

混合混沌系统的并行多通道彩色图像加密

肖 锋¹, 张丽丽², 冯 飞¹

(1 西安工业大学 计算机科学与工程学院, 陕西 西安 710032,

2 西安工业大学 理学院, 陕西 西安 710032)

摘 要: 为了提高彩色图像信息的安全性和加密性能, 并使高维混沌系统具有更高的安全性, 提出了一种混合混沌系统的并行多通道图像加密方法. 将彩色图像分解成为 R 、 G 、和 B 的单色图像, 对三种单色图像分别使用不同的高维混沌系统产生混沌序列, 并使用三种不同的混沌加密结构进行对像素位置置乱和像素值的多轮扩散, 进而实现图像的加密. 对 R 分量采用 Lorenz 混沌系统; G 分量采用 Ressler 混沌系统; B 分量采用 Chen 混沌系统. 仿真实验结果表明: 该算法具有足够大的密钥空间, 具有良好的加密效果和较高的安全性和加密性能.

关键词: 混沌; 图像加密; 双重置乱; 明文图像; 密文图像

中图分类号: TP309.7

文献标识码: A

文章编号: 1000-7180(2016)08-0076-06

Parallel Multi-channel Color Image Encryption Based on Hybrid Chaotic System

XIAO Feng¹, ZHANG Li-li², FENG Fei¹

(1 School of Computer Science and Engineering, Xi'an Technological University, Xi'an 710032, China;

2 School of Science, Xi'an Technological University, Xi'an 710032, China)

Abstract: In order to improve security and encryption performance of the color image information, and at the same time high-dimensional chaotic system with higher security, a new color image encryption algorithm is proposed based on a hybrid chaotic system of multi-channel parallel. The color image decomposed into R , G , and B of monochrome images, the three monochrome images using different high-dimensional chaotic system chaotic sequence, using three different structure chaotic encryption scrambling pixel position and the pixel value several rounds of proliferation, so as to realize image encryption. The R component image used Lorenz chaotic system; G component image used Ressler chaotic system; B component image used Chen chaotic system. Simulation results show that the algorithm not only has a sufficiently large key space, but also has a good effect and high security encryption and encryption performance.

Key words: chaos; image encryption; dual scrambling; plain image; cipher image

1 引言

图像信息是目前广泛应用的主要信息载体之一, 是主流的表达信息方式, 因而关于图像安全的问题备受关注^[1]. 彩色图像含有更多的图像信息, 其加密逐渐成为人们的研究热点^[2], 很多学者提出了一些针对彩色图像的加密方法^[3-4], 但依旧将图像作为

普通的一维数据流进行加密, 图像数据是具有矩阵形式的二维数据, 像素间及彩色图像分量之间具有非常强的相关性, 传统加密方法无法完全覆盖二维空间上所有的图像数据, 这样就有可能泄露明文数据. 彩色图像比灰度图像具有更大的数据量, 运用传统加密方法难以和图像实时传输速率相匹配; 近些年来, 提出的基于混沌动力学系统的彩色图像加密

成为主要的研究方向^[4],方法大都采用低维混沌系统,这样混沌序列复杂度不高,密钥空间小,会导致加密系统的安全性不高.而高维以及超高维的混沌系统具有 2 个以上的 Lyapunov 指数,结构与特性更为复杂,非线性行为更加难以预测,密钥空间更大.研究发现,目前提出彩色图像的加密算法对不同彩色分量进行混沌加密采用相同的混沌加密方法,混沌加密方法比较单一,但是混沌序列复杂度不高、密钥空间较小,加密安全性不高.

为了增强彩色图像加密的安全性,本文提出了一种新的高维混沌系统的彩色图像加密方法.

2 混沌系统

混沌是非线性动力学系统中一种不规则运动现象,输出序列结果不具有周期性,也不收敛;同时对初值非常敏感,两个具有细微差别的初始值所产生的混沌序列互不相关,迭代出来的运动轨迹不可预测,差别非常大;加密时对数据各个位产生异或操作,产生密钥流需要寄存的变量有限,时间与空间开销等具有非常好的特性,这些特点非常符合加密的一系列要求,因此,混沌系统的这些特点,很适合对包括图像在内各种数据加密与隐藏.

