

文章编号:1001-9081(2011)10-2682-05

doi:10.3724/SP.J.1087.2011.02682

# 基于 Arnold 变换的图像分存加密方法

侯文滨,吴成茂

(西安邮电学院 电子工程学院, 西安 710121)

(418202619@qq.com)

**摘要:**为提高图像分存加密的安全性,提出一种将置乱加密、分存技术和像素扩散相结合的分存加密方法。首先,利用一维 Logistic 混沌映射产生 Arnold 变换的参数;其次,利用变参数的二维 Arnold 变换对图像进行像素位置置乱;最后,利用变参数的三维 Arnold 变换对置乱后图像进行像素值扩散并分存为两幅图像。实验结果表明,该方法的外部密钥敏感度较强,具有良好的雪崩效应,能够有效地抵抗明文和差分等攻击,且解密密钥与明文图像紧密相关。

**关键词:**图像分存;Logistic 映射;Arnold 变换;图像置乱;像素扩散

**中图分类号:**TP309.7;TN911.73   **文献标志码:**A

## Image encryption and sharing based on Arnold transform

HOU Wen-bin, WU Cheng-mao

(School of Electronic Engineering, Xi'an University of Posts and Telecommunications, Xi'an Shaanxi 710121, China)

**Abstract:** To improve the security of image sharing and encryption, an algorithm which combined the scrambling encryption with sharing technology and pixel diffusion was proposed. Firstly, the Logistic chaotic mapping algorithm was used to generate the parameter of Arnold transform. Secondly, two-dimensional Arnold transform with variable parameters was adopted to scramble pixel positions of the image. Finally, three-dimensional Arnold transform with variable parameters was adopted to diffuse pixel values of the scrambled image, so the image could be decomposed into two images. The experimental results show that the algorithm has a strong sensitive effect on the external keys, resists plaintext attack and differential attack effectively, and possesses favorable avalanche effect. Moreover, there is a close relationship between the internal keys and the original plaintext image.

**Key words:** image sharing; Logistic mapping; Arnold transform; image scrambling; pixel diffusion

## 0 引言

图像分存是图像信息安全保护中的重要内容,已得到了广泛的应用。图像分存是把一幅秘密的数字图像分解成几幅无意义或者杂乱无章的图像,并伪装到几幅有意义的图像中进行存储或传输,它可以避免由于少数图像信息泄露而造成严重的安全事故,同时在通信中个别图像信息的丢失不会引起整个图像信息的丢失<sup>[1]</sup>。文献[2]提出了一种利用矩阵分解来实现图像分存的方法,该方法实现简单、运算量小、数据膨胀率低,但是存在图像细节信息暴露的缺陷。文献[3]利用混沌与不定方程相结合实现图像分存,消除了数据膨胀,但分存图像结果不具有唯一性。针对文献[2-3]中图像分存方法存在的不足,本文提出了一种基于 Arnold 变换的图像分存加密方法,它将原图像像素置乱扩散并分解成两幅分存图像,其 Arnold 变换的参数由 Logistic 混沌映射产生,图像分存结果的安全性受到外部密钥和原图像信息共同控制,能够抵抗诸如选择性明文、差分等攻击。

## 1 混沌映射

混沌系统是非线性动力系统中出现的具有确定性、类似随机的过程,既非周期又不收敛,并且对初始值有极其敏感的依赖性。图像信息安全中常用的混沌映射有 Logistic 映射,Arnold 变换和 Henon 映射等。本文选取 Logistic 映射和

Arnold 变换实现图像分存加密。

### 1.1 Logistic 映射

一类非常简单却被广泛研究的动力系统是 Logistic 映射,其典型定义式为:

$$x_{n+1} = \mu x_n (1 - x_n) \quad (1)$$

其中:  $0 \leq \mu \leq 4$  称为分支参数,  $x_n \in (0,1)$ 。混沌动力系统的研究表明:当  $0 < \mu \leq 3.569945$  时,该动力系统从稳定状态分叉产生倍周期;当  $3.569945 < \mu \leq 4$  时,该动力系统进入混沌状态,由初始条件  $x_n$  在 Logistic 映射的作用下所产生的序列  $\{x_n | n = 0, 1, \dots\}$  非周期、不收敛,且对初始值非常敏感。

### 1.2 Arnold 变换

Arnold 变换是 Arnold 在遍历理论研究中提出的一种变换,是典型的混沌系统。Arnold 变换实际上是一种点的位置移动,并且这种变换是一一对应的。根据所选择相位空间的不同可分为二维、三维、四维直至  $F$  维的 Arnold 变换。常用的二维离散 Arnold 变换可描述为:

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \cdot \begin{bmatrix} x_n \\ y_n \end{bmatrix} \bmod (F) \quad (2)$$

其中:  $x_n$  和  $y_n$  为变换前的值,  $x_{n+1}$  和  $y_{n+1}$  为变换后的值。需要注意的是,Arnold 变换具有周期性,即当迭代到某一步时,将重新得到原始数据。Dyson 和 Falk 分析了离散 Arnold 变换的周期性,给出了对于任意  $F > 2$ , Arnold 变换的周期为  $T_F \leq F^2/2$ ,并对部分的最小周期证明了  $P(F) \leq 12 \times F/7$ 。考虑到

