一种基于混合混沌序列的图像置乱加密算法

范延军 孙燮华 阎晓东 郑林涛
(中国计量学院计算机科学与技术系,杭州 310034)

摘 要 由 Logistic 映射产生的混沌序列常被用来置乱加密数字图像,但迄今为止,在国内外有关文献中,均未提到由 Logistic 映射产生的混沌序列中存在"平凡密钥"和"拟平凡密钥"的现象。如果用"平凡密钥"和"拟平凡密钥"作为 Logistic 映射的初始值,则将无法产生可用于图像置乱的混沌序列,并且在 Logistic 映射中存在无穷多个"平凡密钥"和"拟平凡密钥",这可能会导致对图像置乱加密无效,这是值得注意的问题.针对该问题,在对由 Logistic 映射产生的混沌序列中存在的"平凡密钥"和"拟平凡密钥"进行研究的基础上,提出了一种新的基于混合混沌序列的图像置乱加密算法,从而彻底解决了"平凡密钥"和"拟平凡密钥"对图像置乱加密无效的问题。

关键词 混沌 混合混沌序列 排列变换 加密 小波变换 平凡密钥 拟平凡密钥
中图法分类号: TP309 **文献标识码**: A **文章编号**: 1006-8961(2006)03-0387-07

An Image-scrambling Algorithm Based on Mixed Chaotic Sequences

FAN Yan-jun, SUN Xie-hua, YAN Xiao-dong, ZHENG Lin-tao
(*Department of Computer Science and Technology, China Institute of Metrology, Hangzhou* 310034)

Abstract The Logistic-Map chaotic sequence is often used to scramble and encrypt the digital images. In the former papers, the invalid-keys and the quasi invalid-keys existing in the Logistic-Map have not yet been discussed. If using the invalid-keys or the quasi invalid-keys as the initial value of the Logistic-Map, we can't get the chaotic sequence to scramble the digital images. Furthermore, there are infinite invalid-keys and quasi invalid-keys in the Logistic-Map. So we should take the problems seriously. In this paper, the invalid-keys and the quasi invalid-keys existing in the Logistic-Map chaotic sequence are deeply discussed. Then, an image-scrambling algorithm based on mixed chaotic sequences is proposed. Using this algorithm, the invalidity of the invalid-keys and the quasi invalid-keys is avoided thoroughly.

Keywords chaos, mixed chaotic sequences, scrambling transformation, encryption, wavelet, invalid-key, quasi invalid-key

1 引 言

随着对多媒体信息安全重视程度的提高,图像加密技术的应用迫在眉睫,急需加强发展。对于多媒体信息,尤其是图像和声音信息,由于传统的加密技术将其作为普通的数据流进行加密,而未考虑多媒体数据的特点,因此具有一定的局限性。

图像置乱(排列)变换是一种经典的基于内容的图像加密方法。如今图像置乱加密方法已有许多,如经典的 Arnold 变换、Hilbert 曲线变换、E 曲线变换[1]、几何变换[2]以及骑士巡游置乱变换[3]等等。虽然用这些方法置乱图像后的效果各不相同,但由于它们都具有一定的确定性,即在置乱过程中均只改变像素点的位置,而不改变其灰度值,所以置乱后的图像还是具有一定的规律性。文献[4]提出的基于混沌序列的加密算法,则既改变像素点的位置,又改变其灰度值,该算法属于空间域算法。尽管空间域的排列加密算法实现较为简单,且计算量较少,不过,空间域的局部随机置乱效果不是很好。文献[5]中提出的算法是基于 DCT(discret cosine transform)的频域算法,由于频域算法的优势是,在

收稿日期:2004-05-19;**改回日期**:2005-05-16

第一作者简介:范延军(1977 ~),男。2004 年获中国计量科学研究院硕士学位,现为中国计量学院计算机科学与技术系教师。主要研究方向为计算机图形学、数字水印、图像置乱、分形几何等。E-mail: fanyanjun2002@yahoo.com.cn