在本文的加密算法中,采用了 Lorenz 混沌系统, Rossler 混沌系统和 Chen 混沌系统.

Logistic 映射,也叫虫口模型,表达方式如下:

$$x_{n+1} = \lambda x_n(1 - x_n) = f(x_n, \lambda)$$

Lorenz 混沌系统的动力学表达式如下:

$$\begin{cases} \dot{x} = a(y - x) \\ \dot{y} = rx - y - xz \\ \dot{z} = -bz + xy \end{cases} \quad (1)$$

式中, x, y, z 分别是系统的状态变量; $\dot{x}, \dot{y}, \dot{z}$ 是状态变量随着时间 t 的变换率; a, b, r 为系统参数,当 $a = 10, b = \frac{8}{3}, r = 28$ 时, Lorenz 系统呈混沌特性.

Rossler 混沌系统的动力学表达式如下:

$$\begin{cases} \dot{x} = -(y + z) \\ \dot{y} = x + \alpha y \\ \dot{z} = \beta + z(x - \zeta) \end{cases} \quad (2)$$

式中 α, β, ζ 为系统参数. 当参数 $\alpha = 0.2, \beta = 0.2, \zeta = 5.0$ 时, Rossler 系统呈混沌特性.

Chen 混沌系统是在 Lorenz 系统方程组中第二

个方程中引入一个线性反馈控制想,其动力学表达式如下:

$$\begin{cases} \dot{x} = a(y - x) \\ \dot{y} = (c - a)x - xz + cy \\ \dot{z} = -bz + xy \end{cases} \quad (3)$$

Chen 系统在形式上与 Lorenz 系统相近,但是比 Chen 系统复杂. 当参数 $a = 35, b = 3, c = 28$ 时, Chen 系统呈混沌特性.

3 混沌系统的预处理^[5]

上述混沌系统产生的混沌序列有较大的不足,均匀分布特性较差;局部取值显示出一定的单调性,序列间的相关特性比较高,易受到线性预测攻击^[6],容易破译,所以在使用混沌序列对于图像加密之前进行混沌序列预处理,步骤如下所示.

Step1: 将序列值的小数点右移,然后与其整数值作差,得到值域在 $(-1, 1)$ 间新的混沌序列. 数学模型为

$$\begin{cases} R(i) = 10^n R(i) - \text{round}(10^n R(i)) \\ G(i) = 10^n G(i) - \text{round}(10^n G(i)) \\ B(i) = 10^n B(i) - \text{round}(10^n B(i)) \end{cases} \quad (4)$$

Step2: 彩色图像的三种颜色分量取值范围在 $[0, 255]$, 将序列值做余运算,映射到 $[0, 255]$, 取之最相近的整数. 数学模型为

$$\begin{cases} R(i) = \text{round}(R(i) + 0.5) * 10^n \bmod 255 \\ G(i) = \text{round}(G(i) + 0.5) * 10^n \bmod 255 \\ B(i) = \text{round}(B(i) + 0.5) * 10^n \bmod 255 \end{cases} \quad (5)$$

在式(4)、(5)中, n 为移位控制参数, $\text{round}(\cdot)$ 为取最接近整数运算函数, $\bmod$ 为取模函数. 经过上述的预处理过程,可以增强混沌序列取值的无规则性及整体分布的均匀性. 利用上述预处理过程得出的 $\{R(i), G(i), B(i)\}$, 用于下面算法中的异或操作. 在算法实现过程中,经过预处理的混沌序列具有良好的混沌特性、自相关性和接近于 0 的互相关特性^[7-8].

