Journal of Computer Applications
计算机应用,2013,33(9):2501 -2504
ISSN 1001-9081
CODEN JYIIDU
2013-09-01
http://www.joca.cn

文章编号:1001-9081(2013)09-2501-04
doi:10.11772/j.issn.1001-9081.2013.09.2501

基于位置交换的快速图像置乱

曹光辉[1,2*],贾　丹[1],张毅智[1]
(1.辽宁工业大学 电子与信息工程学院,辽宁 锦州 121001;　2.北京航空航天大学 计算机学院,北京 100191)
(*通信作者电子邮箱 caoguanghuineu@163.com)

摘　要:为了提高图像置乱算法的置乱效率,提出了一种基于帐篷映射的快速随机排列算法,并把这种方法应用到图像置乱领域,构建了基于混沌序列的快速图像置乱算法。该快速随机排列以位置交换为核心,通过应用概率的几何意义,把由帐篷映射产生的服从非均匀分布的混沌序列转化为服从均匀分布的随机序列,驱动图像元素位置交换完成随机排列。理论和实验结果表明:快速随机排列在效率上优于基于排序算法的随机排列,构建的快速图像置乱算法与传统基于混沌排序图像置乱算法相比,密钥空间更大,运行效率更高。

关键词:图像置乱;位置交换;均匀分布;帐篷映射;排序置乱
中图分类号:TP309　　**文献标志码**:A

Fast image scrambling based on position interchange

CAO Guanghui[1,2*], JIA Dan[1], ZHANG Yizhi[1]
(1. *School of Electronics and Information Engineering, Liaoning University of Technology, Jinzhou Liaoning* 121001, *China*;
2. *School of Computer Science and Technology, Beihang University, Beijing* 100191, *China*)

Abstract: In order to efficiently scramble image, based on skew tent map, a fast random permutation procedure was firstly presented, and then a fast image scrambling algorithm, based on the preceding procedure, was designed. The main idea behind the fast random permutation was position interchange. Its implementation process was, based on geometrical meaning of probability, non-uniform distribution chaos sequence generated by skew tent map was transformed into uniform random sequence, which then drove image element to interchange position. Theory and experiments results demonstrate that the fast random permutation has better efficiency then sorting-based random permutation, the proposed image scrambling method has larger key space and higher running efficiency than sorting-based image scrambling.

Key words: image scrambling; position interchange; uniform distribution; skew tent map; sorting permutation

0　引言

图像置乱算法最早由 Bourbakis 等[1]提出,其思想源于扫描语言的规范和发展,致力于二维数字图像的加密。随着网络和多媒体技术的发展,图像置乱算法不仅在图像加密领域取得巨大的进展[2-3],而且在信息隐藏[4-5]和数字水印[6-7]等领域也得到广泛应用。为了更好地满足这些领域的节能降耗需求,设计高效的图像置乱算法最为关键。

目前常见的图像置乱方法有:基于 Arnold 变换[8]、Gray 码与广义 Gray 码变换的置乱方法[9];基于分形几何 IFS 模型的置乱方法[10];基于 Hilbert 曲线[8]、FASS 曲线以及基于 Tangram 算法等置乱方法[10]。近年来,随着对混沌理论的研究深入,出现了以混沌序列排序为基础的图像置乱,如基于像素比特图像置乱[2]、基于组合矩阵图像置乱[11]、基于多混沌系统像素置乱彩色图像加密[12],以及完全置乱算法[3]等方法。因为这类算法具有安全性高、简单易用等优点,得到了广泛的应用,本文致力于提高这类算法的效率。这类算法的核心是利用混沌序列的不可预测性、随机性,对该数据序列进行排序,驱动图像的像素或比特完成行或列的随机排列。考虑到基于数据排序随机排列时间是 $O(n\ \mathrm{lb}\ n)$,而基于位置交换的随机排列时间是 $O(n)$,故本文提出基于位置交换的随机排列实现快速图像置乱。