收稿日期:2011-04-19;修回日期:2011-06-16。

基金项目:陕西省自然科学基金资助项目(2009JM8004);陕西省教育厅科技计划项目(09JK730;2010JK816)。

作者简介:侯文滨(1985-),男,陕西西安人,硕士研究生,主要研究方向:图像编码、加密; 吴成茂(1968-),男,四川仪陇人,高级工程师,主要研究方向:图像处理。

固定参数 Arnold 变换的安全性仅与变换轮数有关, 缺乏图像加密的灵活性和安全性, 于是文献[4] 提出了变参数二维离散 Arnold 变换, 其方程如下:

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} = \begin{bmatrix} 1 & a \\ b & 1+ab \end{bmatrix} \cdot \begin{bmatrix} x_n \\ y_n \end{bmatrix} \bmod (F)$$

文献[5] 将变参数的 Arnold 变换推广到三维, 其变换如下:

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \\ z_{n+1} \end{bmatrix} = A H Q \begin{bmatrix} x_n \\ y_n \\ z_n \end{bmatrix} \bmod (F) \quad (3)$$

其中:

$$A = \begin{bmatrix} 1 & a_z & 0 \\ b_z & a_z b_z + 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

$$H = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & a_x \\ 0 & b_x & a_x b_x + 1 \end{bmatrix}$$

$$Q = \begin{bmatrix} 1 & 0 & a_y \\ 0 & 1 & 0 \\ b_y & 0 & a_y b_y + 1 \end{bmatrix}$$

$a_x, a_y, a_z, b_x, b_y, b_z$  都是正整数, 并且  $\det(AHQ) = 1$ 。

## 2 Arnold 变换参数的选取

根据图像的类型选定有限域  $GF(2^t)$ , 其中  $t$  为正整数(本文  $t = 8$ )。Arnold 变换的参数及轮数取值于 Logistic 映射生成的离散混沌序列, 考虑到分存加密过程在模 256 内进行, 因此 Arnold 变换的参数取 1 ~ 255 的整数。其详细步骤如下:

第 1 步 用 Logistic 映射  $x_{n+1} = \mu x_n (1 - x_n)$  产生一维混沌实数序列  $\{x_n | x_n \in (0, 1)\}$ , 其中  $3.569945 \cdots < \mu \leq 4$ 。

第 2 步 如果  $(w+1)/257 \leq x_n < (w+2)/257$ , 则  $x_n = w$ , 显然这样得到  $x_n \in \{1, 2, \dots, 255\}$ 。

## 3 图像分存

图像分存需要考虑到的一个重要因素是数据膨胀率, 文献[6] 生成的分存图像是原图大小的 4 倍, 增加了存储空间。本文提出的分存方法使分存图像的大小与原图像大小相同, 可有效降低现有分存方法的数据膨胀。

### 3.1 图像分存

应用离散 Arnold 变换实现图像分存, 将每个位置的像素都分解成两个值, 选用  $M \times N$  的图像  $I$ , 其相应的离散 Arnold 变换表达式如下:

$$\begin{cases} (x_{i,j} + a_{i,j} y_{i,j}) \bmod (256) = I_{i,j} \\ (x_{i,j} b_{i,j} + (1 + a_{i,j} b_{i,j}) y_{i,j}) \bmod (256) = 255 - I_{i,j} \end{cases} \quad (4)$$

其中:  $a_{i,j}$  和  $b_{i,j}$  是由 Logistic 映射控制的可变参数,  $I_{i,j}$  是图像位置  $(i, j)$  的像素值大小,  $x_{i,j}$  和  $y_{i,j}$  分别是分解后两幅分存图像位置  $(i, j)$  处的像素值大小。选取图像位置  $(i, j)$  处灰度值的补码值  $255 - I_{i,j}$  作为 Arnold 变换中  $y$  的初值, 可以避免像素值为零时 Arnold 变换产生零值序列的问题。

本文 Arnold 变换系数矩阵:

$$S = \begin{bmatrix} 1 & a_{i,j} \\ b_{i,j} & 1 + a_{i,j} b_{i,j} \end{bmatrix}$$

其行列式  $|S| = 1$ , 因此满足系数矩阵在模 256 运算下存在逆

矩阵的充要条件  $\gcd(|S|, 256) = 1$ , 所以该方程在有限域下的解具有唯一性, 即得到的分解值是唯一的。由此可知图像  $I$  的每个像素  $I_{i,j}$  用变参数的离散 Arnold 变换产生的两个像素值  $x_{i,j}, y_{i,j}$  具有唯一性, 即分存图像与原图像每个位置上的灰度值一一对应。因此, 图像  $I$  经过 Arnold 变换所产生的两幅分存图像  $X, Y$  的大小均与  $I$  相同。其详细步骤如下:

1) 用 3 个初始值分别是  $k_i (i = 1, 2, 3)$ , 参数分别是  $\mu_i (i = 1, 2, 3)$  的 Logistic 映射生成离散 Arnold 变换的参数  $a_{i,j}, b_{i,j} (i = 1, 2, \dots, M; j = 1, 2, \dots, N)$  和轮数  $d_{i,j} (i = 1, 2, \dots, M; j = 1, 2, \dots, N)$ 。

2) 将原图像  $I$  中位置  $(i, j)$  处的像素灰度  $I_{i,j}$  及其补码值  $255 - I_{i,j}$  作为离散 Arnold 变换的初始值  $x_0, y_0$ , 进行  $d_{i,j}$  轮迭代运算, 得到分存图像  $X$  和  $Y$  中位置  $(i, j)$  处的灰度值  $x_{i,j}, y_{i,j}$ 。

### 3.2 像素扩散的图像分存加密

使用二维离散 Arnold 变换得到的分存图像中每个位置的像素值仅与原图像中该位置的像素值有关, 因此不能抵抗明文攻击和差分攻击。这里首先对图像像素进行置乱, 再利用三维离散 Arnold 变换将图像分存并使像素值扩散, 从而使算法具有更高的抗攻击能力。

因变参数的离散 Arnold 变换消除了周期性, 所以选用变参数的二维离散 Arnold 变换对图像置乱, 以提升加密的效果。首先用两个初始值分别是  $k_i (i = 1, 2)$ , 参数分别是  $\mu_i (i = 1, 2)$  的 Logistic 映射生成二维离散 Arnold 变换的参数  $a_{i,j}, b_{i,j} (i = 1, 2, \dots, lu)$ , 其中  $lu$  为置乱轮数。其次在第  $i$  轮使用参数为  $a_i, b_i$  的二维离散 Arnold 变换对图像进行置乱, 经过  $lu$  轮后得到置乱加密图像  $I_o$ 。Logistic 映射的初始值  $k_i (i = 1, 2)$ , 参数  $\mu_i (i = 1, 2)$  和置乱循环轮数  $lu$  均作为密钥使用。

三维离散 Arnold 变换的系数矩阵也满足有限域下可逆的充要条件  $\gcd(|AHQ|, 256) = 1$ , 因此其分解值具有唯一性。本文三维离散 Arnold 变换表达式如下:

$$\begin{bmatrix} x_{i,j} \\ y_{i,j} \\ z_{i,j} \end{bmatrix} = AHQ \begin{bmatrix} I_{i,j} \\ 255 - I_{i,j} \\ r_{i,j} \end{bmatrix} \bmod (256) \quad (5)$$

其中  $I_{i,j}$  是图像位置  $(i, j)$  处像素值的大小。为便于算法描述, 记  $I_{(i,j)} = I_{(Ni+j)}$ , 令  $M \times N = l$ , 二维下标的  $I_{i,j}$  被记为一维下标的  $I_{(Ni+j)}$ , 即为  $I_1, I_2, \dots, I_l$ ,  $r$  取  $0 \sim 255$  中的任意整数。

分存步骤如下:

1) 用初始值分别是  $k_i (i = 1, 2, \dots, 7)$ , 参数分别是  $\mu_i (i = 1, 2, \dots, 7)$  的 Logistic 映射生成离散 Arnold 变换的参数  $a_{x(i)}, b_{x(i)}, a_{y(i)}, b_{y(i)}, a_{z(i)}, b_{z(i)} (i = 1, 2, \dots, 2 \times l)$  和轮数  $d_i (i = 1, 2, \dots, 2 \times l)$ 。

2) 选取参数是  $a_{x(1)}, b_{x(1)}, a_{y(1)}, b_{y(1)}, a_{z(1)}, b_{z(1)}$  的离散 Arnold 变换, 将  $I_1$  及  $255 - I_1$  作为变换的初始值  $x_0$  和  $y_0$ ,  $r$  作为初始值  $z_0$ , 进行  $d_1$  轮迭代运算, 生成  $x_1, y_1, z_1$ , 然后  $X_1 \leftarrow x_1, Y_1 \leftarrow y_1, r \leftarrow z_1$ 。

3) 选取参数是  $a_{x(2)}, b_{x(2)}, a_{y(2)}, b_{y(2)}, a_{z(2)}, b_{z(2)}$  的离散 Arnold 变换, 将  $I_2$  及  $255 - I_2$  作为变换的初始值  $x_0$  和  $y_0$ ,  $r$  作为初始值  $z_0$ , 进行  $d_2$  轮迭代运算, 生成  $x_2, y_2, z_2$ , 然后  $X_2 \leftarrow x_2, Y_2 \leftarrow y_2, r \leftarrow z_2$ 。

如此继续, 直到  $i = l$ 。

4) 选取参数是  $a_{x(l)}, b_{x(l)}, a_{y(l)}, b_{y(l)}, a_{z(l)}, b_{z(l)}$  的离散 Arnold 变换, 将  $I_l$  及  $255 - I_l$  作为变换的初始值  $x_0$  和  $y_0$ ,  $r$  作为初始值  $z_0$ , 进行  $d_l$  轮迭代运算, 生成  $x_l, y_l, z_l$ , 然后  $X_l \leftarrow x_l, Y_l \leftarrow y_l, r \leftarrow z_l$ 。

