基于魔方的混沌图像置乱算法①

何创毅　陈乐庚　王志达 (桂林电子科技大学 计算机与控制学院 广西 桂林 541004)

摘　要： 提出了一种新的基于魔方的混沌图像置乱算法。该算法基于魔方的循环移位的思想，把二维图像数据矩阵中的行或列中的若干个连续的像素值看作是一个二进制串，通过对该串的移位实现图像的置乱。而移位的次数则由混沌映射 Logistic 所产生的序列控制。实验仿真表明，该加密算法具有良好的加密效果，能有效地抵御各种外部攻击。

关键词： 图像置乱；图像加密；循环移位；混沌；魔方

Chaotic Image Scrambling Algorithm Based on Magic Cube

HE Chuang-Yi, CHEN Le-Geng, WANG Zhi-Da

(Department of Computer and Control, Guilin University of Electronic Technology, Guilin 541004, China)

Abstract: In this paper, a new algorithm is proposed for image scrambling based on magic cube and chaotic. The proposed algorithm based on the idea of circulate shift regards some consecutive pixels in a row or a column in the image matrix as a group of bianry and scrambles the image by shifting these groups of bianry. And the number of shifting is controlled by the chaotic sequence generated by Logistic-map. Simulation shows that the proposed algorithm has good scrambling performance and can resist all kinds of attacks effectively.

Keywords: image scrambling; image encryption; circulate shift; chaotic; magic cube

数字图像作为多媒体信息的一种，是一类具备独有的感官效果和内容丰富的信息载体。在信息化时代中，数字图像逐渐成为人们网络信息交流的一种重要手段，应用十分广泛。它们给社会带来了方便的同时，也带来了安全隐患，如信息的泄露、篡改和破坏等。特别是在现有的脆弱的公共传输信道上，如何对一些敏感数据实施保密是数字图像安全一个研究热点。随着研究的深入，各种各样的技术层出不穷。

1　引言

图像置乱是图像加密的一种重要手段。常见的置乱技术有以下几种：基于 Arnold 变换、正交拉丁方、骑士巡游置乱变换等。虽然这些方法都具有其自身的优点，但是对图像的要求严格，如大小有限制。同时这些置乱方法只是对像素的位置进行置乱，并没有涉及过多的变化。基于以上种种原因，图像的加密效果不够理想，算法安全强度不高，容易被破解。

基于混沌的图像置乱技术[1,2]是近年来才发展起来的一种加密技术。混沌信号具有的非周期性、连续宽带频谱、类似噪声的特性，使得它具有天然的隐蔽性；对初始条件和微小扰动的高度敏感性，又使混沌信号具有长期不可预测性。混沌系统所具有的这些优良的密码学特性，为图像置乱技术的发展提供了基础。由邓绍江等人提出的一种基于混沌的图像置乱算法[3] 提出了通过混沌序列值构造对换规则矩阵，由该矩阵控制二维图像的像素进行对换置乱。而 Gilani 等人则提出了一种基于块的增强型的置乱算法[4]，通过对图像的分块，再对块进行两轮的翻转，从而实现图像的置乱。由 Sabery 提出的改进算法[5]中，则通过一个长度为 80 个二进制位的密钥控制混沌序列值的产生，扩大了整个密钥空间，有效的增强了算法安全性。本文提出了一种新的结合混沌映射、基于魔方的图像置乱算法。实验表明，该

① 收稿时间:2009-08-12;收到修改稿时间:2009-09-19

算法具有优良的特性。

2　基于魔方的混沌图像置乱算法

2.1 混沌映射 Logistic

Logistic 映射来源于著名的统计学模型，是目前广泛应用的一种混沌动力系统，其动态的数学模型可表示为：

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

其中x_n是系统变量，而λ为系统参数，$x_n \in (0,1)$, $n \in N$,当时$3.569945 < \lambda \le 4$，映射(1)处于混沌状态，(1)式迭代得到在$(0,1)$上的伪随机序列$\{x_k\}_{k=0}^{\infty}$。图 1 是在映射参数$\lambda = 3.889$,初值$x_0 = 0.485$时(1)式所产生的 500 个伪随机序列数在区间的分布图。其中 x 轴表示 n，y 轴表示x_n。