频域中每一点的变化对整个数据集合都产生一定的影响,因此效率高,相对于空间域算法,频域算法的加密效率比较高,其虽计算量较大,但执行速度仍可以满足实际应用的要求。为了克服 Logstic 映射存在"平凡密钥"和"拟平凡密钥"而导致图像加密置乱无效的问题。本文提出了一种新的基于混合混沌序列的小波域图像置乱加密算法。

2 混沌系统

由于混沌理论是动力系统从有序突然变为无序状态的一种演化理论,也是对确定性系统中出现的内在"随机过程"形成的途径、机制进行的研讨,如果给定一个离散混沌系统两个非常接近的初始植,则经过几次迭代后,输出的结果可以完全不相关,因此利用混沌系统对初始条件极其敏感的依赖性,可以提供数量众多、非相关、类随机而又可确定可再生的混沌序列,其非常大的周期性和优良的随机性,不仅非常适合产生符合安全要求的序列密码,而且可以提供数量众多的密钥。

一个 1 维离散时间非线性动力系统定义为

$$x_{n+1} = \tau(x_n) \tag{1}$$

其中,$x_n \in V, n = 0,1,2,3,\cdots$,可称之为状态;而 $\tau: V \to V$ 则是一个映射,它可将当前状态 x_n 映射到下一个状态 x_{n+1}。如果从初值 x_0 开始,反复应用 τ,那么就可得到一个序列 $\{x_n, n = 0,1,2,3,\cdots\}$,这一序列就称为该离散时间动力系统的一条轨迹。

一类非常简单却被广泛研究的动力系统就是 Logistic 映射,其定义为

$$x_{j+1} = \mu x_j(1 - x_j) \tag{2}$$

其中,$0 < \mu \leqslant 4$ 称为分支参数,$x_j \in (0,1), j = 0,1,2,3,\cdots$。混沌动力系统的研究工作指出,当分支参数 $3.569\,945\,6\cdots \leqslant \mu \leqslant 4$ 时,则 Logistic 映射工作于混沌态。也就是说,在 Logistic 映射的作用下由初始值 x_0 所产生的序列 $\{x_j, j = 0,1,2,3,\cdots\}$ 是非周期、不收敛的,并对初始值非常敏感。

不失一般性,为简单起见,本文主要考虑 $\mu = 4$ 时的情形,即

$$x_{j+1} = 4x_j(1 - x_j) \tag{3}$$

由于 Logistic 映射的输入和输出都分布在(0,1)上,因此可以用概率统计方法来定量分析其序列的特性,Schuster 证明的由式(3)产生的混沌序列 $\{x_j, j = 0,1,2,3,\cdots\}$ 的概率分布密度函数 $\rho(x)$[6] 如下式所示:

$$\rho(x) = \begin{cases} \dfrac{1}{\pi\sqrt{x(1-x)}} & 0 < x < 1 \\ 0 & x \leqslant 0;\ x \geqslant 1 \end{cases} \tag{4}$$

从式(4)可以看出,由于 Logistic 映射生成的混沌序列具有遍历性,同时它还具有 δ-like 型自相关函数和零的互相关函数[7],因而可以作为良好的图像置乱序列产生器。

3 平凡密钥与拟平凡密钥

文献[4]、[5]、[8~11]等均采用了式(3)中的 Logistic 映射来产生混沌序列,并用之来进行图像置乱加密。当初始值 $x_0 = 0.75$ 时,由式(3)产生的序列为 $\{x_j = 0.75, j = 0,1,2,3,\cdots\}$;当初始值 $x_0 = 0.25$ 时,由式(3)产生的序列为 $\{x_0 = 0.25, x_j = 0.75, j = 1,2,3,\cdots\}$。显然这两种情况下的序列均无法用于图像置乱加密,可将这两种情形称为平凡密钥和拟平凡密钥。下面给出平凡密钥和拟平凡密钥的定义。

