# 基于灰度级出现频数的数字图像置乱程度衡量方法

贺楚雄 田绍槐
(湖南大学软件学院, 长沙 410082)

**摘 要** 数字图像置乱程度是评价数字图像置乱算法的重要方面, 对数字水印算法的研究也起到重要的指导作用。利用灰度级出现频数可以对数字图像的最佳(理想)置乱效果进行描述, 以数字图像的最佳(理想)置乱效果为参照系, 基于灰度级出现频数提出了一种衡量数字图像置乱程度的新方法。采用 Matlab为实验研究工具, 进行仿真实验。实验结果表明, 该置乱程度衡量方法与视觉的主观评价基本一致, 具有对各种类型的图像加密方法都适用的高泛化性, 还具有与原图像无关性。

**关键词** 数字图像 置乱变换 置乱程度 灰度级出现频数
**中图法分类号**: TP391 **文献标志码**: A **文章编号**: 1006-8961(2010)02-0220-09

# Digital Image Scrambling Degree Evaluation Method Based on Frequency of Gray Levels

HE Chu-xiong, TIAN Shao-huai
*(Software School of Hunan University, Changsa 410082)*

**Abstract** Digital image scrambling degree is one of the most important aspects of evaluating digital image scrambling algorithm, it has significant effects on the research of digital watermark algorithm. It can describe the best effects of digital image scrambling by taking the frequency of gray levels. Using the best effects of digital image scrambling as parameters, this paper has presented a new method of measuring digital image scrambling degree based on the frequency of gray levels. Emulational experiments have been carried out in MATLAB. The results of the experiment have suggested that the digital image scrambling degree evaluation method is the same as all sorts of image encrypting. The resulting digital image scrambling degree is accordant with visual subjective evaluation, it would not differ a lot for the sake of the changing of its former image as well.

**Keywords** digital image; scrambling transformation; image scrambling degree(ISD); frequency of gray levels

## 0 引 言

图像信息生动形象, 已经成为人类表达信息的重要手段之一。随着 Internet技术与多媒体技术的飞速发展, 图像数据的保护越来越受到社会的重视。

国内外的专家学者提出了许多数字图像加密方法。经分析发现, 这些加密变换可分为以下 3种类型: 1)仅变换像素位置的图像加密; 2)仅变换像素灰度值的图像加密; 3)像素位置及灰度值都发生变换的图像加密[1]。

由此可见, 图像加密的本质就是像素的位置或

收稿日期: 2008-09-02; 改回日期: 2008-12-03

第一作者简介: 贺楚雄(1972— ), 男, 江西工业工程职业技术学院副教授。湖南大学软件学院硕士研究生。主要研究方向为图像处理与信息安全、应用数学。E-mail: hechuxiong@tom.com

灰度值的置乱。

目前, 数字图像置乱算法的置乱分布性的衡量是评价数字图像置乱算法的重要方面[2]。

另外, 数字水印技术也是图像数据版权保护的重要方法, 置乱程度衡量对于置乱到什么程度时水印算法的鲁棒性最强起到重要的指导作用。

因此, 研究置乱程度衡量有着重要的理论和实际意义。

许多学者对图像的置乱程度及其衡量进行了研究, 提出了一些衡量图像置乱程度的方法。文献[3]利用图像所有像素的一阶距离均值和方差之比定义一阶置乱度, 再将其推广为 $n$阶置乱度, 该方法对变换像素位置的置乱具有较好的效果; 文献[4]利用原图像中相邻像素变换后距离变化的均值和方差之比定义置乱度, 该方法对变换像素位置的置乱也具有较好的效果; 文献[5]综合利用不动点、自然率、$k$阶位置因子、$k$阶矩、置乱矩阵的相关性等性能指标较好地对变换像素位置的置乱程度进行了度量; 文献[1, 6]综合利用不动点比、信息熵、灰度平均变化值、图像的自相关度、图像相似度等参数进行置乱程度的度量, 可以有效地对加密图像的置乱度及安全性进行分析和评价; 文献[7-8]根据相邻点的相关性, 通过比较置乱前后每个点与其相邻点相关性的差异来衡量图像的置乱程度, 该方法可以有效衡量图像置乱程度及反映加密次数与置乱效果程度的关系; 文献[9]在相邻灰度差置乱度的基础上, 进一步得到平均相邻灰度差置乱度, 再利用 Canny算子的良好特性, 提出了基于 Canny算子的置乱度, 该方法与人的主观评价相近, 且不受原图影响; 文献[2]将像素移动的距离和像素点与周围像素点灰度值偏差两方面结合起来度量图像的置乱程度, 可以较好地反映置乱程度; 文献[10]将熵的方法引入图像置乱度的衡量中, 提出用灰度差分熵来定义图像置乱程度, 较好地刻画了图像的置乱效果; 文献[11]在文献[10]的基础上, 提出用一阶距和二阶距灰度差分熵的平均值来计算置乱度的方法, 得到一些较好的性质, 具有一些优点; 文献[12]将交叉熵的方法引入图像置乱度的衡量中, 将交叉熵与图像的最优分块处理相结合, 提出基于分块交叉熵的图像置乱程度评价方法, 文献[13]将均方信噪比(SNR)与图像的最优分块处理相结合, 提出了基于SNR的数字图像置乱程度的评价方法, 这两种方法都能较好地刻画图像的置乱程度, 反映了加密次数与置乱程度的关系, 与人的视觉基本相符; 文献[14]首先提出了理想置乱变换和置乱程度的定义, 然后利用 Walsh变换的能力集中特性, 并考虑置乱程度应满足的性质, 提出了基于 Walsh变换的图像置乱程度的评价方法, 该方法能较好地刻画仅变换像素位置的置乱图像的置乱程度, 与人的主观评价更接近。

本文在对数字图像的最佳(理想)置乱状态的本质特征进行分析的基础上, 提出一种新的基于灰度级出现频数的数字图像置乱程度衡量方法及其性质。采用 Matlab为实验研究工具, 进行仿真实验。首先, 在图像加密方法的 3种类型中各选择一种方法作为代表; 其次, 用 3种加密方法对同一图像进行置乱, 得到同一图像的不同置乱的效果; 最后, 分别对多幅不同的图像进行置乱, 得到各自对不同图像的置乱效果。实验结果表明, 该置乱程度衡量方法与视觉的主观评价基本一致, 而且具有对不同类型的加密方法都适用的高泛化性和与原图像无关性。