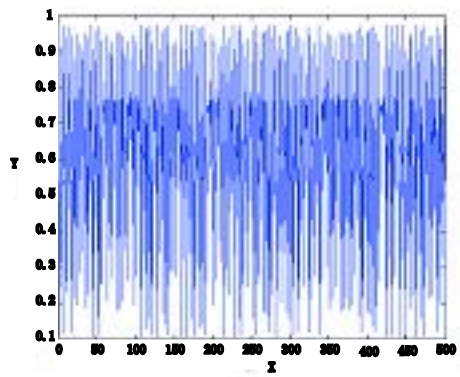


图 1　参数 λ=3.889，初值 x0=0.485 的 Logistic 映射序列分布

2.2 基于魔方的混沌图像置乱算法

基于置乱技术的图像加密技术总体上来说可以等效为对图像矩阵进行有限步的初等矩阵变换，从而改变像素在图像中的位置。但初等矩阵变换是一线性变换，其保密性不高。本文提出的基于魔方的混沌图像置乱算法引入了循环移位的思想，对二维图像中的像素值的二进制位实行“旋转”，改变其像素值，从而实现图像的置乱。

算法的设计思想：该算法主要是基于魔方的循环移位思想。把二维图像的每行和每列都看作是若干位的二进制串，通过串的左移或右移，实现像素值的置乱。通过混沌系统 Logistic 所产生的序列，置乱过程将其离散化后生成置乱矩阵。通过该置乱矩阵控制移动的次数。具体算法步骤如下：

2.2.1 加密算法

该算法可对任意 m × n 的灰度图像进行加密处理，只要对图像进行适当的填充，将其变成 k×k 的图像即可，其中 k=max(m,n)。在这里，为求简便处理，假定要对一幅 m × m 的灰度图像进行置乱加密，图像的二维数据矩阵为 T。

加密过程：

1) 分析原图，取得图像的信息，特别是图像的大小。

2) 生成 2m 个混沌序列值，以行为主序，顺序扫描各行的像素值。

3) 把每行的像素值看作是一个二进制串，前 m 个序列值决定了各行的二进制串的循环移位次数。依次对 m 行进行循环移位。

4) 由步骤 3 得行处理完毕的二维矩阵 T1，将矩阵进行转置，得到新的矩阵 T2。

5) 用后 m 个序列值对 T2 各行进行循环移位，处理完毕得到新矩阵 T3。

6) 将 T3 转置得到矩阵 T4，T4 就是 T 置乱后所得的密文图像。

以上是对图像置乱的一个迭代过程，若要得到更好的置乱效果，不妨将图像进行多次迭代。

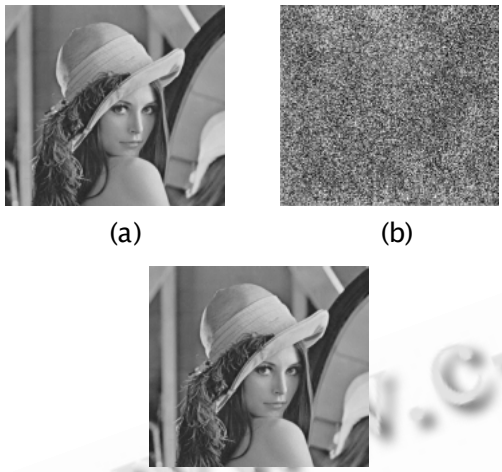
2.2.2 解密算法

加密过程的顺序是先行后列，那么解密过程则是先列后行。为对密文图像 T4 进行解密，先对密文矩阵的二维数据矩阵 T4 进行转置，得到 T5。用后 m 个序列值对 T5 的 m 行逆向循环移位，得到 T6。将 T6 进行转置得到 T7，再用前 m 个序列值对 T7 的 m 行逆向循环移位后，得到 T8，再将 T8 转置得到 T9。T9 就是原图的二维数据矩阵。

3　实验仿真

鉴于仿真工具 MATLAB 对矩阵数据的处理较为直观、简单。所以该实验采用 MATLAB 平台进行实验仿真，采用模块设计的方法实现加密算法和解密算法。在该实验中，用于图像置乱的灰度图像大小取为 256×256 pixels。在 Logistic 混沌映射中，取密钥初值如图 1 所示。用本文的循环移位算法对图像进行置乱加密，所得到的图像均是一种类似于噪声的均匀图像，且完全不能