1　基础元素及相关定义

1)帐篷映射(skew tent map)[13]。

方程　$$F_{a,b}(x)=\begin{cases}b+((1-b)/a)x, & 0\leqslant x<a\\(1-x)/(1-a), & a\leqslant x\leqslant 1\end{cases}$$

$$a\in(0,1),b\in[0,1] \tag{1}$$

在参数空间 $D_0=\{(a,b):b<1/(2-a)\cap(b<1-a)\}$ 时,整个 $x\in[0,1]$ 空间表现出混沌动力学行为。

2)帐篷映射概率密度[13]。

对于方程(1),具有如下密度函数:

$$h(x)=\begin{cases}h_1, & x\in(0,b)\\h_2, & x\in[b,F(b))\\\vdots\\h_{p-1}, & x\in[a,1)\end{cases} \tag{2}$$

其中:

$$h_i=\frac{1-b}{1-b-ab(p-1)}\left(1-\left(\frac{a}{1-b}\right)^i\right)$$

$$h_{p-1}=\frac{1-a-b}{(1-a)(1-b-ab(p-1))}$$

$i=1,2,\cdots,p-2$;p 为区间$[0,1]$划分数。

收稿日期:2013-03-22;**修回日期**:2013-04-18。
基金项目:国家自然科学基金资助项目(61073013);航空重点基金资助项目(2010ZA04001)。
作者简介:曹光辉(1974-),男,辽宁锦州人,讲师,博士研究生,CCF 会员,主要研究方向:混沌图像加密、算法设计;　贾丹(1972-),女,辽宁锦州人,副教授,主要研究方向:算法优化、信息安全;　张毅智(1963-),女,辽宁锦州人,副教授,主要研究方向:图像安全。

2 均匀分布随机变量的构造

快速图像置乱的核心是基于位置交换随机排列，该随机排列需要均匀分布随机数，尽管混沌能够生成很好的随机序列，但通常不具有均匀分布，下面给出基于帐篷映射生成均匀分布随机数方法。

2.1 构造[0,1]区间均匀分布的随机变量

2.1.1 基本原理

设两个随机变量 x 和 y，其概率密度函数分别为 $f(x)$ 和 $g(y)$，并且 $f(x)$ 和 $g(y)$ 分别在区域 (a, b) 和 (c, d) 内可积，令：

$$\int_a^x f(t)\,\mathrm{d}t = \int_c^y g(t)\,\mathrm{d}t \tag{3}$$

结合概率密度函数的实际意义，式(3)实际上就是对于 (a, b) 内任意一个 x，都有 (c, d) 内的一个 y，使得概率 $p(x)=p(y)$。这就给出了 x 与 y 的一个映射关系，即定义了一个定义域为 (a,b)，值域为 (c,d) 的关于随机变量 x,y 的单调函数 $y=f(x)$。

若 x 为服从(0, 1)均匀分布的随机变量，则式(3)可写为：

$$x = \int_c^y g(t)\,\mathrm{d}t \tag{4}$$

这就是由服从任意分布的随机变量 y 推导服从均匀分布随机变量的构造原理。

2.1.2 均匀分布随机变量的实现

基于以上原理，可得如下定理：

定理 1 设随机变量 x 服从概率密度函数：

$$h(x) = \begin{cases} h_1, & x \in (0,b) \\ h_2, & x \in [b,F(b)) \\ \vdots & \\ h_{p-1}, & x \in [a,1) \end{cases}$$

则随机变量

$$y = \varphi(x) = \begin{cases} \int_0^x h_1\,\mathrm{d}t, & x \in (0,b) \\ \int_0^b h_1\,dt + \int_b^x h_2\,\mathrm{d}t, & x \in [b,F(b)) \\ \vdots & \\ \int_0^b h_1\,\mathrm{d}t + \int_b^{F(b)} h_2\,\mathrm{d}t + \cdots + \int_a^x h_{p-1}\,\mathrm{d}t, & x \in [a,1) \end{cases} \tag{5}$$

为服从区间(0,1)上的均匀分布的随机变量。

证明 以 $x\in[b, F(b))$ 为例，由构造服从均匀分布的随机变量的原理，可得

$$y = \int_0^x h(t)\,\mathrm{d}t = \int_0^b h_1\,\mathrm{d}t + \int_b^x h_2\,\mathrm{d}t$$

其他类同。

由定理1，帐篷映射概率密度函数为式(2)，经由式(5)把帐篷映射生成的混沌序列转换为区间(0,1)上服从均匀分布的随机变量。本文把式(1)、(5)合称为修正帐篷映射，能够产生具有均匀分布的随机变量。