5) 重复 1) ~ 4) 一遍, 其中离散 Arnold 变换的参数为  $a_{x(l+i)}, b_{x(l+i)}, a_{y(l+i)}, b_{y(l+i)}, a_{z(l+i)}, b_{z(l+i)}$ , 轮数为  $d_{l+i}$  ( $i = 1, 2, \dots, l$ )。

6) 将得到的  $X, Y$  作为分存图像, 最终的  $r$  值作为解密密钥。

### 3.3 彩色图像分存

一幅彩色图像由 RGB 3 个灰度分量图像组成, 因此加密彩色图像可以看做对 RGB 3 个灰度分量图像进行加密。这里为了使 RGB 灰度图像间的像素得到扩散, 采用如下三维离散 Arnold 变换:

$$\begin{bmatrix} x_{i,j}^1 \\ y_{i,j}^1 \\ z_{i,j}^1 \end{bmatrix} = \mathbf{AHQ} \begin{bmatrix} R_{i,j} \\ 255 - G_{i,j} \\ r_r \end{bmatrix} \bmod (256) \quad (6)$$

$$\begin{bmatrix} x_{i,j}^2 \\ y_{i,j}^2 \\ z_{i,j}^2 \end{bmatrix} = \mathbf{AHQ} \begin{bmatrix} G_{i,j} \\ 255 - B_{i,j} \\ r_g \end{bmatrix} \bmod (256) \quad (7)$$

$$\begin{bmatrix} x_{i,j}^3 \\ y_{i,j}^3 \\ z_{i,j}^3 \end{bmatrix} = \mathbf{AHQ} \begin{bmatrix} B_{i,j} \\ 255 - R_{i,j} \\ r_b \end{bmatrix} \bmod (256) \quad (8)$$

其中每组离散 Arnold 变换产生分存图像的方法与灰度图像方法相同, 首先, 使用参数可变的二维离散 Arnold 变换对灰度图像分量分别进行轮数为  $lu_1, lu_2, lu_3$  的置乱; 其次, 用 Logistic 映射生成长度为  $6 \times l$  的混沌序列, 每组三维离散 Arnold 变换依次取  $2 \times l$  个混沌值作为参数和轮数, 得到灰度分量图像  $\mathbf{R}$  的分存图像为  $X_1, Y_3$ , 灰度分量图像  $\mathbf{G}$  的分存图像为  $X_2, Y_1$ , 灰度分量图像  $\mathbf{B}$  的分存图像为  $X_3, Y_2$ , 则原彩色图像  $\mathbf{I}$  的分存图像  $\mathbf{X}$  由  $X_1, X_2, X_3$  组成, 分存图像  $\mathbf{Y}$  由  $Y_1, Y_2, Y_3$  组成, 最终的  $r, r_g, r_b$  的值作为解密密钥。

### 4 解密过程

解密是分存加密的逆过程, 需要利用离散 Arnold 变换的逆变换, 根据密钥参数进行逆向迭代运算可得到原图像。

本文选取的二维 Arnold 变换逆变换为:

$$\begin{bmatrix} 1 + a_{i,j}b_{i,j} & -b_{i,j} \\ -a_{i,j} & 1 \end{bmatrix} \cdot \begin{bmatrix} x_{i,j}^n \\ y_{i,j}^n \end{bmatrix} \bmod (256) = \begin{bmatrix} x_{i,j}^{n+1} \\ y_{i,j}^{n+1} \end{bmatrix} \quad (9)$$

而三维 Arnold 变换的逆变换为:

$$(\mathbf{AHQ})^{-1} \begin{bmatrix} x_{i,j} \\ y_{i,j} \\ z_{i,j} \end{bmatrix} \bmod (256) = \begin{bmatrix} I_{i,j} \\ 255 - I_{i,j} \\ r_i \end{bmatrix} \quad (10)$$

### 5 实验结果及分析

分别对灰度图像和彩色图像进行加密测试, 然后分析灰度图像的密钥敏感度、密钥空间、像素相关性和抗攻击能力等, 以便验证算法的高安全性。

#### 5.1 加密实验

针对如图 1(a) 所示的灰度图像, 取初始值  $lu = 150$ ,  $k_1 = 0.7$ ,  $k_2 = 0.7001$ ,  $k_3 = 0.5006$ ,  $k_4 = 0.3009$ ,  $k_5 = 0.4009$ ,  $k_6 = 0.8004$ ,  $k_7 = 0.9003$ ;  $\mu_1 = 3.99$ ,  $\mu_2 = 3.88$ ,  $\mu_3 = 3.77$ ,  $\mu_4 = 3.44$ ,  $\mu_5 = 3.56$ ,  $\mu_6 = 3.68$ ,  $\mu_7 = 3.58$ ; 经过 Arnold 置乱后如图 1(b) 所示; 分存图像  $X, Y$  如图 1(c) 和 (d) 所示。