## 1　理想图像置乱变换及基于灰度级出现频数的置乱程度的定义

数字图像置乱的目的在于打乱图像, 使攻击者不能识别其内容。一般来说, 置乱后的图像相对于原始图像越“乱”表明该置乱算法就越有效, 保密性就越高。然而, “乱”是人的视觉效果, 带有一定主观性, 不同的观察者评价结果可能不同。实际上, “乱”的理想状态应是置乱后的数字图像的像素服从均匀分布的白噪声特性。

因此, 数字图像置乱的基本特征是置乱的分布性, 理想数字图像置乱的本质特征是置乱后像素均匀分布。

首先, 对图像理想置乱效果进行比较客观的描述。

文献[15]给出了图像中灰度级 $v$出现频数的定义:

**定义 1**　设图像 $\boldsymbol{A}=[\alpha(x, y)]_{m\times n}$是一幅 $L$级灰度图像, $f_A(v)$表示图像 $\boldsymbol{A}$中灰度值为 $v$的像素个数, $\|\boldsymbol{A}\|$表示图像 $\boldsymbol{A}$中的像素数, 则称 $f_A(v)$与 $\|\boldsymbol{A}\|$的比值为图像 $\boldsymbol{A}$中灰度级 $v$的出现频数, 记为 $p_A(v)$. 即

$$p_A(v)=\frac{f_A(v)}{\|\boldsymbol{A}\|}=\frac{f_A(v)}{m\times n}\qquad v=0,1,2,\cdots,L-1 \tag{1}$$

这样, 就可以在图像中取任意区域 $\boldsymbol{D}$, 如果区域 $\boldsymbol{D}$ 中每个灰度级 $v$ 的出现频数 $p_D(v)$ 与它在原图像中的出现频数 $p_A(v)$ 相等, 那么可以说明该图像的像素分布是均匀的, 该图像达到了最佳 (理想 )置乱状态。

由此, 可以给出图像最佳 (理想 )置乱效果的定义如下:

**定义 2** 设 $L$ 级灰度图像 $\boldsymbol{A}=[a(x,y)]_{m\times n}$ 经置乱变换 $T$ 变为 $\boldsymbol{B}=[b(x,y)]_{m\times n}$, 取图像 $\boldsymbol{B}$ 任意区域 $\boldsymbol{D}$, 若区域 $\boldsymbol{D}$ 中每个灰度级 $v$ 出现的频数与它在图像 $\boldsymbol{B}$ 中出现的频数相等, 即

$$\frac{f_D(v)}{\|\boldsymbol{D}\|}=\frac{f_B(v)}{m\times n}\qquad v=0,1,2,\cdots,L-1 \tag{2}$$

则称图像 $\boldsymbol{B}$ 为图像 $\boldsymbol{A}$ 的最佳置乱效果或理想置乱效果, 置乱变换 $T$ 为图像 $\boldsymbol{A}$ 的最佳置乱变换或理想置乱变换。

其次, 以图像理想置乱效果为参照系给出基于灰度级出现频数的图像置乱程度的定义如下:

**定义 3** 若 $L$ 级灰度图像 $\boldsymbol{A}=[a(x,y)]_{m\times n}$ 经置乱变换 $T$ 变为 $\boldsymbol{B}=[b(x,y)]_{m\times n}$, 则称

$$\min_{\boldsymbol{D}}\left|1-\frac{1}{2}\sum_v\left|\frac{f_D(v)}{\|\boldsymbol{D}\|}-\frac{f_B(v)}{m\times n}\right|\right|\qquad \|\boldsymbol{D}\|\geqslant L \tag{3}$$

为图像 $\boldsymbol{A}$ 经变换 $T$ 置乱后基于灰度级出现频数的置乱程度, 记为 $ISD_{T(A)}$。

由于图像区域 $\boldsymbol{D}$ 的离散性, 如果 $\|\boldsymbol{D}\|$ 太小, 计算结果就会出现较大误差, 因此一般要求 $\|\boldsymbol{D}\|\geqslant L$。

可以证明, $ISD_{T(A)}$ 满足如下性质:

**性质 1** $0\leqslant ISD_{T(A)}\leqslant 1$

证明:

由 $\left|\frac{f_D(v)}{\|\boldsymbol{D}\|}\right|-\left|\frac{f_B(v)}{m\times n}\right|\leqslant\left|\frac{f_D(v)}{\|\boldsymbol{D}\|}-\frac{f_B(v)}{m\times n}\right|\leqslant\left|\frac{f_D(v)}{\boldsymbol{D}}\right|+\left|\frac{f_B(v)}{m\times n}\right|$,

可得 $\sum_v\left|\frac{f_D(v)}{\|\boldsymbol{D}\|}\right|-\sum_v\left|\frac{f_B(v)}{m\times n}\right|\leqslant\sum_v\left|\frac{f_D(v)}{\|\boldsymbol{D}\|}-\frac{f_B(v)}{m\times n}\right|\leqslant\sum_v\left|\frac{f_D(v)}{\|\boldsymbol{D}\|}\right|+\sum_v\left|\frac{f_B(v)}{m\times n}\right|$

由于 $\sum_v\left|\frac{f_B(v)}{m\times n}\right|\leqslant\sum_{v=0}^{L-1}\left|\frac{f_B(v)}{m\times n}\right|$

于是 $\sum_v\left|\frac{f_D(v)}{\|\boldsymbol{D}\|}\right|-\sum_{v=0}^{L-1}\left|\frac{f_B(v)}{m\times n}\right|\leqslant\sum_v\left|\frac{f_D(v)}{\|\boldsymbol{D}\|}\right|-\sum_v\left|\frac{f_B(v)}{m\times n}\right|\leqslant\sum_v\left|\frac{f_D(v)}{\|\boldsymbol{D}\|}\right|+\sum_v\left|\frac{f_B(v)}{m\times n}\right|\leqslant\sum_v\left|\frac{f_D(v)}{\|\boldsymbol{D}\|}\right|+\sum_{v=0}^{L-1}\left|\frac{f_B(v)}{m\times n}\right|$