2.1.3 计算机模拟验证

图1~2是使用式(1)，参数为 $a=0.6$，$b=0.2708$，迭代50 000次，频率图区间间隔100得到的实验结果，图1给出的是原始帐篷映射生成混沌序列的频率直方图，图2为修正帐篷映射产生的具有均匀分布的随机序列频率直方图。计算机模拟结果显示，修正帐篷映射能够把非均匀分布序列转化为均匀分布随机序列。

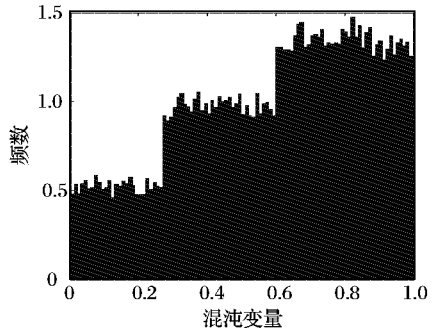


图1 帐篷映射频率图

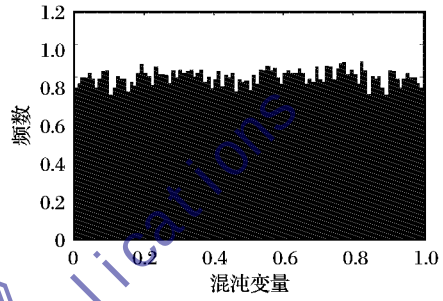


图2 修正帐篷映射频率图

2.2 构造[1,n]区间均匀分布的随机变量

定理 2 设 U 在区间(0,1)上服从均匀分布，则

$$X = \mathrm{Int}(nU) + 1 \tag{6}$$

以相等的概率取值 1, 2, …, n 中的任一个。

证明 因为 U 在区间(0, 1)上均匀分布，令

$$X = \begin{cases} 1, & 0 < U < \dfrac{1}{n} \\ 2, & \dfrac{1}{n} \leqslant U < \dfrac{2}{n} \\ \vdots & \\ n, & \dfrac{n-1}{n} \leqslant U < 1 \end{cases}$$

对于 $0<a<b<1$，由于 $p\{a \leqslant U < b\} = b-a$，故有，$p\{X=j\} = p\{(j-1)/n \leqslant U < j/n\} = 1/n$，即，当 $j-1 \leqslant nU < j$ 时，$X=j$，或等价地有 $X=\mathrm{Int}(nU)+1$。所以，X 的分布满足等概率取值 1, 2, …, n。 证毕。

3 基于位置交换图像置乱算法

基于帐篷映射位置交换随机排列算法是本文提出的快速图像置乱的核心，首先给出其具体实现。

3.1 基于帐篷映射位置交换随机排列算法

设数的初始顺序是 $P_1, P_2, \cdots, P_n$，其中 $P_i \in [1,n]$，则在位置 1, 2, …, n 中随机任选一个，把此位置上的数与位置 n 上的数互换。然后，从位置 1, 2, …, $n-1$ 中再任选一个，把此位置上的数与位置 $n-1$ 上的数互换，以此类推。数的随机排列是通过其位置的随机排列得到的。

因为 $X=\mathrm{Int}(nU)+1$ 等可能地在 1, 2, …, n 中任取一值，当随机变量 U 由修正 Skew tent map 生成时，基于位置的普通随机排列就形成本文提出的基于修正帐篷映射随机排列(Skew tent map Random Permutation based on Position Interchange, SRPPI)，伪代码如下：

```
A[1:n] ← 1...n
  for   j ←n to 2
        x ←F_{a,b}(x)
        y ← φ(x)
        val← fix(y ×j) +1;
        A(j) ↔ A(val);
  end
        yt(A,:) ←yt(1:m,:)
```

3.2　快速图像置乱算法

对于一幅任意大小的图像 I(灰度或彩色图像),以灰度图像为例,设其大小为 $M \times N$。

1)快速图像置乱算法步骤如下:

①给出生成随机序列的初始密钥,即产生随机序列初值或初始向量;

②依据 SRPPI 算法,生成 M 个元素的随机向量 $\boldsymbol{V}_1 = \{t_1, t_2, \cdots, t_M\}$;