从图像中得到原图的任何信息，具有良好的加密效果。解密过程则刚好是加密的逆过程，在得到正确的密钥前提下，可以重构混沌，用所得的混沌序列对已加密图像执行解密算法，便能得到解密图像。如图 2 所示：



(a)　(b)　(c)

图 2　(a) 原图　(b) 经过置乱加密后的图像　(c) 经过解密后的图像

4　算法安全性分析

4.1 密钥空间

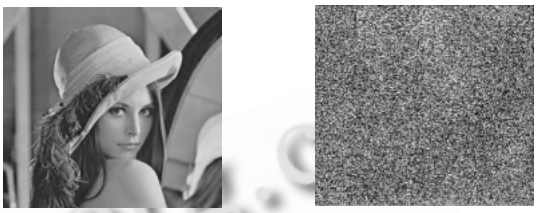
一个安全可靠的加密算法理应拥有足够大的密钥空间。而对于基于混沌映射的加密算法，参数(包括初始值)往往用作密钥，因此控制参数多就意味着密钥多，参数空间大才能保证密钥空间大。本文提出的算法中，假设混沌映射的参数的选择空间为 M_1,初始条件的选择空间为 M_2。我们设定还有这么一个参数 M_3。如果我们在所产生的映射序列中选取 10^4 个以后的若干个序列值，那么在这里 $M_3=10^4$。所以这个算法的密钥空间 M 可用以下的公式[6]计算：

$$M= M_1 * M_2 * M_3$$

我们选择 $M_1=10^{10}$，$M_2=10^{14}$，$M_3=10^4$，则 $M=10^{28}$，在这样的一个密钥空间中，采用穷举法进行攻击，在一些实时性要求较高的保密通信系统中，即使找到了加密密钥，由于其滞后的时间太多，已经失去了攻击的价值。可见，密钥的空间已经足够大了。

4.2 密钥敏感性分析

研究表明，若一个加密系统具有很强的密钥敏感性，可以有效的抵抗差分攻击。在对加密图像进行解密的过程中，其他条件均不变，只是初始值(密钥)发生极其细微的变化。例如 $x_0=0.4850000000001$，解密后的图像则不能恢复到原图像，且与原图像差异巨大，依然是类似于噪声的均匀图像，完全不能获得原图像的几乎任何信息。实验结果表明，加密图像对密钥具有高度的敏感依赖性，可以抵抗差分攻击。



(a)　(b)

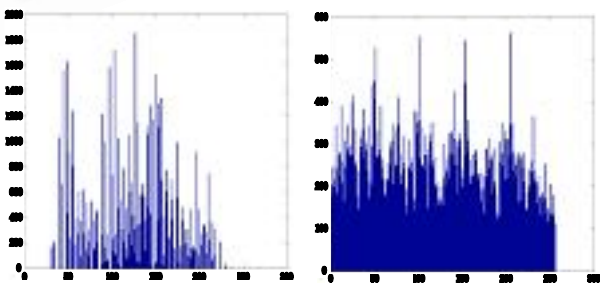
图 3　(a)用初值 $x_0=0.485$ 解密所得的图像(b) 用初值 $x_0=0.4850000000001$ 解密所得的图像

4.3 统计分析

为了验证算法在面对统计攻击时的稳定性，给出了原图和经过加密后的图像的直方图。实验表明两幅图像没有任何的相关性。同时对原图和经过加密后的图像的相邻像素的相关系数进行了分析。

4.3.1 直方图

从原图像的直方图(图 4(a))和经过加密的图像的直方图(图 4(b))，我们可以看出，图像在加密前后的直方图差别很大，这就意味着原图中的绝大部分的像素的值都得到了改变，同时算法具有良好的置乱特性。密文图像的直方图呈均匀分布，它掩盖了加密前的分布规律，从而增加了破译的难度。



(a)　(b)