因此 $\sum_v\left|\frac{f_D(v)}{\|\boldsymbol{D}\|}\right|-\sum_{v=1}^{L-1}\left|\frac{f_B(v)}{m\times n}\right|\leqslant\sum_v\left|\frac{f_D(v)}{\|\boldsymbol{D}\|}-\frac{f_B(v)}{m\times n}\right|\leqslant\sum_v\left|\frac{f_D(v)}{\|\boldsymbol{D}\|}\right|+\sum_{v=0}^{L-1}\left|\frac{f_B(v)}{m\times n}\right|$

又由于 $\sum_v\left|\frac{f_D(v)}{\|\boldsymbol{D}\|}\right|=1,\ \sum_{v=0}^{L-1}\left|\frac{f_B(v)}{m\times n}\right|=1$

即 $1-1\leqslant\sum_v\left|\frac{f_D(v)}{\|\boldsymbol{D}\|}-\frac{f_B(v)}{m\times n}\right|\leqslant 1+1$

$0\leqslant\sum_v\left|\frac{f_D(v)}{\|\boldsymbol{D}\|}-\frac{f_B(v)}{m\times n}\right|\leqslant 2$

于是 $0\leqslant\frac{1}{2}\sum_v\left|\frac{f_D(v)}{\|\boldsymbol{D}\|}-\frac{f_B(v)}{m\times n}\right|\leqslant 1$

那么 $0\leqslant 1-\frac{1}{2}\sum_v\left|\frac{f_D(v)}{\|\boldsymbol{D}\|}-\frac{f_B(v)}{m\times n}\right|\leqslant 1$

所以 $0\leqslant\min_{\boldsymbol{D}}\left|1-\frac{1}{2}\sum_{v=0}^{L-1}\left|\frac{f_D(v)}{\|\boldsymbol{D}\|}-\frac{f_B(v)}{m\times n}\right|\right|\leqslant 1$

即 $0\leqslant ISD_{T(A)}\leqslant 1$

**性质 2** 对理想置乱变换 $T$ 来说, $ISD_{T(A)}=1$。

证明: 对理想置乱变换 $T$ 来说, 总有

$$\frac{f_D(v)}{\|\boldsymbol{D}\|}=\frac{f_B(v)}{m\times n}$$

则 $\left|\frac{f_D(v)}{\|\boldsymbol{D}\|}-\frac{f_B(v)}{m\times n}\right|=0$

所以 $\min_{\boldsymbol{D}}\left|1-\frac{1}{2}\sum_v\left|\frac{f_D(v)}{\|\boldsymbol{D}\|}-\frac{f_B(v)}{m\times n}\right|\right|=1$

即 $ISD_{T(A)}=1$

## 2　基于灰度级出现频数的置乱程度的实现方法

由于定义 3所定义的置乱程度计算公式 (3) 中区域 $\boldsymbol{D}$ 的任意性, 使得该计算公式在实际应用中不便于计算, 因此, 必须寻求更易于计算的实现方法。

在图像处理中, 有图像最优分块算法, 如 Matlab 软件中的 bestblk 函数。本文通过图像最优分块确定分块的大小 $mb \times nb$, 再从原图中随机抽取 $\frac{m \times n}{L}$ 块大小不小于 $mb \times nb$ 的区域 (其中 $\frac{m \times n}{L}$ 为每个灰度级出现的平均次数 )。这样使公式 (3) 易于计算又体现了区域选取的任意性。具体算法如下:

1) 将置乱后的图像读入矩阵 $\boldsymbol{B}$,

$\boldsymbol{B} = (b_{ij})_{m \times n},\ b_{ij} \in \{0, 1, 2, \cdots, L-1\}$;

2) 在分块的大小 $mb \times nb \geqslant L$ 的条件下, 对矩阵 $\boldsymbol{B}$ 进行最优分块, 确定分块的大小 $mb \times nb$, 同时算出每个灰度级出现的平均次数 $t = \frac{m \times n}{L}$;

3) 从矩阵 $\boldsymbol{B}$ 中随机抽取 $t$ 块区域, 每个区域的大小至少为 $mb \times nb$;

4) 将步骤 3) 中抽取的区域分别存入矩阵 $\boldsymbol{D}_1, \boldsymbol{D}_2, \cdots, \boldsymbol{D}_t$;

5) 分别计算出

$$1 - \frac{1}{2}\sum_v \left| \frac{f_{\boldsymbol{D}_1}(v)}{\|\boldsymbol{D}_1\|} - \frac{f_{\boldsymbol{B}}(v)}{m \times n} \right|,$$

$$1 - \frac{1}{2}\sum_v \left| \frac{f_{\boldsymbol{D}_2}(v)}{\|\boldsymbol{D}_2\|} - \frac{f_{\boldsymbol{B}}(v)}{m \times n} \right|, \cdots,$$

$$1 - \frac{1}{2}\sum_v \left| \frac{f_{\boldsymbol{D}_t}(v)}{\|\boldsymbol{D}_t\|} - \frac{f_{\boldsymbol{B}}(v)}{m \times n} \right|;$$

6) 求出上面这 $t$ 个数值中的最小值, 即为图像 $\boldsymbol{B}$ 的置乱程度。

## 3　仿真实验结果与分析

为了分析上文给出的置乱程度评价方法的性能, 在前面所说的 3类图像加密方法中各选择一种作为代表, 然后对这 3种加密方法的置乱程度进行仿真实验和分析。

### 3.1　加密方案的描述

3.1.1 基于 Arnold变换的图像置乱技术 (仅变换像素位置的图像加密 )

Arnold变换是一种纯粹的变换像素位置的加密方法, 它通过如式 (4) 所示的 Arnold变换实现图像置乱和加密

$$\begin{vmatrix} x' \\ y' \end{vmatrix} = \boldsymbol{A} \begin{vmatrix} x \\ y \end{vmatrix} \tag{4}$$

式中, $\boldsymbol{A} = \begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix}$ 是变换矩阵。

Arnold变换将数字图像中的点的位置移动, 使之重新排列。也就是将原来点 $(x, y)$ 处像素对应的灰度值移动至变换后的点 $(x', y')$ 处。经过多次置乱达到最佳效果。实验中, 选用 $\boldsymbol{A} = \begin{vmatrix} 1 & 1 \\ 1 & 2 \end{vmatrix}$ [16]。

3.1.2 基于 Logistic混沌序列的加密方法 (仅变换图像灰度值的图像加密 )