3.1 平凡密钥

记

$$f(x) = \mu x(1 - x)$$

则 Logistic 映射可表示为

$$x_{j+1} = f(x_j), (j = 0,1,2,\cdots) \tag{5}$$

若一个初始点 $x_0 \in (0,1)$,使得 $x_1 = x_0, x_j = x_0 (j = 1,2,\cdots)$,则称这种密钥为周期 1 平凡密钥。类似的,对于某个正整数 k,若使得 $x_k = x_0, x_{j+k} = x_j (j = 0,1,2,\cdots)$,则称这种密钥为周期 k 平凡密钥,显然,当 x_0 等于周期 k 平凡密钥时,则 Logistic 映射(式(5))只取 k 个值

$$x_0, x_1, \cdots, x_{k-1}$$

且不会产生混沌序列。

3.2 拟平凡密钥

设 $x^{(k)}$ 是周期 k 平凡密钥,则满足

$$x^{(k)} = f^{(m)}(x)$$

的 x 为周期 k 拟平凡密钥,其中 $f^{(0)}(x) = f(x)$, $f^{(m)}(x) = f(f^{(m-1)}(x)), (m = 1,2,\cdots)$。据研究,这种周期 k 拟平凡密钥是存在的。求拟平凡密钥就是求解下面方程

$$x^{(k)} = \mu x(1 - x) = \mu x - \mu x^2$$

当 $\mu^2 - 4\mu x^{(k)} \geqslant 0$ 时,上式存在实数解。例如,若 $x^{(1)}$ 是周期 1 平凡密钥,则求解得到的 $1 - x^{(1)}$ 就是

周期 1 拟平凡密钥。

3.3 平凡密钥和拟平凡密钥的存在性

若周期 1 平凡密钥满足方程

$$x = \mu x(1 - x)$$

则解得

$$x = 1 - \frac{1}{\mu} \tag{6}$$

若周期 2 平凡密钥满足方程

$$x = \mu(\mu x(1 - x))(1 - \mu x(1 - x))$$

则消去 x 得三次方程

$$1 = \mu(\mu(1 - x))(1 - \mu x(1 - x))$$

即

$$x^3 - 2x^2 + \left(1 + \frac{1}{\mu}\right)x + \left(\frac{1}{\mu^3} - \frac{1}{\mu}\right) = 0 \tag{7}$$

因为周期 1 平凡密钥必为周期 2 平凡密钥,所以式(6)必为三次方程(式(7))的根,用式(7)左边的多项式除以 $x - 1 + \frac{1}{\mu}$ 可得

$$x^2 - \left(1 + \frac{1}{\mu}\right)x + \left(\frac{1}{\mu} + \frac{1}{\mu^2}\right) = 0$$

记该一元二次方程式的判别式为

$$\Delta = \left(1 + \frac{1}{\mu}\right)^2 - 4\left(\frac{1}{\mu} + \frac{1}{\mu^2}\right) = \frac{(\mu - 3)(\mu + 1)}{\mu^2}$$

所以当 $3 < \mu \leqslant 4$ 时,式(7)有两个根。即有两个周期 2 平凡密钥。

$$x_{1,2} = \frac{\left(1 + \frac{1}{\mu}\right) \pm \sqrt{\Delta}}{2}$$

当 $\mu = 4$ 时,则

$$x_{1,2} = \frac{5 \pm \sqrt{5}}{8}$$

利用 MATLAB 求解周期 3 平凡密钥可得,当 $3.828\,427\,1\cdots < \mu \leqslant 4$ 时,则存在周期 3 的平凡密钥 $x_i^{(3)} \in (0,1)$,$(i = 0,1,\cdots,7)$,并且同时存在周期 3 的拟平凡密钥 $\hat{x}_i^{(3)} \in (0,1)$,$(i = 0,1,\cdots,7)$。