4 加密算法和解密算法

图像加密主要是利用混沌序列的不可预测性、随机性等进行图像中像素位置的置乱和像素灰度值的扩散. 单纯的置乱技术只是依据已知密钥产生的混沌序列改变图像像素排列的位置,并不改变像素的值,也没有改变图像的直方图,只是降低图像的相

关性,而且使用中非常容易遭受统计特性的攻击;而单纯的像素灰度值的扩散容易受到明文的攻击.无论是置换和扩散,单独采用一种方式对可以实现图像加密,但是安全性不高,很容易遭受攻击,进而解密,常用的方法是将两者结合起来,从而具有较高的安全性.加密算法设计如下所示.

Step1:预处理

Step 1.1:读入原图像,图像大小为 $M \times N$.

Step 1.2:将图像的 R 、 G 和 B 三个分量分离,生成单色的灰度图像,即为 $I(R)$ 、 $I(G)$ 和 $I(B)$.

Step2:生成随机混沌序列

Step 2.1:对于 Lorenz 混沌映射来说,给定系统参数 $a = 10, b = \frac{8}{3}, r = 28$,初值 $x(0), y(0)$ 和 $z(0)$,代入式(1),按照上述式(4)、(5)混沌系统预处理过程生成长度为 $i = M \times N$ 的序列.

Step 2.2:对于 Rossler 混沌映射来说,给定系统参数 $\alpha = 0.2, \beta = 0.2, \zeta = 5.0$,初值 $x_1(0), y_1(0)$ 和 $z_1(0)$,代入式(2),生成长度为 $i = M \times N$ 的序列.

Step 2.3:对于 Chen 混沌映射来说,给定系统参数 $a = 35, b = 3, c = 28$,初值 $x_2(0), y_2(0)$ 和 $z_2(0)$,代入式(3),生成长度为 $i = M \times N$ 的序列.

为了避免混沌系统过渡过程的影响,进一步增强算法抗攻击的能力,在生成的三个混沌序列中,每个混沌序列的前 t 项舍弃,本文把前 3 000 个序列数舍弃,即 $t = 3\,000$.

Step3:像素位置置乱

为了提高图像加密效率,不破坏图像压缩效率,将图像进行 8×8 分块,以块为单位进行位置置乱,这样可以抵抗图像压缩攻击^[5]. 图像的行与列不够 8 的整数倍,边界填充 0(黑色).

以红色图像 $I(R)$ 为例,将 Step2.1 产生的混沌序列的 $M \times N$ 个数,分成 l 个段,其中 $l = \frac{M \times N}{8 \times 8}$,每一段的大小为 64 个混沌序列数,这 64 个混沌数和图像分块 8×8 相应的像素一一对应;再把每段的 64 个混沌序列数按升序(或者降序)排列,生成 64 个位置索引,构成位置索引矩阵;根据排序后的位置,将排序前对应的像素按照排序后混沌序列数的位置进行移动,重新排列 $I(R)$ 中像素位置,得到位置置乱后的红色图像 I_R .

分别按照 Step 2.2 和 Step 2.3 得到混沌序列,重复上述步骤,可以得到位置置乱后的绿色图像 I_G

蓝色图像 I_B . 这样原来明文图像某一位置上的 R 、 G 和 B 分量在图像矩阵中随机分布在不同的位置,从而实现彩色图像的 R 、 G 和 B 位置置乱.

Step4:图像像素扩散

图像加密中的图像像素扩散包括像素值改变和像素值扩散两个过程.像素值改变指的是图像中像素的灰度值发生变化;像素值扩散通常会有一个值传递过程,明文图像中一个像素值的改变可以影响到整个密文图像发生变化.一般来说,参与图像扩散的像素个数越多,灰度值改变的越大,扩散的效果就会越好.

Step 4.1:以置乱后的红色图像 I_R 为例,随机选取 1 000 个像素,求和,像素值的和作为小数部分,形成初值,作为 Lorenz 混沌系统产生混沌序列的初值,生成混沌序列 $P_R(i)$. 同理,对于置乱后 I_G 和 I_B ,采用相同的方式分别采用 Rossler 和 Chen 混沌系统生成混沌序列 $P_G(i)$ 和 $P_B(i)$,其中 $i = 1, \dots, M \times N$.