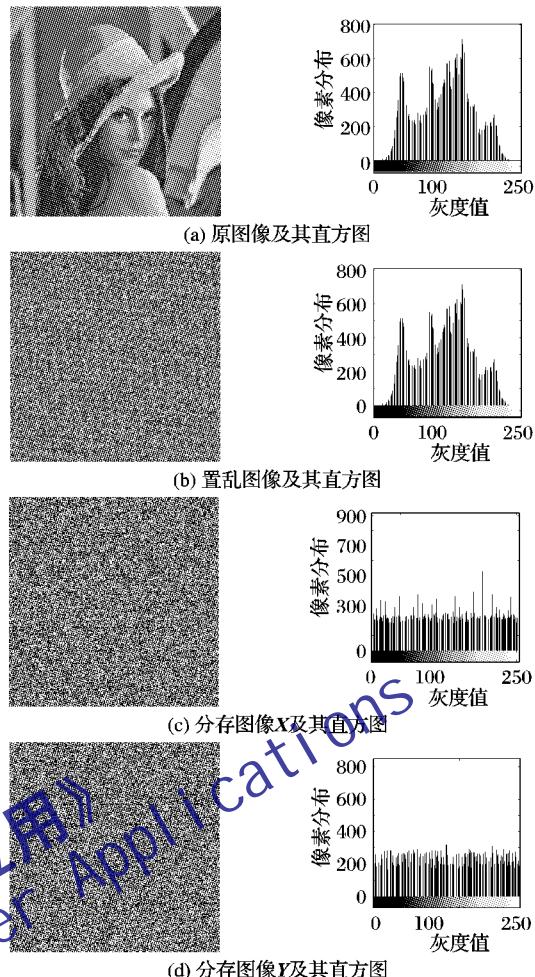


图 1 原灰度图像及分存加密结果

针对如图 2(a) 所示的彩色图像, 取初始值  $lu = 150$ ,  $k_1 = 0.7$ ,  $k_2 = 0.7001$ ,  $k_3 = 0.5006$ ,  $k_4 = 0.3009$ ,  $k_5 = 0.4009$ ,  $k_6 = 0.8004$ ,  $k_7 = 0.9003$ ;  $\mu_1 = 3.99$ ,  $\mu_2 = 3.88$ ,  $\mu_3 = 3.77$ ,  $\mu_4 = 3.44$ ,  $\mu_5 = 3.56$ ,  $\mu_6 = 3.68$ ,  $\mu_7 = 3.58$ ; 分存图像  $X$  见图 2(b); 分存图像  $Y$  见图 2(c)。

#### 5.2 密钥敏感性测试

以灰度图像为例, 选取 3 组错误的密钥解密以检测密钥敏感性。图 3(a) 为使用了错误密钥  $lu = 150$ ,  $k_1 = 0.7002$ ,  $k_2 = 0.7001$ ,  $k_3 = 0.5006$ ,  $k_4 = 0.3009$ ,  $k_5 = 0.4009$ ,  $k_6 = 0.8004$ ,  $k_7 = 0.9003$ ;  $\mu_1 = 3.99$ ,  $\mu_2 = 3.88$ ,  $\mu_3 = 3.77$ ,  $\mu_4 = 3.44$ ,  $\mu_5 = 3.56$ ,  $\mu_6 = 3.68$ ,  $\mu_7 = 3.58$  解密的图像。图 3(b) 为使用了错误密钥  $lu = 150$ ,  $k_1 = 0.7$ ,  $k_2 = 0.7001$ ,  $k_3 = 0.5006$ ,  $k_4 = 0.4000$ ,  $k_5 = 0.4009$ ,  $k_6 = 0.8004$ ,  $k_7 = 0.9003$ ;  $\mu_1 = 3.99$ ,  $\mu_2 = 3.88$ ,  $\mu_3 = 3.77$ ,  $\mu_4 = 3.44$ ,  $\mu_5 = 3.56$ ,  $\mu_6 = 3.68$ ,  $\mu_7 = 3.58$  解密的图像。图 3(c) 为使用了错误密钥  $lu = 150$ ,  $k_1 = 0.7$ ,  $k_2 = 0.7001$ ,  $k_3 = 0.5006$ ,  $k_4 = 0.3009$ ,  $k_5 = 0.4009$ ,  $k_6 = 0.8004$ ,  $k_7 = 0.8023$ ;  $\mu_1 = 3.99$ ,  $\mu_2 = 3.88$ ,  $\mu_3 = 3.77$ ,  $\mu_4 = 3.44$ ,  $\mu_5 = 3.56$ ,  $\mu_6 = 3.68$ ,  $\mu_7 = 3.58$  解密的图像。图 3(d) 为使用了错误密钥  $lu = 140$ ,  $k_1 = 0.7$ ,  $k_2 = 0.7001$ ,  $k_3 = 0.5006$ ,  $k_4 = 0.3009$ ,  $k_5 = 0.4009$ ,  $k_6 = 0.8004$ ,  $k_7 = 0.8023$ ;  $\mu_1 = 3.99$ ,  $\mu_2 = 3.88$ ,  $\mu_3 = 3.77$ ,  $\mu_4 = 3.44$ ,  $\mu_5 = 3.56$ ,  $\mu_6 = 3.68$ ,  $\mu_7 = 3.58$  解密的图像。图 3(e) 为使用了错误密钥  $lu = 150$ ,  $k_1 = 0.7$ ,  $k_2 = 0.7001$ ,  $k_3 = 0.5006$ ,  $k_4 = 0.3009$ ,  $k_5 = 0.4009$ ,  $k_6 = 0.8004$ ,  $k_7 = 0.8023$ ;  $\mu_1 = 3.98$ ,  $\mu_2 = 3.88$ ,  $\mu_3 = 3.77$ ,  $\mu_4 = 3.44$ ,  $\mu_5 = 3.56$ ,  $\mu_6 = 3.68$ ,  $\mu_7 = 3.58$  解密的图像。图 3(f) 为使用正确密钥解密的图像。