李-约克定理[12]　如果区间 S 上的连续自映射 f 存在 3-周期点,则对任意正整数 m,自映射 f 具有 m-周期点。

由李-约克定理得,当 $3.828\,427\,1\cdots < \mu \leqslant 4$ 时,在 Logistic 映射中必存在周期 k 平凡密钥 $x^{(k)}$ 和周期 k 拟平凡密钥 $\hat{x}^{(k)}$。而且当 $k \to \infty$ 时,$(0,1)$ 内存在着可列个平凡密钥 $x^{(k)}$ 和拟平凡密钥 $\hat{x}^{(k)}$。这些点相对于整个 $(0,1)$ 区间来讲虽是"稀疏"的,但是对于置乱加密算法却是不容忽视的。设 $\{x_j, j = 0, 1, 2, 3, \cdots\}$ 是由 Logistic 映射产生的混沌序列,而且当 x_j 等于周期 k 平凡密钥 $x^{(k)}$ 或周期 k 拟平凡密钥 $\hat{x}^{(k)}$ 时,则从 x_j 之后的序列必然具有周期性,且周期为 k。这是不符合混沌置乱加密算法的要求的,例如由式(6)可知,当 $x_0 = 1 - \frac{1}{\mu}$ 时,Logistic 映射产生的序列为 $\{x_j = 1 - \frac{1}{\mu}, j = 0, 1, 2, 3, \cdots\}$,这样的序列是无法达到置乱加密目的的。

4 图像的小波变换处理

小波变换是图像的时-频表示。与传统的 DCT 变换相比,一方面 DCT 是时频不相关的,由于 WT (wavelet transform)的空间分辨率是随频率增加的,因此对于剧烈变化的边缘有更好的适应性;另一方面,通常图像都是能量集中在低频中,而 WT 中频率变化率却与频率成反比,其允许把低频分解成更精细的子带。

每次小波变换将图像分解成 4 块子图,其中 1 块对应平滑版本,另 3 块对应细节版本(如图 1 所示)。

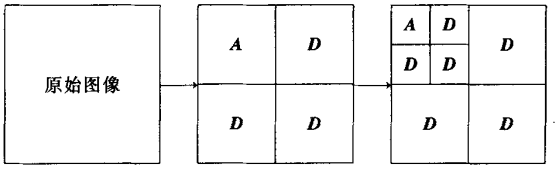


图 1　小波分解示意图

(A:平滑版本,D:细节版本)

Fig. 1　Image processing by using wavelet analyze tools

(A:smooth part, D:detail part)

由上图知,通过小波变换可将图像数据变换到频域,并且可分解成平滑版本和细节版本。如果在小波域内的平滑版本 A 中用图像置乱算法进行置乱,则频域内每一点的变化将对空间域中整个数据集合产生一定的影响,其不仅能取得很好的置乱效果,而且所需的混沌序列的长度可以成倍地减少,这可使算法速度大大提高。

5 基于混合混沌序列的图像置乱算法

鉴于 Logistic 映射中存在平凡密钥和拟平凡密钥,因此本文提出了一种基于混合混沌序列的图像

加密算法,这就从根本上避免了产生平凡密钥和拟平凡密钥的缺陷。

5.1 算法原理

实际上,为了避免单个 Logistic 映射中存在平凡密钥和拟平凡密钥的缺陷,可以简单地取以下两个 Logistic 映射:

$$x_{j+1}=\mu_1 x_j(1-x_j)$$

$$x_{j+1}=\mu_2 x_j(1-x_j)$$

其中,$3.828\,427\,1\cdots<\mu_1,\mu_2\leqslant 4$,且 $\mu_1\neq\mu_2$。利用这两个 Logistic 映射来交替生成混合混沌序列,即可避免大量的平凡密钥和拟平凡密钥的产生,但是由于当采用两个 Logistic 映射时,若它们在表达式结构上具有一定的相似性,则它们各自的平凡密钥与拟平凡密钥不可避免地也有一定的相似性,这将无法从根本上避免平凡密钥和拟平凡密钥,所以可采用 Chebyshev 映射和 Logistic 映射来交替产生混合混沌序列。由于 Chebyshev 映射与 Logistic 映射在表达式结构上相异程度很大,所以它们各自的平凡密钥与拟平凡密钥具有相似性的概率极小(或者根本没有相似性),同时,在算法中产生混合混沌序列时,本文采用了动态设置两个映射的交替周期的方法,这就进一步降低了产生平凡密钥和拟平凡密钥的可能性。这将可以从根本上避免产生平凡密钥和拟平凡密钥的缺陷。

n 阶 Chebyshev 映射定义如下:

$$\tau(x_{j+1})=\cos(n(\cos^{-1}x_j)) \tag{8}$$

其中的定义区间为(-1,1),本文中取其定义区间为(0,1)。

在本文提出的算法中,先使用 Logistic 映射式(式 3)和 Chebyshev 映射式(式 8)来交替生成混合混沌序列,然后利用混合混沌序列产生相应的置换矩阵和偏移矩阵。对任一图像 $\boldsymbol{I}$,设 $\boldsymbol{I}$ 的大小为 $M\times N$,利用本文算法对图像进行加密的过程为:

(1)对图像进行小波(wavelet)变换,$\boldsymbol{I}_{\mathrm{W}}=\boldsymbol{T}_{\mathrm{W}}(\boldsymbol{I})$,记其中的平滑版本图像的系数矩阵为 $\boldsymbol{I}_{\mathrm{WA}}$

(2)利用偏移矩阵来改变 $\boldsymbol{I}_{\mathrm{WA}}$ 中的系数值,记改变后的矩阵为 $\boldsymbol{I}_{\mathrm{WAF}}$

(3)利用置换矩阵对 $\boldsymbol{I}_{\mathrm{WAF}}$ 进行排列变换,记排列变换后的矩阵为 $\boldsymbol{I}_{\mathrm{WAFT}}$

(4)记矩阵 $\boldsymbol{I}_{\mathrm{WE}}$ 为用 $\boldsymbol{I}_{\mathrm{WAFT}}$ 替换 $\boldsymbol{I}_{\mathrm{W}}$ 中的 $\boldsymbol{I}_{\mathrm{WA}}$ 后所得到的矩阵,对 $\boldsymbol{I}_{\mathrm{WE}}$ 进行逆小波变换,得 $\boldsymbol{I}_{\mathrm{E}}=\boldsymbol{T}_{\mathrm{W}}^{-1}(\boldsymbol{I}_{\mathrm{WE}})$ 即完成图像的加密,其中 $\boldsymbol{I}_{\mathrm{E}}$ 代表加密后的图像。

5.2 算法设计

5.2.1 置换矩阵的生成及置乱运算

对于一个 2 维图像 $\boldsymbol{I}_{M\times N}$(为了讨论方便,假定 $\frac{M\times N}{4}$ 为整数),利用 Logistic 映射和 Chebyshev 映射产生实数混合混沌序列 $\{x_j,\ j=0,1,2,3,\cdots\}$。序列 $\{x_j\}$ 乘以 $\frac{M\times N}{4}$ 并且向上取整后,即得到一整数混合混沌序列 $\{y_j\in[1,\frac{M\times N}{4}],\ j=0,1,2,3\cdots\}$。将序列 $\{y_j\}$ 中的元素值依次填入空矩阵 $\boldsymbol{P}_{\frac{M\times N}{4}}$ 中,并保证矩阵中任一元素 $p_{i,j}\in[1,2,\cdots\frac{M\times N}{4}]$,若 $p_{i,j}=p_{k,l}$,当且仅当 $i=k$,$j=l$。根据生成的混合混沌序列在区间(0,1)具有遍历性可知,可知 $\boldsymbol{P}_{\frac{M\times N}{4}}$ 必能被填满,填满后的 $\boldsymbol{P}_{\frac{M\times N}{4}}$ 即为置换矩阵。置换矩阵 $\boldsymbol{P}_{\frac{M\times N}{4}}$ 同样具有混沌特性。

5.2.2 偏移矩阵的生成

利用已生成的置换矩阵 $\boldsymbol{P}_{\frac{M\times N}{4}}$,除以一个预先设定的阈值,则可以生成偏移矩阵 $\boldsymbol{R}_{\frac{M\times N}{4}}$。偏移矩阵中的数值不仅可用来改变平滑版本中的小波系数,同样偏移矩阵 $\boldsymbol{R}_{\frac{M\times N}{4}}$ 也具有混沌特性。

5.2.3 加密算法的实现

加密算法步骤如下:

(1)输入参数

①原始图像文件名 InImage;

②结果图像文件名 OutImage;

③密钥 x_0(即初始值)。

(2)加密过程

①由密钥 x_0 生成实数值混合混沌序列 $\{x_j,\ j=0,1,2,\cdots\}$ 和整数值混合混沌序列 $\{y_j,\ j=0,1,2,\cdots\}$;