Logistic映射是一个源于人口统计的动力学系统, 其系统方程可写为如下形式:

$$x_{n+1} = 1 - \mu x_n^2 \tag{5}$$

式中, $x_n$ 为映射变量, $\mu$ 为系统参量, 它们的取值范围分别为 $-1 \leqslant x_n \leqslant 1$, $0 \leqslant \mu \leqslant 2$。

在该算法中, 把 Logistic映射的初始值 $x_0$、结构参数 $\mu$ 和过渡过程参数 $c$ 作为密钥, 根据密钥产生相应的混沌序列 $x_k$ 和 $y_k$, 然后, 由 $x_k$, $y_k$ 生成相应的符号矩阵 $\boldsymbol{S}$ 和灰度矩阵 $\boldsymbol{G}$, 实现对数字图像的加密。具体算法如下:

1) 由式 (5), 利用密钥 $x_0$ 产生相应的实值混沌序列 $x_k$ 和 $y_k$;

2) 利用生成的实值混沌序列 $x_k$, 通过定义阈值来产生符号序列:

$$\mathrm{sgn}(x_k) = \begin{cases} -1 & -1 \leqslant x_k < 0 \\ 1 & 0 \leqslant x_k \leqslant 1 \end{cases} \tag{6}$$

根据原始图像的大小按行或按列生成符号矩阵 $\boldsymbol{S}$;

3) 利用生成的实值混沌序列 $y_k$, 通过如下的变换生成序列 $g(y_k)$, 使得 $g(y_k) \in [0, L-1]$, 并根据原始图像的大小生成相应的灰度矩阵 $\boldsymbol{G}$,

$$g(y_k) = \mathrm{round}\left[ y_k \times \frac{L-1}{2} + \frac{L-1}{2} \right]; \tag{7}$$

式中, round( )为四舍五入函数。

4) 将原图像 $\boldsymbol{W}$ 和灰度矩阵 $\boldsymbol{G}$ 进行位异或, 得到 $\boldsymbol{WG}$ (该图像仅变换了灰度值 );

5) 将 $\boldsymbol{WG}$ 和符号矩阵 $\boldsymbol{S}$ 进行点乘, 得到加密图像 $\boldsymbol{WGS}$, 完成加密过程 (该图像也仅变换了灰度值 ) [17]。

由上面的加密过程可知, 该算法只是对图像像素的灰度值进行了变换, 而没有变换像素的位置。

3.1.3 基于混沌系统的图像加密算法 (像素位置及灰度值都发生变换的图像加密)

Logistic映射的另一种形式为

$$x_{n+1} = \mu x_n (1 - \mu x_n) \tag{8}$$

式中, $x_n$ 为映射变量, $\mu$为控制参数, 它们的取值范围分别为 $0 \leqslant x_n \leqslant 1$, $0 \leqslant \mu \leqslant 4$。

在该算法中, 利用密钥值 $x_0$, 由式 (5) 生成实数值混沌序列 $x_k$, 由式 (8) 生成实数值混沌序列 $y_k$, 然后由 $x_k$ 和 $y_k$ 分别生成全局置乱变换矩阵 $\boldsymbol{P}$ 和灰度变换矩阵 $\boldsymbol{G}$, 实现对数字图像的加密。具体算法如下:

1) 利用密钥值 $x_0$, 由式 (5) 生成实数值混沌序列 $x_k$, 由式 (8) 生成实数值混沌序列 $y_k$;

2) 将原图像 $\boldsymbol{W}$ 的像素进行分块, 原图像 $\boldsymbol{W}$ 的大小为 $m \times n$, 分块的大小为 $k \times l$。并按行序对块进行编号, 构成序号矩阵 $\boldsymbol{WB} = (wb_{ij})_{\frac{m}{k} \times \frac{n}{l}}$, $wb_{ij}$表示图像 $\boldsymbol{W}$ 中第 $i$行第 $j$列的像素块的编号, 即

$$wb_{ij} = j + (i-1) \times \frac{n}{l}, \text{ 且 } wb_{ij} \in \left| 1, 2, \cdots, \frac{m}{k} \times \frac{n}{l} \right|;$$

3) 由实数值混沌序列 $x_k$ 生成全局置乱变换矩阵 $\boldsymbol{P}$。

首先, 在实数值混沌序列 $x_k$ 中连续选取$\frac{m}{k} \times \frac{n}{l}$个值 $\{x_1, x_2, \cdots\}$, 把它们由小到大排成有序序列 $\{x'_1, x'_2, \cdots\}$, $\{x_1, x_2, \cdots\}$中的每个 $x_i$ 在有序序列 $\{x'_1, x'_2, \cdots\}$中的位置编号, 形成一个对应的位置编号序列为 $\{t_1, t_2, \cdots\}$, $t_i \in \left| 1, 2, \cdots, \frac{m}{k} \times \frac{n}{l} \right|$;

其次, 将位置编号序列$\left| t_1, t_2, \cdots \right|$按行或列排成大小为$\frac{m}{k} \times \frac{n}{l}$的全局置乱变换矩阵 $\boldsymbol{P}$;

4) 按全局置乱变换矩阵 $\boldsymbol{P}$ 中的序号对原图像中的像素分块重新排列, 得到原图像的置乱图像 $\boldsymbol{WP}$ (该图像仅对像素的位置进行了变换);

5) 由实数值混沌序列 $y_k$ 生成灰度变换矩阵 $\boldsymbol{G}$; 利用生成的实值混沌序列 $y_k$, 通过式 (9) 的变换生成序列 $g(y_k)$, 使得 $g(y_k) \in [0, L-1]$, 并根据原始图像的大小生成相应的灰度矩阵 $\boldsymbol{G}$,

$$g(y_k) = \text{round}(y_k \times (L-1)) \tag{9}$$

6) 将置乱图像 $\boldsymbol{WP}$ 的每个像素与灰度变换矩阵 $\boldsymbol{G}$ 中对应元素进行位异或运算, 得到最终加密图像 $\boldsymbol{WPG}$ (该图像在对像素位置进行变换的基础上又对像素的灰度值进行了变换)[18]。