图 4　(a)原图像的直方图 (b)加密后的图像的直方图

4.3.2 相关系数

原图中的相邻像素具有很大的相关性。一个有效的加密算法必须要降低相邻像素的相关性，才能更好

的抵御统计攻击。像素的相关性可按如下相关系数定义进行计算：

$$R_{xy}=\frac{|\mathrm{cov}(x,y)|}{\sqrt{D(x)}\sqrt{D(y)}} \tag{2}$$

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

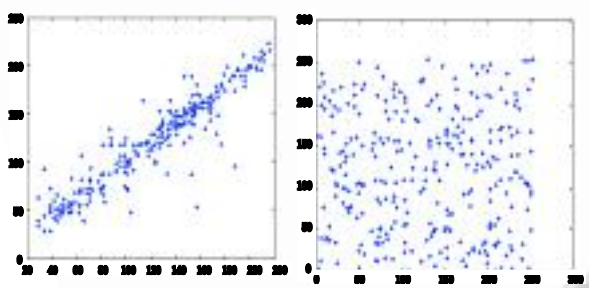
$$=\frac{1}{N}\sum_{k=1}^{N}(x_k-E(x))(y_k-E(y)) \tag{3}$$

$$E(x)=\frac{1}{N}\sum_{k=1}^{N}x_k \tag{4}$$

$$D(x)=\frac{1}{N}\sum_{k=1}^{N}(x_k-E(x))^2 \tag{5}$$

x 和 y 分别为相邻像素的灰度值

在测试图像水平方向、垂直方向和对角线方向的像素相关性时，分别在原图像和加密后的图像中随机选取300对的相邻像素，并进行了相关性系数的计算。图 5(a)给出了原图的水平方向相邻像素的相关关系，而图 5(b)则给出了加密后的图像的水平方向相邻像素的相关关系。



(a) (b)

图 5 (a) 原图的水平方向相邻像素的相关关系 (b) 加密后的图像的水平方向相邻像素的相关关系

对比图 5 中的(a) 和(b)，不难发现原图中的相邻像素呈现出明显的相关性；而加密后的图像的相邻像素的相关性则呈现非常随机的对应关系。表 1 列出了图像加密前后各个方向的相邻像素的相关系数：

表 1 原图和加密后的图像的相邻像素的相关系

方向	原始图像	加密后图像
水平方向相邻像素的相邻系数	0.9422	0.0194
垂直方向相邻像素的相邻系数	0.9712	0.0177
对角方向相邻像素的相邻系数	0.9206	0.0578

由图 5 中的(a) 和(b)以及表 1 的结果我们可以得出结论，原图的相邻像素具有非常强的线性相关性，而加密后的图像的相邻像素不再具有线性相关性，其相邻像素的灰度值的对应关系具有明显的随机性。相关系数相对于原图有了大幅的下降。由此可见该加密算法有效的降低像素的相关性。

5 结论

该算法是把二维图像的行或列若干像素的值看作是一组二进制串。通过循环移位，像素值的每个二进制位在理论上都有可能出现在整幅图像的任何位置，实现全方位的置乱。实验结果表明，该算法具有很好的加密效果，能有效抵御各种外部攻击。本文所提出的算法是基于栅格图像的。目前，针对矢量图形数据的信息安全技术的研究工作还比较少。随着制造业的发展和工程图纸日益应用广泛，矢量图形数据的安全技术将逐渐得到了关注。如何把当前多媒体的一些成熟的安全技术应用到矢量图形数据中成为研究的重点，本文将继续关注这方面的发展。

参考文献

1 李昌刚,韩正之,张浩然.图像加密技术综述.计算机研究与发展, 2002,39(10):1317－1324.

2 刘金梅,丘水生.混沌系统在密码学中的应用现状及展望.计算机工程与应用, 2008,44(14):5－12.

3 邓绍江,张岱固,濮忠良.一种基于混沌的图像置乱算法.计算机科学, 2008,35(8):238－240.

4 Gilani SAN, Bangash MA. Enhanced Block Based color Image Encryption technique with confusion. Multitopic Conference, INMIC 2008. IEEE International 23-24 Dec. 2008. 200－206.

5 Sabery MK, Yaghoobi MA New Approach for Image Encryption Using Chaotic Logistic Map. Advanced Computer Theory and Engineering, 2008. ICACTE'08. International Conference on 20-22 Dec. 2008. 585－590.

6 Fu C, Zhu ZL. A Chaotic Image Encryption Scheme Based on Circular Bit Shift Method. Young Computer Scientists,2008.ICYCS 2008. The 9th International Conference for 18-21 Nov. 2008. 3057－3061.