②生成置换矩阵 $\boldsymbol{P}_{\frac{M\times N}{4}}$ 和偏移矩阵 $\boldsymbol{R}_{\frac{M\times N}{4}}$;

③将图像 $\boldsymbol{I}_{M\times N}$ 进行小波变换,设其中的平滑版本图像为 $\boldsymbol{I}_{\mathrm{WA}}$

④利用 $\boldsymbol{R}_{\frac{M\times N}{4}}$ 改变 $\boldsymbol{I}_{\mathrm{WA}}$ 中的小波系数值,然后利用 $\boldsymbol{P}_{\frac{M\times N}{4}}$ 对其进行置乱运算;

(3)对已完成置乱运算的图像数据进行逆小波变换,然后输出结果图像。

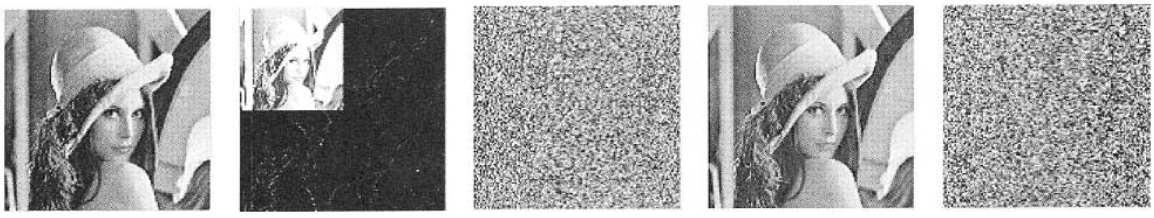
5.2.4 解密算法实现

用户必须输入正确的密钥,然后对加密图像进行加密算法逆向运算,即可获得解密图像。

6　实验结果与结论

本文采用 Daubechies 小波变换族中的 db1 小波实现了本文提出的算法。图 2 为用该算法对 256 × 256 大小的 Lena 图像进行加密的结果。

实验结果证明,当 $\mu=4$ 时,将 Logistic 映射的周期 1 平凡密钥 $x_0^{(1)}=0.75$ 或周期 1 拟平凡密钥 $\hat{x}_0^{(1)}=0.25$作为初始值时,本算法仍能产生符合要求的混沌序列,这是利用单一 Logistic 映射所无法产生的结果。同时,采用这种混合混沌序列来进行置乱加密后,还可进一步加大对图像解密攻击的难度。



(a) Lena 原图　(b) 小波分解后的图像　(c) 加密图像　(d) 解密恢复的图像　(e) 用错误密钥解密的图像

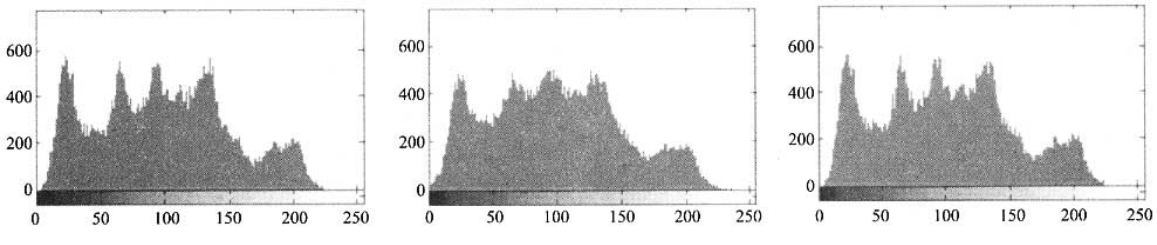
图 2　图像加密与解密结果

Fig. 2　The result of image encrypt & decrypt

本算法在小波域通过改变部分(低频部分)小波系数的值,极大地改变了原图像的质量。由于一般的空间域置乱加密算法只改变像素点的位置,并没有改变其灰度值,所以加密图像与原图像有相同的直方图;而本算法,由于像素点的位置及其灰度值都被改变了,从而提高了加密质量。这一点也可从图 3(a)和图 3(b)图像加密前后直方图的变化看出。图 2(c)是密钥 x_0 为 0.7 的加密图像,图 2(d)为用正确密钥解密的图像。图 2(e)为用错误的密钥(取值为0.700 001)解密得到的图像;由此可以看出,由于混沌序列对初始值非常敏感,即使密钥值有微小的变化也会得到完全不同的解密结果,这样就有大量的密钥空间供选择,从而可大大提高加密的安全性。