由上面的加密过程可知, 该算法对图像像素的位置和灰度值都进行了变换。

## 3.2 仿真实验结果及其置乱程度分析

3.2.1 同一图像的不同置乱的效果

原图像选用大小为 256 × 256的 Lena图像, 如图 1(a)所示。对其进行 15次 Arnold变换后的效果依次如图 1(b) ~ 图 1(p)所示。对原图像用基于Logistic混沌序列的加密方法的步骤 4)、步骤 5)进行置乱后的结果如图 1(q)、图 1(r)所示。对原图像用基于混沌系统的图像加密算法的步骤 4)、步骤 6)进行置乱后的结果如图 1(s)、图 1(t)所示。图 1中各图的置乱程度 ISD如表 1所示。

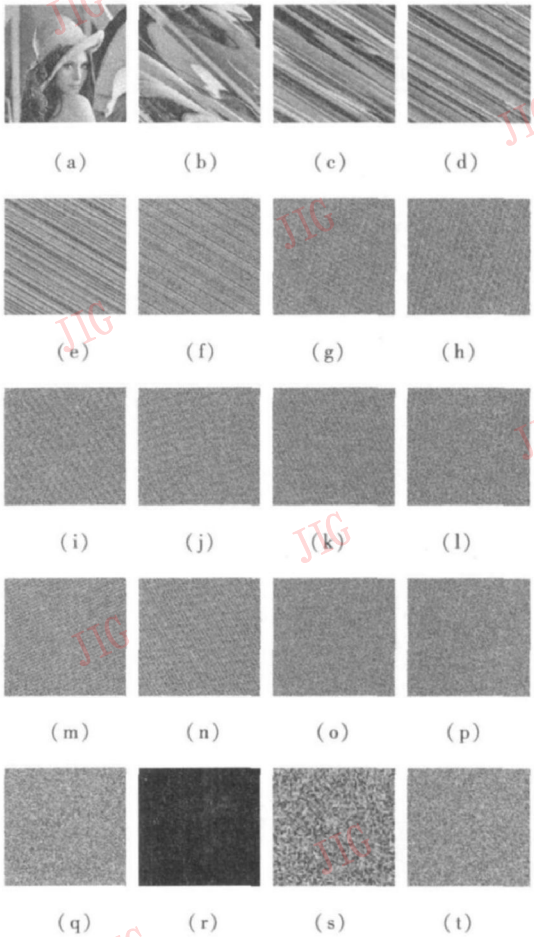


图 1 Lena 图像的 Arnold 置乱效果

Fig. 1 The scrambling effect of Arnold transformation about Lena

通过对图 1和表 1的比较, 可以知道, 对同一图像的不同置乱效果, 用本文所提出的方法得到的置乱程度与视觉的主观评价基本一致。视觉上感觉置乱效果越好的, 其置乱程度就越高; 视觉上差不多的, 得到的置乱程度的差别也不大; 另外, 视觉上感

表 1　图 1中各图的置乱程度

Tab 1　The scrambling degree of Fig 1

| 图像序号 | (a) | (b) | (c) | (d) | (e) |
|---|---|---|---|---|---|
| 各图的 ISD | 0.525 5 | 0.533 1 | 0.555 6 | 0.736 5 | 0.760 1 |
| 图像序号 | (f) | (g) | (h) | (i) | (j) |
| 各图的 ISD | 0.795 3 | 0.792 8 | 0.786 0 | 0.778 8 | 0.787 0 |
| 图像序号 | (k) | (l) | (m) | (n) | (o) |
| 各图的 ISD | 0.772 7 | 0.800 3 | 0.795 6 | 0.785 5 | 0.799 7 |
| 图像序号 | (p) | (q) | (r) | (s) | (t) |
| 各图的 ISD | 0.783 4 | 0.759 0 | 0.794 1 | 0.748 0 | 0.772 3 |

觉置乱效果差不多的, 也不会因为所使用的置乱方法的种类不同而有比较大的差别。这说明本文所提出的置乱程度计算方法能比较客观准确地描述图像的置乱效果, 而不会受到置乱方法类型的影响。因此, 它具有与视觉主观评价的一致性和对不同置乱方法的高泛化性。