Step 4.2:将混沌序列 $P_R(i)$ 、 $P_G(i)$ 和 $P_B(i)$ 以 0.5 为阈值,二值化为 0,1 和序列,并将这三个序列异或生成一个序列 $P_{RGB}(i)$,即 $P_{RGB}(i) = P_R(i) \oplus P_G(i) \oplus P_B(i)$.

Step 4.3:将这个序列与 $I_0(R)$ 的图像第一轮加密,加密公式如式(6)所示.加密后,得到第一轮加密后三个分量图像.

$$\begin{cases} F_R^1(i) = I_R(i) \oplus P_R(i) \\ F_G^1(i) = I_G(i) \oplus P_G(i) \\ F_B^1(i) = I_B(i) \oplus P_B(i) \end{cases} \quad (6)$$

Step 4.4:接下来进行第二轮加密,根据式(7)、(8)对分量图像进行扩散.当 $i = 1$ 时, F_R^2, F_G^2, F_B^2 的初值分别等于第一轮加密后的各分量图像的第一个和最后一个像素的灰度值异或的结果,如式(7)所示.经式(7)、(8)执行后,得到经过第二轮加密后的分量图像.

$$\begin{cases} F_R^2(1) = F_R^1(1) \oplus F_R^1(M \times N) \\ F_G^2(1) = F_G^1(1) \oplus F_G^1(M \times N) \\ F_B^2(1) = F_B^1(1) \oplus F_B^1(M \times N) \end{cases} \quad (7)$$

$$\begin{cases} F_R^2(i) = F_R^2(i) \oplus P_{RGB}(i) \oplus F_R^2(i-1) \oplus F_G^2(i-1) \oplus F_B^2(i-1) \\ F_G^2(i) = F_G^2(i) \oplus P_{RGB}(i) \oplus F_R^2(i-1) \oplus F_G^2(i-1) \oplus F_B^2(i-1) \\ F_B^2(i) = F_B^2(i) \oplus P_{RGB}(i) \oplus F_R^2(i-1) \oplus F_G^2(i-1) \oplus F_B^2(i-1) \end{cases} \quad (8)$$

Step 4.5 :接下来,进行第三轮的加密,加密过程如式(9) 所示.

$$\begin{cases} F_R^3(i) = (F_G^2(i) + F_B^2(i))\text{mod}256 \oplus F_R^2(i) \\ F_G^3(i) = (F_R^2(i) + F_B^2(i))\text{mod}256 \oplus F_G^2(i) \\ F_B^3(i) = (F_R^2(i) + F_G^2(i))\text{mod}256 \oplus F_B^2(i) \end{cases}$$

(9)

在式(8) 中,每一个像素点的值都会影响下一

个像素的灰度取值;经过三轮的加密,每轮像素值加密的结果反映到下轮的密文中.

Step 5:将三轮加密后得到的分量图像 F_R^3, F_G^3, F_B^3 合并,得到加密后的彩色图像,即最终的密文图像.

解密算法即为上述步骤的逆过程. 加密过程如图 1 所示.

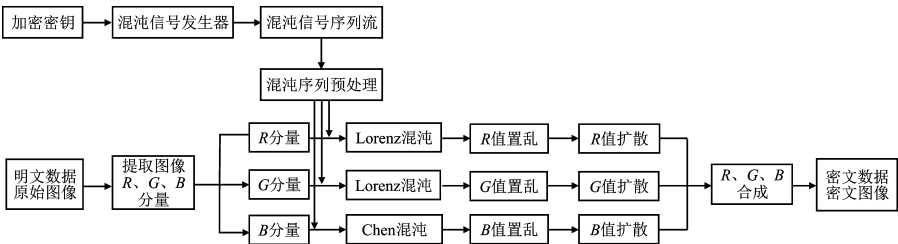


图 1 加密过程

整个加密过程主要分为三部分:一是对混沌序列的预处理过程;二是图像像素位置的置乱;三是图像像素灰度值的扩散. 预处理使得混沌序列具有更强的伪随机性,并且对每个单色图像,可以使用不同的混沌系统的产生的混沌序列,提高图像的置乱程度和算法破译难度,增强加密效果.