当平凡密钥或拟平凡密钥为无理数时,从理论上讲,由于利用单一的 Logistic 映射:$x_{j+1}=4x_j(1-x_j)$产生的序列具有某种周期性,因此不是混沌序列,但是实际的实验现象并非如此。为什么会出现这样的现象呢? 因为用小数来逼近某个无理数,当小数部分的位数大于等于某个数值(该数值与计算机的精度有关)时,则计算机会认为这个小数等于该无理数,此时可称在这种计算机精度下"取到"了该无理数的值,即"取到"的数值等于这个有理小数(小数位大于等于某个特定的数值)。例如,可用 2.236 067 977 499 789 696 4……来逼近$\sqrt{5}$,即当小数位的位数大于等于某个数值 m 时,计算机会认为 $\sqrt{5}=\underbrace{2.236\,067\,977\,499\,789\,696\,4}_{m}\cdots\cdots$,此时就称在这种计算机精度下"取到"了无理数$\sqrt{5}$。

当平凡密钥或拟平凡密钥为无理数时,虽然无法精确地取到无理数的值,但可以在当前的计算机精度下"取到"无理数的值。将"取到"的无理数平凡密钥或拟平凡密钥作为初始值代入 Logistic 映射:$x_{j+1}=4x_j(1-x_j)$,虽然从理论上讲,产生的序列应



(a) Lena 原图直方图　(b) 加密图像直方图　(c) 解密图像直方图

图 3　图像的直方图

Fig. 3　The histograms

具有某种周期性,但是由于计算过程中计算机的舍入误差和混沌映射对初始值极其敏感的特性,其产生的序列会逐渐脱离该周期轨道,所以最终仍可以产生混沌序列,但作为理论研究,平凡密钥与拟平凡密钥仍是混沌置乱加密中不可忽视的问题。

在现代通信网络中,传输数字图像时,为了提高传输效率,往往会先改变原图像的存储格式,然后再进行传输,而且在传输过程中常常会受到噪声信号的干扰,这些都会对加密图像产生一定影响而影响加密效果,因此,为了验证本算法的有效性,本文对置乱加密后的图像进行了 JPEG 攻击和加入噪声的实验。实验结果(如图 4 所示)表明,本算法在抗 JPEG 攻击和抗噪声信号的干扰等方面能够取得令人满意的结果。

(a) 对加密图像进行 JPEG 压缩(保留 30% 图像质量)后的解密效果

(b) 对加密图像进行 JPEG 压缩(保留 60% 图像质量)后的解密效果

(c) 对加密图像加入椒盐噪声后的解密效果

(d) 对加密图像加入随机噪声后的解密效果

图 4 对加密图像进行 JPEG 攻击和加入噪声后进行解密的实验结果

Fig. 4 The results of anti-attack experimentation

本文首先讨论了 Logistic 映射中存在的平凡密钥和拟平凡密钥的现象,进而提出了一种基于混合混沌序列的图像加密算法,这不仅从根本上避免了产生平凡密钥和拟平凡密钥的缺陷,而且极大地提高了图像加密的性能。同时,选用小波变换作为时频转换工具,充分利用了小波分解后的图像特性,以便选择分解后的图像平滑版本部分进行置乱加密。由于本文算法属于频域算法,而频域中每一点的变化对空间域中的整个数据集合都会产生一定的影响,即虽然置乱时只在小波域中实施置乱变换,但其中每一点的变化都会对原始图像中所有点产生影响,所以本算法仍然能取得良好的加密效果。与传统的 DCT 图像置乱算法相比,显然本文的算法效率高。因为在传统的 DCT 图像置乱算法中,要产生与原图像像素点矩阵一一对应的置换矩阵,而本文算法产生的置换矩阵则只有像素点矩阵的 1/4 大小,所以极大提高了算法的效率。

在其他一些非线性动力系统中,是否也存在类似于 Logistic 映射中的平凡密钥和拟平凡密钥现象?它们具有哪些性质?以及如何避免其产生?这些问题具有重要的研究价值,是下一步研究工作的重点。

参考文献(References)

1 LU Zhao-yang, ZHOU Xin-ni. A new algorithm of matrix disordering of computer files[J]. Computer Engineering and Science, 1998, **20**(3):28 ~ 41. [卢朝阳,周幸妮. 一种新的数据信息置乱算法[J]. 计算机工程与科学,1998,**20**(3):28 ~ 41.]