3.2.2　不同图像的同一置乱的效果

选用 20幅大小为 256×256的不同图像, 如图 2所示。

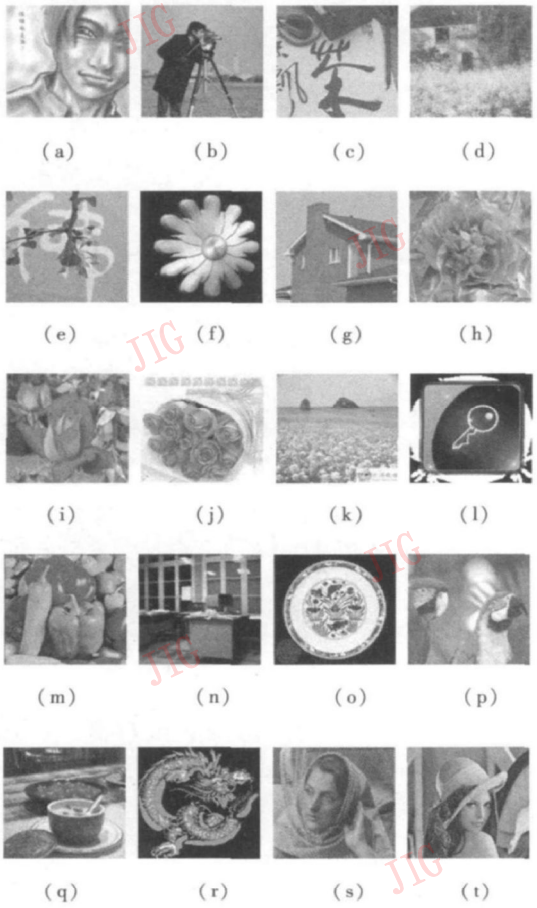


图 2　20 幅原图像

Fig. 2　Primary image

1)基于 Arnold变换的图像置乱技术的置乱效果

将图 2中的各图用基于 Arnold变换的图像置乱技术充分置乱后的效果, 依次如图 3 (a)~图 3(t)所示。$n$为达到充分置乱时的置乱次数。

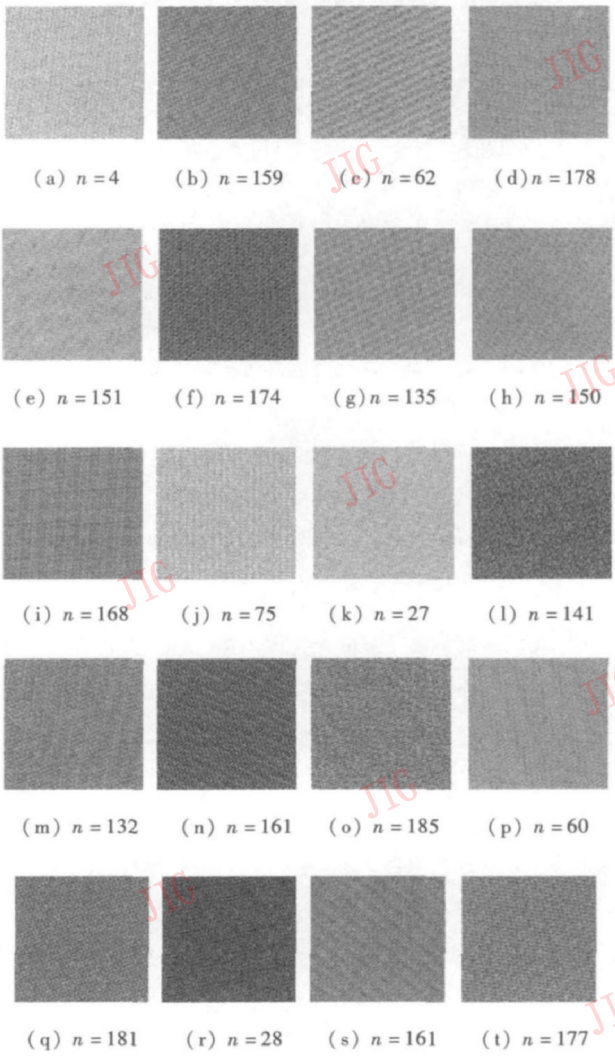


图 3　图 2 用基于 Arnold 变换的图像置乱技术充分置乱的效果

Fig. 3　The full scrambling effects of digital image scrambling technology besed on Arnold transformation about Fig. 2

2)基于 Logistic混沌序列的加密方法的置乱效果

将图 2中的各图用基于 Logistic混沌序列的加密方法置乱后的效果, 依次如图 4( a) ~ 图 4( t) 所示。

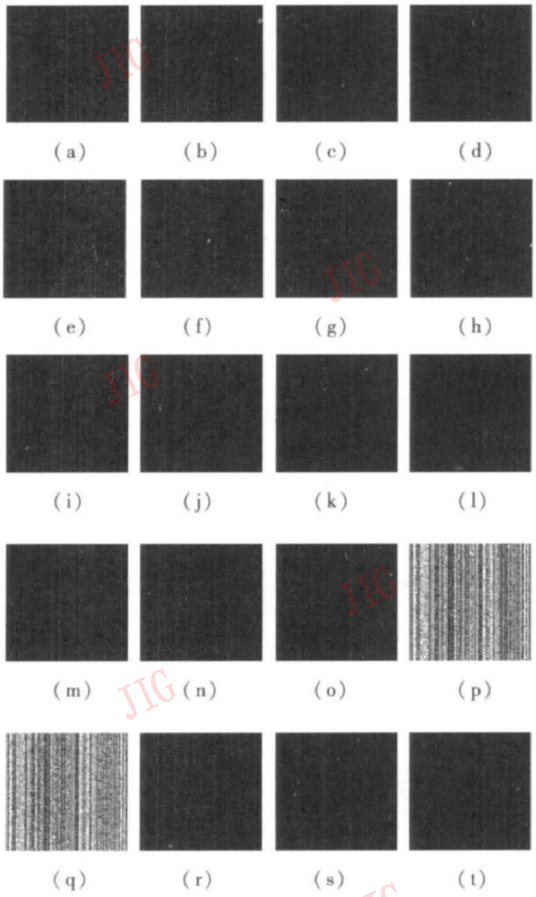


图 4 图 2用基于 Logistic 混沌序列的加密方法置乱后的效果

Fig. 4 The scrambling effects of digital image encryption besed on Logistic chaotic sequence about Fig. 2

3) 基于混沌系统的图像加密算法的置乱效果

将图 2中的各图用基于混沌系统的图像加密算法置乱后的效果, 依次如图 5( a) ~ 图 5( t)所示。

图 3~ 图 5各图的置乱程度如表 2所示。

图 3中各图的置乱程度曲线如图 6所示, 由此可知, 对于不同的图像来说, 用基于 Arnold变换的图像置乱技术置乱后的置乱程度基本在 0.825 7附近浮动, 且浮动的幅度都不大; 图 4中各图的置乱程度曲线如图 7所示, 由此可知, 对于不同的图像来说, 用基于 Logistic混沌序列的加密方法置乱后的置乱程度基本在 0.789 6附近浮动, 且浮动的幅度都不大; 图 5中各图的置乱程度曲线如图 8所示。由此可知, 对于不同的图像来说, 用基于混沌系统的图像加密算法置乱后的置乱程度基本在 0.783 3附近浮动, 且浮动的幅度都不大。这说明本文所给出的置乱程度的评价方法对各种类型的图像加密方法都有效, 对同一种图像加密方法来说, 只与这种加密方法的置乱性能有关, 置乱性能好置乱程度就高, 置乱性能差置乱程度就小, 并不会由于原图像的不同而有很大的改变。因此, 它具有与原图像无关性。

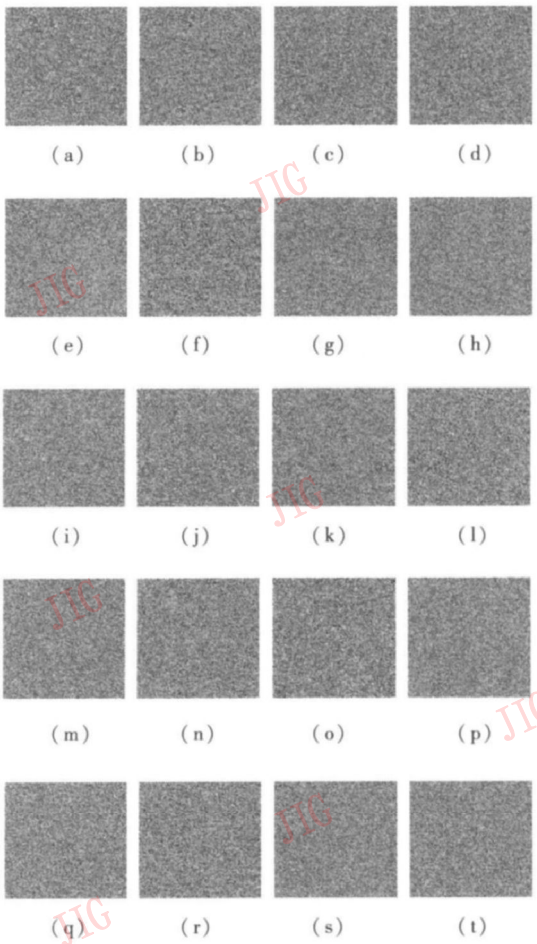


图 5 图 2用基于混沌系统的图像加密算法置乱后的效果

Fig. 5 The scrambling effects of image encryption algorithm besed on chaos system about Fig. 2