③置乱图像所有行,得到 $\boldsymbol{R}' = \{R_1', R_2', \cdots, R_M'\}$,其中 $R_i' = R_{t_i}$;

④对于图像每一行,首先把每一像素转化为 8 比特的字符串,然后顺次连接形成一长串,其长度为 $L = N * 8$;

⑤依据 SRPPI 算法,生成 L 个元素的随机向量 $\boldsymbol{V}_2$;

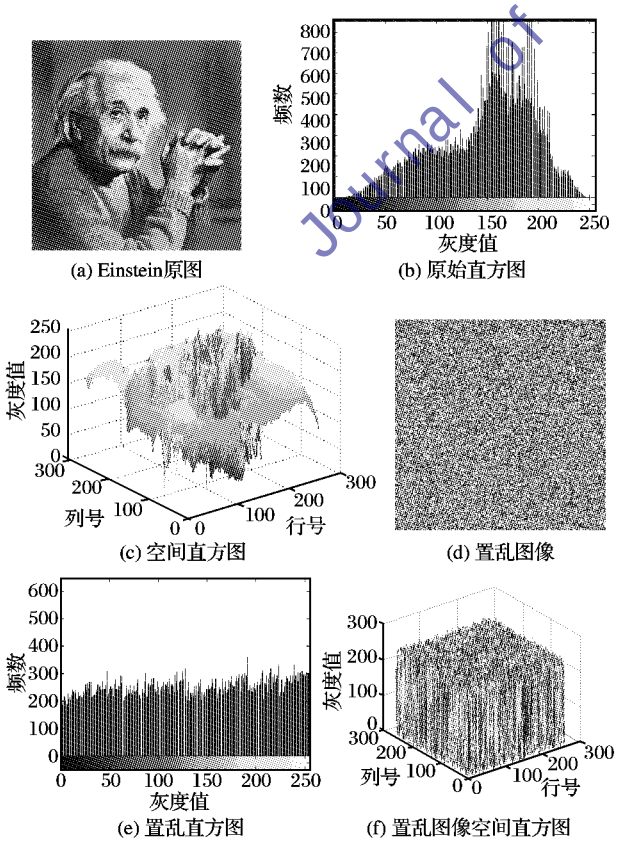
⑥以随机向量 $\boldsymbol{V}_2$ 中的元素为索引序重排图像每一行的长串,再以 8 比特为一组,合成每个像素,循环图像每一行直到结束,完成图像比特最小粒度全置乱。

2)逆置乱算法。

解密过程类似加密算法,除了④、⑥完成逆操作外。

4　实验结果

以 Einstein 图像为例,应用提出的快速图像置乱算法,实验结果见图 3,从普通直方图和空间直方图可见,快速图像置乱算法具有很好的安全性。



(a) Einstein原图　(b) 原始直方图　(c) 空间直方图　(d) 置乱图像　(e) 置乱直方图　(f) 置乱图像空间直方图

图 3　本文算法实验结果

5　与基于混沌排序类算法比较

Ye 算法[2]是基于混沌排序这一类算法的基础和典范,为了更好地论证本文提出算法的优越性,在如下几个重要方面与 Ye 算法进行比较。

5.1　密钥空间

一个安全可靠的图像置乱算法应拥有足够大的密钥空间。Ye 算法采用 Logistic 映射,密钥空间包括混沌方程初值和 1 个参数;快速图像置乱算法由于采用帐篷映射,密钥空间包括混沌方程初值和 2 个参数。因此,本文算法密钥空间大于 Ye 算法密钥空间。

5.2　相邻像素点的相关性分析

为了了解图像置乱后相邻像素的相关性,垂直(水平、对角)相邻像素的相关性被考察。表 1 给出了原始图像经过 Ye 算法或快速图像置乱算法置乱后,置乱图像相邻像素间的平均相关系数。作为参考数据,本文也给出了由随机数组成二维矩阵形成的 Rand 图像,并计算了它的相关系数。

像素相关系数 r_{xy} 计算方法如下:

以水平相关性为例,从图像中随机选择 1000 对两个水平邻接像素,选择 1000 次,运用下面公式计算每一对相邻像素的平均相关系数。

$$cov(x,y) = E(x - E(x))(y - E(y))$$

$$r_{xy} = \frac{cov(x,y)}{\sqrt{D(x)}\sqrt{D(y)}}$$

$$r = mean(r_{xy})$$

其中 x、y 代表图像中两个邻接像素灰度值,在数值计算中下面的离散公式被使用:

$$E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i$$

$$D(x) = \frac{1}{N}\sum_{i=1}^{N} (x_i - E(x))^2$$

$$cov(x,y) = \frac{1}{N}\sum_{i=1}^{N} (x_i - E(x))(y_i - E(y))$$

从表 1 可知,快速图像置乱算法、Ye 算法具有和 Rand 图像同样数量级的相关性,相关系数接近 0。这说明攻击者很难通过统计攻击方法破解快速图像置乱算法。

表 1　相邻像素间的平均相关系数

相关性	原始图像	Rand 图像	快速图像置乱	Ye 算法[2]
水平	0.9058	0.0161	-0.0580	0.0234
垂直	0.9322	0.0122	0.0060	-0.0474
对角	0.8783	-0.0141	-0.0169	0.0218

5.3　运行时间分析

为了证明快速图像置乱算法的高效性,本文应用估值法和实测法进行论证。

1)估值法。从伪代码可见,基于位置交换的随机排列运行时间是 $O(n)$,而传统基于排序的随机排列是 $O(n \text{ lb } n)$。因此,基于排序随机排列运行时间是基于位置交换随机排列运行时间的 lb n 倍。

2)实测法。计算机硬件配置:Intel Core 2 Quad CPU 2.66 GHz,内存 3.37 GB;应用软件:Matlab 7.0。考虑到 Matlab 函数库中的 sort( ) 函数已经编译和优化,为了公平比较,实验用 Matlab 语言实现了适用于结构体类型的quicksort( ) 函数,用于基于排序随机排列。表 2 给出的是两种随机排列

算法实测时间,表 3 给出的是两种图像置乱算法实测时间。

表 2 数据置乱时间测试

数据序列长度	排序随机排列/s	位置交换随机排列/s	排序和位置交换时间比	理论估值比 lb n
100	0.015	0	—	6.500
1000	0.157	0.016	9.800	9.868
10000	3.969	0.593	6.600	13.150
50000	234.500	16.031	14.628	15.450
100000	955.515	68.922	13.800	16.440

表 3 图像置乱时间测试

图像大小/像素	置乱时间/s		置乱比
	Ye 算法	快速图像置乱	
64×64	13.813	9.406	1.468
128×128	58.610	38.032	1.541
256×256	239.703	150.500	1.583

从上述结果可见,理论估值和实测值有一定区别,实测值受计算机硬件、软件以及当前计算机内存实际分配、运行进程等众多条件影响。但从总体来看,以基于位置交换随机排列为图像置乱核心算法,很大程度减少了置乱算法的运行时间,提高了算法的运行效率。

6 结语

本文采用基于位置交换的数据随机排列作为图像置乱的核心算法,解决了混沌排序图像置乱这一类算法中的核心模块——基于排序变换的随机数据排列,运行时间长的问题,实现了图像的快速置乱。该算法安全性高,运行速度快,通过减少置乱算法运行时间,提高了应用程序的运行效率,实现了节能降耗,符合绿色时代的主题。

利用混沌方程产生均匀分布随机序列是基于位置随机排列的关键,本文目前仅实现了利用已知密度函数的混沌方程产生均匀分布随机数的方法,如何利用未知密度函数的混沌方程生成均匀分布随机数是进一步研究的方向。

参考文献:

[1] BOURBAKIS N, ALEXOPOULOS C. Picture data encryption using scan patterns[J]. Pattern Recognition, 1992, 25(6): 567 – 581.

[2] YE G D. Scrambling encryption algorithm of pixel bit based on chaos map [J]. Pattern Recognition Letters, 2010, 31(5): 347 – 354.

[3] WANG X Y, TENG L, QIN X. A novel color image encryption algorithm based on chaos [J]. Signal Processing, 2012, 92(4): 1101 – 1108.

[4] LIN K T. Information hiding based on binary encoding methods and pixel scrambling techniques[J]. Applied Optics, 2012, 49(2): 220 – 228.