5 实验结果与讨论

本文采用大小为 256×256 的标准 Lena 彩色图像作为明文图像,通过实验仿真对密钥空间、密钥敏感性、统计分析与差分攻击等进行分析. 仿真结果如图 2 所示,图 2(a)与图 2(b)分别是明文图像以及加密后图像.

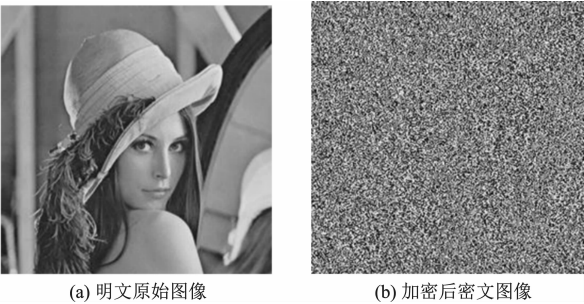


图 2 图像加密效果

5.1 密钥空间分析

在本文算法中,Lorenz,Rossler 和 Chen 混沌系统有 9 个系统参数和 9 个状态变量初值都可以作为单独的密钥使用. 这里,仅仅以系统初值为例,假设双精度浮点数字的精度为 10^{-15} ,则密钥空间至少为 $(10^{15})^9 = 10^{135}$,这个密钥空间足够大,穷举破译是

不可能的,可以抵御穷举攻击.

5.2 密钥敏感性分析

在这里以 Lorenz 混沌系统为例,在其在系统的三个参数中,参数 r 为主要的控制参数,所以一般先设置 $a = 10, b = 8/3$, 在通过改变参数 r 来研究系统的特性. 表 1 给出了参数 r 和初值 $x(0)$ 发生微小变化的测试结果. 这里的位变化率 Loc(R) 指的是 R 分量图像在位置置乱过程中,位置索引发生的变化比例.

表 1 参数微变的敏感性			%
参数微变量	$r+$	$x(0)+$	
10^{-8}	99.995	99.995	
10^{-9}	100	99.995	
10^{-10}	99.995	99.995	
10^{-11}	99.995	99.995	
10^{-12}	99.995	100	

从表 1 可以看出,初值微小的变化能够使得位置置乱完全改变,说明加密系统对系统参数和初值具有非常强敏感性,要想解密,就得知道密钥否则无法解密.

通过以上分析,算法具有非常大的密钥空间,并且具有非常强的初值敏感性,很好的伪随机性,使得算法具有一次一密的安全特性.

5.3 统计分析

统计分析主要包括直方图分析和相邻像素相关性分析.

(1)直方图分析

图 3 是明文图像与密文图像的三个分量图像的

直方图,其中(a)、(b)、(c)分别是加密前 R 、 G 和 B 分量的直方图;(d)、(e)、(f)分别是加密后 R 、 G 和 B 分量的直方图.可以很明显地看出, R 、 G 和 B 分量图像的直方图在加密前后发生了很大变化.明文的 R 、 G 和 B 分量直方图高低起伏,这些像素分布的

不均匀经常是进行密文攻击的主要入口;而加密后的 R 、 G 和 B 分量直方图分布均匀,各个像素出现频率接近,很好地掩饰了明文图像,能够较好地抵抗统计攻击.