以上的仿真实验及分析结果表明, 本文提出的置乱程度评价方法能比较客观准确地描述图像的置乱效果。它具有如下的一些较为优良的特点:

1) 一致性: 它与视觉的主观评价基本一致;

2) 高泛化性: 它对仅变换像素位置的图像、仅变换像素灰度值的图像和像素位置及灰度值都发生变换的图像都适用;

3) 与原图像无关性: 对同一种图像加密方法来说, 该置乱程度不会由于原图像的不同而有很大的改变。

表 2　图 3~ 图 5中各图的置乱程度

Tab. 2　The scrambling degree of Fig. 3~ Fig. 5

| 图像序号 | (a) | (b) | (c) | (d) | (e) | (f) | (g) | (h) | (i) | (j) |
|---|---|---|---|---|---|---|---|---|---|---|
| 图 3各图的 ISD | 0.813 9 | 0.818 8 | 0.840 8 | 0.806 4 | 0.826 0 | 0.863 8 | 0.858 7 | 0.832 1 | 0.813 5 | 0.819 5 |
| 图 4各图的 ISD | 0.790 0 | 0.808 3 | 0.785 0 | 0.771 4 | 0.799 2 | 0.783 1 | 0.774 1 | 0.785 6 | 0.793 6 | 0.801 5 |
| 图 5各图的 ISD | 0.776 2 | 0.788 6 | 0.782 2 | 0.784 1 | 0.780 2 | 0.797 8 | 0.781 3 | 0.790 9 | 0.776 7 | 0.780 2 |
| 图像序号 | (k) | (l) | (m) | (n) | (o) | (p) | (q) | (r) | (s) | (t) |
| 图 3各图的 ISD | 0.830 8 | 0.825 1 | 0.810 8 | 0.818 8 | 0.838 8 | 0.818 8 | 0.805 2 | 0.856 4 | 0.807 4 | 0.807 6 |
| 图 4各图的 ISD | 0.781 1 | 0.827 2 | 0.783 4 | 0.788 6 | 0.790 0 | 0.788 4 | 0.777 5 | 0.788 7 | 0.781 6 | 0.794 1 |
| 图 5各图的 ISD | 0.779 5 | 0.780 5 | 0.787 3 | 0.782 0 | 0.786 4 | 0.785 3 | 0.777 4 | 0.790 6 | 0.786 8 | 0.772 3 |

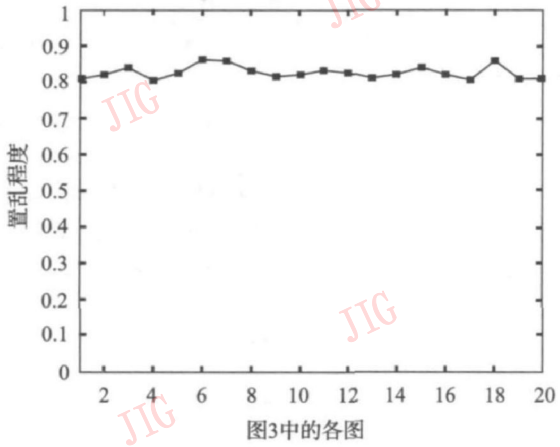


图 6　图 3 中各图的置乱程度曲线

Fig. 6　The scrambling degree of Fig. 3

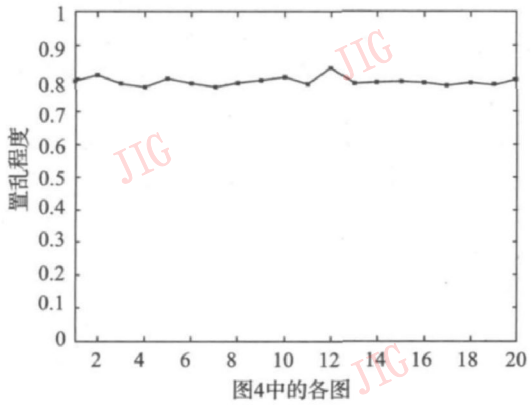


图 7　图 4 中各图的置乱程度曲线

Fig. 7　The scrambling degree of Fig. 4

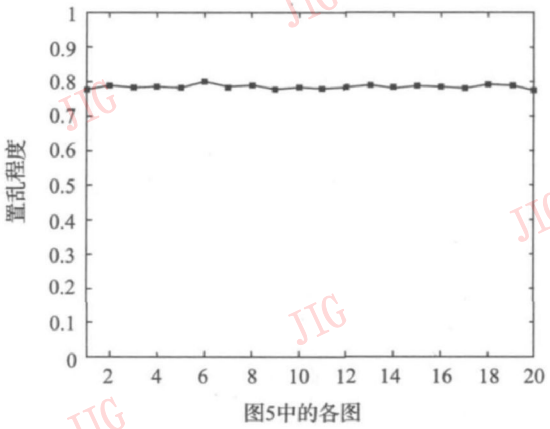


图 8　图 5中各图的置乱程度曲线

*Fig. 8　The scrambling degree of Fig. 5*

## 4　结　论

本文首先指出最佳 (理想 )置乱状态的本质特征是在它的任何区域 ***D*** 中每个灰度级 $v$ 出现的频数与在它本身中出现的频数相等, 从而定义出数字图像的最佳 (理想 )置乱效果, 然后, 以此为参照系, 利用在置乱图像的任何区域 ***D*** 中每个灰度级 $v$ 出现的频数与它在最佳 (理想 )置乱状态中出现的频数的差别提出了一种新的基于灰度级出现频数的数字图像置乱程度衡量方法, 可以证明该置乱程度具有两个很好的性质。同时, 仿真实验结果表明, 该置乱程度衡量方法与视觉的主观评价基本一致, 且对各种类型的图像加密方法都适用, 具有高泛化性; 对同一种图像加密方法来说, 该置乱程度衡量结果不会由于原图像的不同而有很大的改变, 它具有与原图像无关性。

## 参考文献 (References)

[1] Xu Jiang-feng　Yang You　Analysis of scrambling performance of encrypted image[J]. Computer Science, 2006, 33(3): 110-113. [徐江峰, 杨有. 加密图像置乱性能分析[J]. 计算机科学, 2006, 33(3): 110-113.]

