . 设 m 为 M, N 最大公因子,将数据 Y 分解成为 $m \times m$ 个块,对其进行 num 轮变换得到 Y_1 ,并将 Y_1 的最大值和最小值分别调整为 255 和 0,分别设:

$$\begin{cases} \text{coeff}_1 = 255 / (\max - \min) \\ \text{coeff}_2 = 255 * \min / (\max - \min) \end{cases} \quad (4)$$

将 Y_1 变换成 Y_2 得到 $Y_2(i, j) = \text{coeff}_1 * Y_1(i, j) + \text{coeff}_2$,对该公式迭代扩散后得到密钥流 K ,其表达式为 $K = \text{mod}(\text{floor}(Y * 10^{15}), 256)$,同时对 Y_2 进行扩散操作后转换为一维序列 P :

$c_i = c_{i-1} \oplus k_i \oplus \text{mod}(p_i + k_i, 256), i = 1, 2, \dots, MN$,为能够获取得到更好扩散特性,将 C 进行转置后重新执行前述步骤后得到加密图像. 加密图像需要进行逆向解密,首先是进行解扩散操作,其次

开展线性调整逆操作,将其进行 FLT 逆变换,见公式(4),使用重构算法恢复出原图像,使其能够为人们使用.

$$IELT_n = \frac{(F_{n+1} + F_{n-1}) * (-1)^n F_{n+1} (-1)^{n+1}}{(F_n + F_{n-2}) * (-1)^{n+1} F_n (-1)^n}$$

(5)

4 算法仿真实验结果分析

此次选取两种不同大小的图像 A1、A2 来进行改进算法的性能测试,具体的参数设置为 $\alpha=0.985, \mu=0.615, \gamma=1.151$,设置压缩比 M/N 为 0.75,利用此次优化改进算法进行信噪比重构,重构后的图像经过加密后基本上已经看不出任何与原图有关的意义内容.随着压缩比的增加,得到的 PSNR 值逐渐提升,算法在重构性能上虽然表现的略低,但是具有较好的安全性能和效率.图像统计分析主要采用直方图来进行图像分布特性的研究,为了进行防止统计分析攻击,绘制出加密后图像的直方图.直方图平稳分布,则说明了像素之间具有偏弱的相关性,分布越平稳,则说明越接近理想值,图像信息熵越大越好.图 2 是图 A1 加密前后得到的直方图.从图中可以看出,经过加密之后的图像像素呈现为更加均匀的分布,原图图像会有着各种波谷或尖峰,在经过加密后无法从中得到有用的信息.

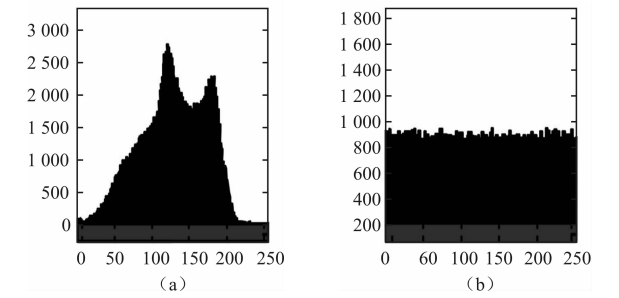


图 2 A1 图像原始图像与加密图像直方图

对于相似直方图而言,图像越平稳分布,那么就说明像素之间的相关性越弱,与之对应的是图像信息熵越大越好,更加贴近于理想值.对于图像统计而言,其非常重要的一个统计特征就是相邻像素之间的相关系数,设第 1 个像素的方差和均值分别是 $D(x)E(x)$,分别从原图像和加密图像中随机抽取 2000 对相邻像素来计算对角、垂直和水平三个方向上的相关系数,计算结果详见表 1 中所示.从表中可以看出,A1、A2 两个图像在经过加密算法处理后,在对角、垂直以及水平这三个方向上的相关系数都

显著下降,说明了此次提出的改进加密算法有着非常好的混淆作用.