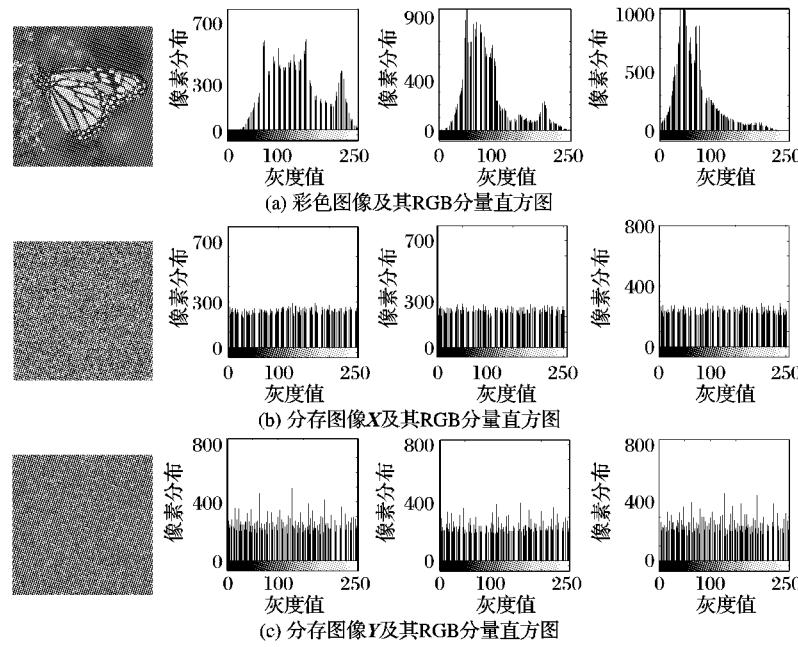


图2 原彩色图像及分存结果

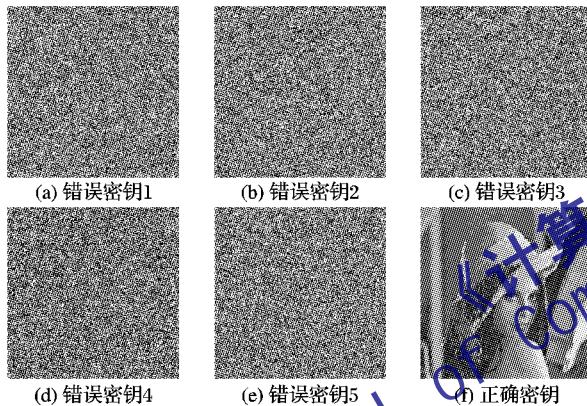


图3 正确或错误密钥下的解密结果

由解密图可知 $k_i$ 、 $lu$ 或 $\mu_i$ 的任何变化都将使解密失败。由以上实验可知,只有与加密密钥完全一致的解密密钥,才能够正确解密,因此算法对密钥敏感。

### 5.3 密钥空间分析

高度的密钥敏感性和足够大的密钥空间可以抵抗穷举攻击。本算法在解密时需要密钥 $k_i$ 、 $\mu_i$ ( $i = 1, 2, \dots, 7$ )、 $lu$ 和 $r_i$ ,由Logistic映射生成的参数长度为 $2 \times M \times N$ 。因此本文算法提供的密钥空间足够大。

### 5.4 统计分析

原灰度图像直方图如图1(a),分存图像灰度直方图如图1(c)和(d)。对比可知分存后图像灰度直方图呈均匀分布,未保留任何明文信息。同时由于加密过程中每个位置的像素都扩散到整幅图中,因此算法能够有效抵抗统计分析攻击和已知明文攻击。

### 5.5 相邻像素的相关性分析

相邻像素的相关性可以反映出图像像素的扩散程度,原始图像中相邻两个像素的相关性通常很大,加密后图像相邻像素的相关性要尽可能小。分别随机选取灰度图像原图和分存图像的10000对水平方向、竖直方向和对角方向上的相邻像素进行测试。利用如式(11)计算其相关系数:

$$\begin{cases} \text{cov}(x, y) = E(x - E(x)) \times (y - E(y)) \\ r_{xy} = \frac{\text{cov}(x, y)}{\sqrt{D(x)} \times \sqrt{D(y)}} \end{cases} \quad (11)$$