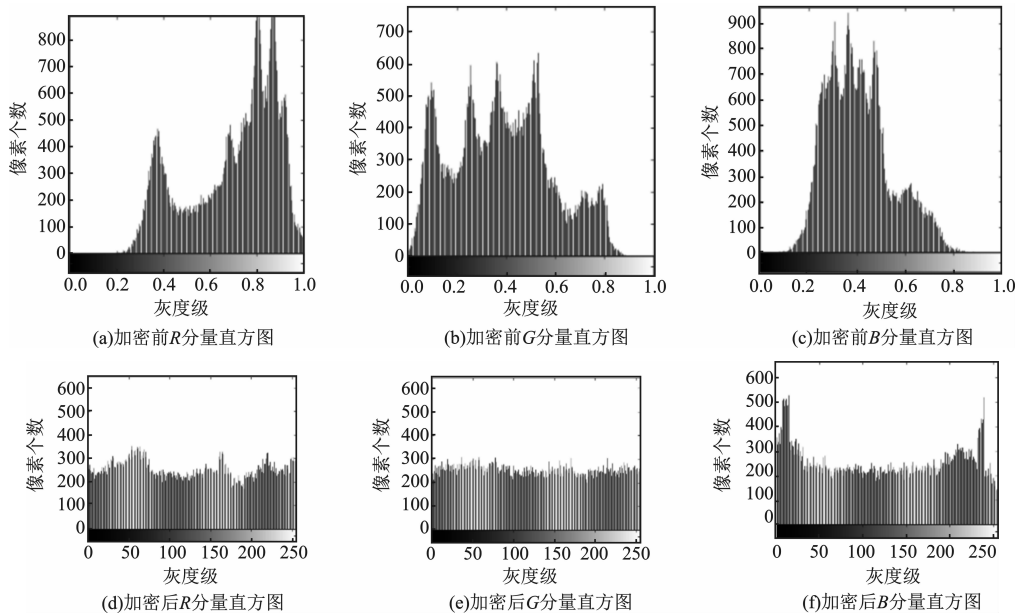


图 3 图像像素灰度分布图

(2)相邻像素相关性分析

为了防御统计攻击,图像加密就要减少相邻像素间的相关性,它反映了图像置乱的程度.图像置乱的效果越好,相邻像素的相关性越小;反之,图像置乱的效果越差,相邻像素的相关性越大.引入相邻像素的相关系数定量地分析相关性^[9].计算公式如下:

$$E(x) = \frac{1}{N} \sum_{i=1}^N x_i$$
$$\text{Cov} = \frac{1}{N} \sum_{i=1}^N [x_i - E(x)][y_i - E(y)]$$
$$r_{xy} = \frac{\text{Cov}}{\sqrt{D(x)} \sqrt{D(y)}}$$
$$r_{xy} = \frac{\text{Cov}}{\sqrt{D(x)} \sqrt{D(y)}} \tag{10}$$

式中, x,y 为两个相邻像素的像素值.从 R 、 G 和 B 分量的明文图像和密文图像中,分别选取 4 098 对相邻像素,分别从水平、垂直和对角方向计算相关系数,结果如表 2 所示.明文图像中相关系数接近 1,说明相邻像素高度相关;而密文图像中的相关系数接近 0,相邻像素的相关性基本消除,表明明文图像中的统计特征已经充分扩散到密文图像中.

5.4 差分分析

差分分析是分析明文敏感性的常用分析方法.

表 2 相邻像素的相关系数

		R 分量	G 分量	B 分量	原图像
明文图像	水平	0.948 9	0.952 1	0.953 7	0.937 8
	垂直	0.971 2	0.962 7	0.973 9	0.945 6
	对角	0.938 2	0.927 8	0.952 2	0.919 6
密文图像	水平	0.004 8	0.003 4	0.002 8	0.005 3
	垂直	0.008 7	0.006 7	0.007 4	0.006 1
	对角	0.002 3	0.003 1	0.001 9	0.003 6

如果明文图像的某一个像素发生变化,能够很大程度上改变加密图像,密文图像和明文图像有显著的差异,那么加密算法有很强的抵抗差分攻击能力,即用像素个数变换率(NPCR)和整体平均变化强度(UACI),分别为

$$\text{NPCR} = \frac{\sum_{i,j} D(i,j)}{M \times N} \times 100\%$$
$$D(i,j) = \begin{cases} 0, C(i,j) = C(i,j) \\ 1, C(i,j) \neq C(i,j) \end{cases}$$
$$\text{UACI} = \frac{1}{M \times N} \left[\sum_{i,j} \frac{|C(i,j) - C(i,j)|}{255} \right] \times 100\% \tag{11}$$

式中, M 和 N 分别是图像的宽度和高度, $C(i,j)$ 和 $C(i,j)$ 是明文图像的某一个像素改变前后的密文

图像. 对于在 (i, j) 处的像素, 如果 $C(i, j) = C'(i, j)$, 令 $D(i, j) = 0$; 否则 $D(i, j) = 1$. 在明文图像随机选择一个像素, 使其像素值加 1, 根据式(11) 计算, 进行 100 组的实验后计算得到的各平均值如表 3 所示.