[5] RAHMAN S M M, HOSSAIN M A, MOUFTA H, *et al*. Chaos-cryptography based privacy preservation technique for video surveillance[J]. Multimedia Systems, 2012, 18(2): 145 – 155.

[6] HAMIDREZA S, MARZIEH A. A robust spread spectrum based image watermarking in ridgelet domain[J]. AEU — International Journal of Electronics and Communications, 2012, 66(5): 364 – 371.

[7] SLEIT A, ABUSHARKH A, ETOOM R. An enhanced semi-blind DWT-SVD-based watermarking technique for digital images[J]. Imaging Science Journal, 2012, 60(1): 29 – 38.

[8] 丁伟, 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): 839 – 943.

[9] 邹建成, 李国富, 齐东旭. 广义 Gray 码及其在数字图像置乱中的应用[J]. 高等应用数学学报: A 辑, 2002, 17(3): 363 – 373.

[10] 齐东旭. 矩阵变换及其在图像信息隐藏中的应用研究[J]. 北京工业大学学报, 1999, 11(1): 24 – 28.

[11] JI W Y, HYOUNGSGICK K. An image encryption scheme with a pseudorandom permutation based on chaotic maps[J]. Communications in Nonlinear Science and Numerical Simulation, 2010, 15(12): 3998 – 4006.

[12] HUANG C K, NIEN H H. Multi chaotic systems based pixel shuffle for image encryption [J]. Optics Communications, 2009, 282(11): 2123 – 2127.

[13] BILLINGS L, BOLLT E M. Probability density functions of some skew tent maps[J]. Chaos, Solitons & Fractals, 2001, 12(2): 365 – 376.

(上接第 2492 页)

类型众多,如何利用信息熵理论来清理其他类型的异常数据是将要开展的工作。

参考文献:

[1] 周傲英, 金澈清, 王国仁, 等. 不确定性数据管理技术研究综述[J]. 计算机学报, 2009, 32(1): 1 – 16.

[2] PRAGATI P, PRATEEKSHA P, MINU C. Uncertain data algorithms and applications [J]. International Journal of Advanced Research in Computer Science and Software Engineering, 2012, 2(7): 274 – 280.

[3] 李建中, 于戈, 周傲英. 不确定性数据管理的要求与挑战[J]. 中国计算机学会通讯, 2009, 5(4): 6 – 14.

[4] CHENG R. Querying and cleaning uncertain data[C]// Proceedings of Quality of Context. Berlin: Springer, 2009: 41 – 52.

[5] OMAR B, ANISH D S, ALON H, *et al*. ULDBs: databases with uncertainty and lineage [C]// Proceedings of the 32nd International Conference on Very Large Data Bases. San Francisco: Morgan Kaufmann Publishers, 2006: 953 – 964.

[6] CHEN H Q, KU W S, WANG H X. Cleansing uncertain databases leveraging aggregate constraints[C]// Proceedings of the 26th International Conference on Data Engineering. Washington, DC: IEEE Computer Society, 2010: 128 – 135.

[7] ERHARD R, HONG H D. Data cleaning: problems and current approaches [J]. IEEE Data Engineering Bulletin, 2000, 23(4): 3 – 13.

[8] GEORGE B, IIYAS I F, LUKASZ G. Sampling the repairs of functional dependency violations under hard constraints [J]. Proceedings of the VLDB Endowment, 2010, 3(1): 197 – 207.

[9] GRAHAM C, DIVESH S, ENTONG S, *et al*. Aggregate query answering on possibilistic data with cardinality constraints[C]// Proceedings of the 28th International Conference on Data Engineering. Washington, DC: IEEE Computer Society, 2012: 258 – 269.

[10] HEIKO M, JOHANN - CHRISTOPH F. Problems, methods, and challenges in comprehensive data cleansing[R]. Berlin: Humboldt University of Berlin, 2003.

[11] 刘惟一, 李维华, 岳昆. 智能数据分析[M]. 北京: 科学出版社, 2007: 9 – 16.

[12] JULIA S, SUSAN D, TOVA M, *et al*. Deriving probabilistic databases with inference ensembles[C]// Proceedings of the 27th International Conference on Data Engineering. Washington, DC: IEEE Computer Society, 2011: 303 – 314.