[2] Shang Yan-hong　Zheng Zheng　Wang Zhirwei　Digital image scrambling technology and analysis of scrambling degree[J]. Journal of Tanshang Teachers college, 2006, 28(2): 80-82 [商

燕红, 郑铮, 王志巍. 数字图像置乱技术及置乱度分析[J]. 唐山师范学院学报, 2006, 28(2): 80-82.]

[3] Zhang Hua-xiong, Qiu Pei-liang. Application of shuffling techniques within watermarking[J]. Journal of Circuits and System, 2001, 6(3): 32-36. [张华熊, 仇佩亮. 置乱技术在数字水印中的应用[J]. 电路与系统学报, 2001, 6(3): 32-36.]

[4] Liu Xing-sha, Li Min, Fei Yao-ping. A digital image encryption algorithm of high security[J]. Microelectronics & Computer, 2007, 24(2): 21-27. [刘星沙, 李敏, 费耀平. 一种高安全性的数字图像加密算法[J]. 微电子学与计算机, 2007, 24(2): 21-27.]

[5] Qin Hong-lei, Hao Yan-lin, Sun Feng. Disign 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.]

[6] Wang Yi-ran, Zhu Wei-jun, Zhan Xin-sheng. Study on scrambling capability based on image encryption[J]. Computer Engineering and Design, 2006, 27(24): 4729-4731. [王迤冉, 朱维军, 詹新生. 基于图像加密的置乱性能分析研究[J]. 计算机工程与设计, 2006, 27(24): 4729-4731.]

[7] Lu Zeng-tai, Li Lou-lou. A new measurement for image encryption effect[J]. Acta Scientiarum Naturalium Universitatis Sunyatseni, 2005, 44(sup): 126-129. [卢振泰, 黎罗罗. 一种新的衡量图像置乱程度的方法[J]. 中山大学学报(自然科学版), 2005, 44(增刊): 126-129.]

[8] Zhang Jian, Yu Xiao-yang, Ren Hong-e, et al. Evaluation method of image scrambling degree[J]. Computer Engineering and Applications, 2007, 43(8): 134-136. [张健, 于晓洋, 任红娥等. 图像置乱程度的衡量方法[J]. 计算机工程与应用, 2007, 43(8): 134-136.]

[9] Sun Qiu-yan, Lei Zhong-kui, Ning Xuan-xi, et al. Application of canny operator in image scrambling degree evaluation[J]. Computer Engineering and Applications, 2007, 43(9): 40-44. [孙秋艳, 雷仲魁, 宁宣熙等. Canny算子在图像置乱程度评价中的应用[J]. 计算机工程与应用, 2007, 43(9): 40-44.]

[10] Chen Zhao-jiong, Xue Xiao-tan. An information hiding method based on sampling theory[J]. Journal of Fuzhou University (Natual Science), 2001, 29(4): 34-42. [陈昭炯, 薛小谭. 数字水印的一个采样型算法[J]. 福州大学学报(自然科学版), 2001, 29(4): 34-42.]

[11] Shang Yan-hong, Li Nan, Zou Jian-cheng. Fibonacci transformation and its applications in digital image watermark[J]. Acta Scientiarum Naturalium Universitatis Sunyatseni, 2004, 43(sup(2)): 148-151. [商燕红, 李南, 邹建成. Fibonacci变换及其在数字图像水印中的应用[J]. 中山大学学报(自然科学版), 2004, 43(增刊(2)): 148-151.]

[12] Chen Yan-mei, Zhang Sheng-yuan. Digital image scrambling degree evaluation method based on cross-entropy[J]. Journal of Image and Graphics, 2007, 12(6): 997-1001. [陈艳梅, 张胜元. 基于交叉熵的数字图像置乱程度评价方法[J]. 中国图象图形学报, 2007, 12(6): 997-1001.]

[13] Li Zhi-wei, Chen Yan-mei, Zhang Sheng-yuan. Digital image scrambling degree evaluation method based on SNR[J]. Journal of Xiamen University (Natual Science), 2006, 45(4): 484-487. [李志伟, 陈燕梅, 张胜元. 基于SNR的数字图像置乱程度评价方法[J]. 厦门大学学报(自然科学版), 2006, 45(4): 484-487.]

[14] Bai sen, Liao Xiao-feng. Image scrambling degree evaluation method based on Walsh Transformation[J]. Acta Scientiarum Naturalium Universitatis Sunyatseni, 2004, 43(sup(2)): 58-61. [柏森, 廖晓峰. 基于Walsh变换的图像置乱程度评价方法[J]. 中山大学学报(自然科学版), 2004, 43(增刊(2)): 58-61.]

[15] Gonzalez R C, Woods R E, Eddins S L. Digital Image Processing Using MATLAB [M]. Publishing House of Electronics Industry, 2004: 55. [冈萨雷斯等. 数字图像处理(MATLAB版)[M]. 电子工业出版社, 2004: 55.]

[16] Ding Wei, Yan Wei-qi, Qi Dong-xu. Digital image scrambling technology based on Arnold transformation[J]. Journal of Computer-aided Desigh & Computer Graphics, 2001, 13(4): 338-341. [丁玮, 阎伟齐, 齐东旭. 基于Arnold变换的数字图像置乱技术[J]. 计算机辅助设计与图形学学报, 2001, 13(4): 338-341.]

[17] Gu Qin-rong, Yao Min-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.]

[18] Sun Xin, Yi Kai-xiang, Sun You-xian. New image encryption algorithm based on chaos system[J]. Journal of Computer-aided Design & Computer Graphics, 2002, 14(2): 136-139. [孙鑫, 易开祥, 孙优贤. 基于混沌系统的图像加密算法[J]. 计算机辅助设计与图形学学报, 2002, 14(2): 136-139.]