计算原始灰度图像和分存灰度图像各方向的相关关系如表1所示。

表1 相关系数

图像	水平	垂直	对角
原图	0.9593	0.9280	0.9151
加密图X	4.987E-004	2.3114E-005	8.974E-005
加密图Y	0.0428	-0.0026	0.0027

由表1可知,分存后图像的相邻像素间相关性显著减少。图4为对角方向上原始图像和分存图像相邻像素的相关关系情况。可见,原始图像像素间的相关性呈现明显的线性相关,而分存图像像素间的相关性呈随机分布特性,这表明本算法具有较强的抗相关分析攻击能力。

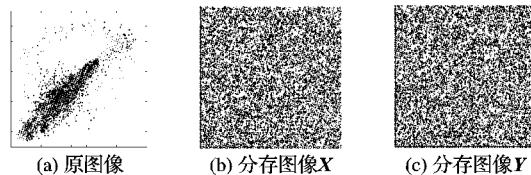


图4 对角方向相邻像素相关分布

### 5.6 抵抗差分攻击

攻击者采取对图像作微小修改来观察解密结果的变化,这样可能发现原始图像和加密图像之间的某些关系。一般采用两个参数对这种变化进行描述,即像素变化率( $R_{RNPC}$ )和平均变化强度( $I_{IUCA}$ ),对于一幅原始图像,其加密图像为 $C_1$ ,若对其修改一个像素点的灰度值进行加密的结果为 $C_2$ ,比较灰度值矩阵 $C_1$ 和 $C_2$ 所有点的值。如果 $C_1(i, j) = C_2(i, j)$ ,则 $V(i, j) = 1$ ;否则为0。

$$R_{RNPC} = \frac{\sum V(i, j)}{M \times N} \times 100\% \quad (12)$$

$$I_{IUCA} = \frac{1}{M \times N} \sum_{i, j} \frac{|C_1(i, j) - C_2(i, j)|}{255} \times 100\% \quad (13)$$

通过计算得到分存图像X的 $R_{RNPC} = 0.0945$ , $I_{IUCA} = 0.0027$ ,分存图像Y的 $R_{RNPC} = 0.0945$ , $I_{IUCA} = 5.4363E-004$ ,表明对原始图像进行微小改变会导致分存图像很大变化,故算法具有较强的抵抗差分攻击能力。

### 5.7 峰值信噪比

峰值信噪比(Peak Signal-to-Noise Ratio, PSNR)是图像信噪比变化情况的统计平均,它是目前广泛应用的衡量图像主观质量的方法。在图像分存处理中,PSNR 可以用来衡量还原后图像与原图像的相近程度。PSNR 定义如下:

$$PSNR = 10 \lg \frac{M \times N \times 255^2}{\sum_{M,N} [I(i,j) - I'(i,j)]^2} \quad (14)$$

其中: $I(i,j)$  为原图像像素值,  $I'(i,j)$  为还原图像像素值。通过实验,本文灰度图像的  $PSNR = INF$ ,说明解密后的图像与原图一致,未产生失真。

## 6 结语

本文采用 Logistic 映射产生的混沌序列控制 Arnold 变换参数,图像先通过 Arnold 变换置乱后再产生两幅分存图像。其加密结果的安全性受到 3 方面因素控制:1) Logistic 映射;2) Arnold 变换;3) 根据明文图像产生的内部密钥。该方法解决了图像细节信息暴露即分存图像显示出原图轮廓特征的问题,而且因为没有采用门限方案,因此可以精确地恢复图像。将位置置乱和像素值分解相结合,不仅对原图像的像素进行了非线性扩散,而且明文、密文、密钥之间的函数关系具有高度的非线性和复杂的统计关系。同时内部密钥与明文图像也紧密相关,明文图像的微小改变不仅会影响整幅分存图像而且还会改变内部密钥,因此能够抵抗差分攻击。通过实验也证明这种算法具较好的安全性,在图像信息安全方面具有很好的应用前景。

### 参考文献:

- [1] 王继军, 张显全, 张军洲, 等. 一种新的数字图像分存方法[J]. 计算机工程与应用, 2007, 43(31): 79–81.