表 3 密文图像 NPCR 和 UACI 值

颜色分量	R	G	B
NPCR	0.997 2	0.997 4	0.998 1
UACI	0.334 6	0.335 2	0.333 8

根据表 3 显示结果, 该算法对明文图像微小的变化十分敏感, 就会引起密文图像的显著变化, 只要密钥不同, 两幅相同图像加密的结果完全不同, 因此本文算法能够抵御差分攻击.

6 结束语

利用混沌系统对图像加密本质利用混沌模型对图像进行某种变换, 使得变换后的图像与原始图像存在视觉差异. 本文提出了一个新的混合混沌系统的多路并行多通道彩色图像加密算法. 在加密过程中, 采用 Lorenz, Rossler 和 Chen 混沌系统分别对彩色图像的 R、G 和 B 分量进行像素的置乱和扩散, 对不同颜色分量采用不同混沌系统, 产生的混沌序列更加难以预测和重构. 实验结果表明, 对彩色图像的三个颜色分量分别进行置乱和扩散双重的加密, 增加了安全性; 整个加密算法只是用到了置乱和异或运算, 易于实现, 有利于对图像进行加密和解密; 同时, 该算法密钥空间大, 有很强的密钥敏感性和均匀统计特性, 密文图像中的相邻像素之间的相关性趋近于零, 可有效抵御统计攻击; 原始图像的微小变化会引起密文图像的明显变化, 能够有效地抵御差分攻击. 实验表明该算法加密效果较好, 具有较高的安全性和实际应用价值.

参考文献:

[1] 田汉清, 全吉成, 程红, 等. 图像情报加密技术综述[J]. 情报科学, 2009, 27(1): 156-160.

[2] Ye G, Wong K W. An efficient chaotic image encryption algorithm based on a generalized Arnold map [J]. Nonlinear dynamics, 2012, 69(4): 2079-2087.

[3] 王红娟, 张颖颖, 黄义定, 等. 基于非对称密码系统的彩色图像加密技术[J]. 应用光学, 2013, 34(6): 980-984.

[4] 庾朝永, 秦拯, 黎谦. 联合二维 logistic 混沌映射与比特重组的彩色图像加密算法[J]. 计算机科学, 2013, 40(8): 300-302.

[5] 王英, 郑德玲, 鞠磊. 基于 Lorenz 混沌系统的数字图像加密算法[J]. 北京科技大学学报, 2004, 249(6): 678-682.

[6] 尹显东, 姚军, 李在铭, 等. 基于混沌序列的频域图像加密技术研究[J]. 计算机工程与应用, 2004, 34(6): 12-14.

[7] 赵怀勋, 程甲. 基于三维超混沌系统的彩色图像加密算法[J]. 微电子学与计算机, 2010, 27(2): 72-74.

[8] 柴秀丽, 郭峻言. 基于多轮扩散的彩色图像加密算法[J]. 微电子学与计算机, 2014, 31(5): 62-66.

[9] Sabery K M, Yaghoobi M. A new approach for image encryption using chaotic logistic map[C] // International Conference on Advanced Computer Theory and Engineering. Phuket: IEEE Press, 2008: 585-590.

作者简介:

肖 锋 男, (1976-), 博士, 副教授. 研究方向为智能信息处理与视觉分析.

张丽丽 女, (1973-), 博士, 教授. 研究方向为智能信息处理、拓扑学.

冯 飞(通讯作者) 男, (1992-), 硕士生. 研究方向为智能信息处理与视觉分析. E-Mail: xffriends@163. com