2 WU Min-sheng, WANG Jie-sheng, LIU Shen-quan. Permutation transform of images[J]. Chinese Journal of Computers, 1998, **21**(6): 514 ~ 519. [吴旻升,王介生,刘慎全. 图像的排列变换[J]. 计算机学报,1998,**21**(6):514 ~ 519.]

3 DING Wei, QI Dong-xu. Digital image transformation and information hiding and disguising technology[J]. Chinese Journal of Computers, 1998, **21**(9):838 ~ 843. [丁玮,齐东旭. 数字图像变换及信息隐藏与伪装技术[J]. 计算机学报,1998,**21**(9):838 ~ 843.]

4 ZHANG Xiao-hua, LIU Fang, JIAO Li-cheng. An image encryption arithmetic base on chaotic sequences[J]. Journal of Image and Graphics, 2003, **8**(4):374 ~ 378. [张小华,刘芳,焦李成. 一种基于混沌序列的图象加密技术[J]. 中国图象图形学报,2003, **8**(4):374 ~ 378.]

5 YI Kai-xiang, SUN Xin, SHI Jiao-ying. An image encryption arithmetic based on chaotic sequences[J]. Journal of Computer - Aided Design and Computer Graphics, 2000, **12**(9):672 ~ 676. [易开祥,孙鑫,石教英. 一种基于混沌序列的图像加密算法[J]. 计算机辅助设计与图形学学报,2000,**12**(9):672 ~ 676.]

6 Heinz Georg Schuster. Deterministic chaos, An introduction(Second revised edition)[M]. Weinheim, Federal Republic of Germany:

VCH(Verlag, Chemie), 1988.

7 WANG Hai, HU Jan-dong. Logistic-map chaotic spread-spectrum sequence[J]. Acta Electronica Sinica(in Chinese), 1997, **25**(1): 19~23. [王亥,胡建栋. Logistic-Map 混沌扩频序列[J]. 电子学报,1997,**25**(1):19~23.]

8 WENG Yi-fang, JU Lei. Chaotic stream cipher encryption algorithms [J]. Computer Engineering, 2002, **28**(11): 79~80. [翁贻方,鞠磊. 基于混沌的序列密码加密算法[J]. 计算机工程,2002,**28**(11):79~80.]

9 WAN Xiang-sheng, GAN Jun-ren. A chaotic sequence encryption method[J]. Chinese Journal of Computers, 2002, **25**(4): 351~356. [王相生,甘骏人. 一种基于混沌的序列密码生成方法[J]. 计算机学报,2002,**25**(4):351~356.]

10 QIN Hong-lei, HAO Yan-ling, SUN Feng. Design of picture permutation network on chaos [J]. Computer Engineering and Applications, 2002, **38**(7): 104~106. [秦红磊,郝燕玲,孙枫. 一种基于混沌的图像置乱网络的设计[J]. 计算机工程与应用,2002,**38**(7):104~106.]

11 GU Qin-long, YAO Ming-hai. A research of digital image encryption based on logistic chaotic sequence[J]. Computer Engineering and Applications, 2003, **39**(23): 114~116. [顾勤龙,姚明海. 基于 Logistic 混沌序列的数字图像加密研究[J]. 计算机工程与应用,2003,**39**(23):114~116.]

12 ZHANG Jing-zhong, YANG Lu, ZHANG Wei-nian. Iteration equation and imbedding flow[M]. Shanghai: Press of the Education of Science and Technology of Shanghai, 1998: 23~24. [张景中,杨路,张伟年. 迭代方程与嵌入流[M]. 上海:上海科技教育出版社,1998:23~24.]