(上接第 2681 页)

### 参考文献:

- [1] PENNY T, BAS P, FRIDRICH J. Steganalysis by subtractive pixel adjacency matrix [J]. IEEE Transaction on Information Forensics and Security, 2010, 5(2): 215–224.
- [2] LYU S, FARID H. Steganalysis using higher-order image statistics [J]. IEEE Transactions on Information Forensics and Security, 2006, 1(1): 111–119.
- [3] SHI YUNQING, XUAN GUORONG, ZOU DEKUN, et al. Image steganalysis based on moments of characteristic functions using wavelet decomposition, prediction-error image, and neural network [C]// Proceedings of 2005 IEEE International Conference on Multimedia and Expo. Piscataway, NJ: IEEE Press, 2005: 269–272.
- [4] HOLOTYAK T, FRIDRICH J, VOLOSHYNOVSKIY S. Blind statistical steganalysis of additive steganography using wavelet higher order statistics [C]// Proceedings of the 9th IFIP TC-6 TC-11 Conference on Communications and Multimedia Security, LNCS 3677. Berlin: Springer, 2005: 273–274.
- [5] GOLJAN M, FRIDRICH J, HOLOTYAK T. New blind steganalysis and its implications [C]// Proceedings of SPIE, Security, Steganography, and Watermarking of Multimedia Contents VII. Berlin: Springer, 2006, 6072: 1–13.
- [6] WANG YING, MOULIN P. Optimized feature extraction for learning-based image steganalysis [J]. IEEE Transactions on Information Forensics and Security, 2007, 2(1): 31–45.
- [7] LIU ZUGEN, PING LINGDI, CHEN JIAN, et al. Steganalysis

- [2] 赖新光, 罗慧. 基于矩阵分解的数字图像分存技术[J]. 计算机工程与应用, 2004, 40(32): 96–98.
- [3] ZHANG YUANBIAO, WANG DE. An image encryption and sharing algorithm based on chaos and indeterminate equation [C]// Proceedings of CiSE 2009. Piscataway, NJ: IEEE Press, 2009: 1–4.
- [4] 马在光, 丘水生. 基于广义猫映射的一种图像加密系统[J]. 通信学报, 2004, 24(2): 51–57.
- [5] CHEN G R, MAO Y B, CHUI C K. A symmetric image encryption scheme based on 3D chaotic cat map [J]. Chaos, Solitons & Fractals, 2004, 21(3): 749–761.
- [6] LUKAC R, PLATANIOTIS K N. Color image secret sharing [J]. Electronics Letters, 2004, 40(9): 529–531.
- [7] 殷国富. 基于复合混沌系统的数字图像加密方法研究[J]. 计算机应用, 2006, 26(4): 827–829.
- [8] 杨帆, 薛模根. 复合混沌二级置乱图像加密算法研究[J]. 合肥工业大学学报: 自然科学版, 2009, 32(8): 1128–1131.
- [9] 张元标. 基于一次不定方程的数字图像加密技术[J]. 成都理工大学学报: 自然科学版, 2006, 33(6): 645–648.
- [10] 唐聃, 王晓京, 陈静. 新的图像加密方法[J]. 电子科技大学学报, 2010, 39(1): 128–132.
- [11] 张瀚, 王秀峰, 李朝晖. 一种基于混沌系统及 Henon 映射的快速图像加密算法[J]. 计算机研究与发展, 2005, 42(12): 2137–2142.
- [12] 彭飞, 丘水生, 龙敏. 外部密钥控制系统参数的图像加密算法[J]. 华南理工大学学报: 自然科学版, 2005, 33(7): 20–23.
- [13] 徐淑华, 王继志. 一类改进的混沌迭代加密算法[J]. 物理学报, 2008, 57(1): 37–41.
- [14] 张欣, 杨德刚, 朱凯. 一种基于外部密钥的混沌加密方法[J]. 重庆师范大学学报: 自然科学版, 2010, 27(2): 57–64.
- [15] 朱从旭, 廖建华. 一种基于外部密钥和密文反馈的混沌密码新算法[J]. 软件导刊, 2010, 9(1): 62–64.

based on differential statistics [C]// Proceedings of CANS 2006, LNCS 4301. Berlin: Springer, 2006: 224–240.

- [8] LI BIN, HUANG JIWU, SHI YUNQING. Textural feature based universal steganalysis [C]// Proceedings of SPIE, Security, Steganography, and Watermarking of Multimedia Contents X. Berlin: Springer, 2008, 6819: 1–12.
- [9] MIELIKAINEN J. LSB matching revisited [J]. IEEE Transactions on Signal Processing, 2006, 13(5): 285–287.
- [10] YANG C H, WENG C Y, WANG S J, et al. Adaptive data hiding in edge areas of images with spatial LSB domain systems [J]. IEEE Transactions on Information Forensics and Security, 2008, 3(3): 488–497.
- [11] LUO WEIQI, HUANG FANGJUN, HUANG JIWU. Edge adaptive image steganography based on LSB matching revisited [J]. IEEE Transaction on Information Forensics and Security, 2010, 5(2): 201–214.
- [12] SOLANKI K, SARKAR A, MANJUNATH B S. YASS: Yet another steganographic scheme that resists blind steganalysis [C]// Proceedings of IH 2007, LNCS 4567. Berlin: Springer-Verlag, 2007, 4567: 16–31.
- [13] LUO XIANGYANG, DAO SHUNWANG, WANG PING, et al. A review on blind detection for image steganography [J]. Signal Processing, 2008, 88(9): 2138–2157.
- [14] LIU QINGZHONG, SUNG A H, RIBEIRO B, et al. Image complexity and feature mining for steganalysis of least significant bit matching steganography [J]. Information Sciences, 2008, 178(1): 21–36.