表 1 原图及加密图相邻像素之间的相关系数

相关系数	对角	垂直	水平
A1 原图	0.7148	0.7724	0.8393
A1 加密图	-0.02471	0.0255	0.0117
A2 原图	0.9437	0.9918	0.9653
A2 加密图	-0.0241	-0.0274	0.0159

利用图像的信息熵来进行灰度值分布情况的度量,该值越大就说明图像灰度值的分布就更加一致,设图像的灰度值为 m_i ,一共有 L 种灰度值,加密算法性能越好,那么经由加密算法加密处理后的图像信息熵应该更接近于理论最大值,就 256 级灰度图像而言,其信息熵最大值为 8,由此分别对图 A1 和 A2 加密前后的信息熵进行计算,具体的结果详见表 2:

表 2 加密前后图像信息熵对比表

信息熵	原图像	加密图像	信息熵差值
A1	7.0451	7.9947	0.9496
A2	7.1248	7.9994	0.8746

从表中分析可以看出,原图像的信息熵值均要小于加密处理后的图像信息熵,而机密处理后的 A1 图像和 A2 图像的信息熵都接近于灰度级 256 的最大信息熵值 8,由此可见加密处理算法对图像处理的有效性.

5 结束语

将混沌理论引入之图像加密技术之中,可以有效改进加密算法的效果,给图像加密的实际应用带来了更大的可能.在分析了一维映射及混沌加密算法的相关数学机理后,此次构造了具有 3 个控制参数的一维复合混沌系统.考虑到压缩感知良好的压缩性能,因而选择具有较大密钥空间的混沌映射引入压缩感知进行图像加密算法的优化改进.通过对优化改进后的图像加密算法的仿真实验可以看出,原图像 A1、A2 经过加密处理后,虽然重构性能略低,但是有着很好的安全性能和效率,重构后图像直方图分布平稳,像素之间具有偏弱的相关性.进一步分析加密图像信息熵值,A1 和 A2 的加密图像信息熵分别为 7.9947、7.9994,接近于灰度级 256 的最大信息熵值 8,综合分析可以看出,此次提出的优化改进图像加密算法具有良好的处理性能.但是此次的研究也存在一定的不足,由于仅仅是采用的常规

置乱-扩散结构,因而没有结合其他领域中的方法进行图像加密算法性能比较测试.

参考文献:

[1] 王帅, 孙伟, 郭一楠, 等. 一种多混沌快速图像加密算法的设计与分析[J]. 计算机应用研究, 2015(2): 512-515

[2] 谢国波, 王添, XIEGuo-bo, 等. 一种新的基于比特置乱的超混沌图像加密算法[J]. 微电子学与计算机, 2016, 33(7):28-32.

[3] 谢国波, 姜先值. 二维离散分数阶 Fourier 变换的双混沌图像加密算法[J]. 计算机工程与应用, 2018(3): 40-45.

[4] 柴秀丽, 甘志华. 基于超混沌系统的位级自适应彩色图像加密新算法[J]. 计算机科学, 2016, 43(4): 134-139.

[5] 姚丽莎, 朱珍元, 程家兴. DNA 序列和分数阶 Chen 超混沌系统彩色图像加密[J]. 激光与光电子学进展,

2016, 53(9):86-95

[6] 廖琪男, 卢守东, 孙宪波. 结合超混沌序列和移位密码的数字图像加密算法[J]. 小型微型计算机系统, 2015, 36(2):332-337.

[7] 赵锋, 吴成茂. 自编码和超混沌映射相结合的图像加密算法[J]. 计算机辅助设计与图形学学报, 2016, 28(1):119-128.

[8] 赵佳星, 张雪锋, ZHAOJia-xing, et al. 基于组合混沌系统的时空彩色图像加密算法[J]. 计算机工程与设计, 2016, 37(9):2354-2360.

[9] 海洁, 杜海龙, 邓小鸿. 基于快速混沌置乱的鲁棒型医学图像加密算法[J]. 计算机应用, 2015, 35(2): 430-434.

作者简介:

李振汕 男, (1972-), 硕士, 副教授. 研究方向为计算机应用、信息安全. E-mail:976456097@qq. com