文章编号:1001 - 9081(2009)10 - 2681 - 03

基于 Logistic 混沌序列和位交换的图像置乱算法

袁 玲[1,2],康宝生[1]
(1. 西北大学 信息科学与技术学院, 西安 710127; 2. 喀什师范学院 信息工程技术系,新疆 喀什 844000)
(Julyyuan@163.com)

摘 要:在分析传统迭代型图像置乱方法不足的基础上,提出一种新的基于混沌序列和位交换的图像置乱算法。算法根据各像素点的位置,采用不同的 Logistic 混沌序列和像素值的二进制序列进行异或操作改变图像像素值,并利用图像本身的自相关性进行加密,不需迭代,经过一次运算即可得到加密图像。仿真实验结果表明,该算法可有效地实现灰度和彩色图像置乱,并能较好地抵抗椒盐和裁剪攻击,在效率上也优于迭代型置乱方法。

关键词:图像置乱;位交换;混沌序列;密钥;迭代
中图分类号: TP309 **文献标志码**:A

Image scrambling algorithm based on Logistic chaotic sequence and bit exchange

YUAN Ling[1,2], KANG Bao-sheng[1]
(1. *School of Information Science and Technology, Northwest University, Xi'an Shaanxi* 710127, *China*;
2. *Department of Information Engineering and Technology, Kashgar Teachers College, Kashi Xinjiang* 844000, *China*)

Abstract: Based on the analysis of the defect of the traditional iterated image scrambling, a new image scrambling algorithm was proposed based on chaotic sequence and bit exchange. According to the pixel location, the algorithm changed the image pixel values by using XOR operation in different Logistic chaotic sequence and the binary sequences of pixel value. Without iteration, the algorithm used the self-relativity of image to encrypt image. Experimental data and results show that the algorithm can achieve more effective image scrambling compared with the traditional algorithm. The algorithm has good performance in resisting the salt pepper and cutting attack. Compared with the iterative type's scrambling methods, it has higher efficiency too.

Key words: image scrambling; bit exchange; chaotic sequence; secret key; iteration

0 引言

信息技术的迅速发展使数字媒体内容可以方便快捷地在互联网发布和传输,同时也带来了许多安全隐患。由于信息容易被非法访问、复制和传播,在多媒体应用中常需要对信息进行保护。对多媒体信息的保护主要采用两种技术:对内容进行加密[1]和在数字媒体中嵌入水印[2]。图像置乱属于第一种技术,通过"打乱"像素位置或颜色,使原始图像貌似杂乱无章,达到加密的目的。图像置乱也可用于信息隐藏的预处理。

数字图像置乱加密技术目前主要有三种:1)基于图像像素点坐标的空间域和频域变换加密;2)基于图像色度域变换加密;3)基于图像空间域和色度域变换加密。其中,基于图像空间域变换的数字图像置乱是一种常见的图像加密方法。图像置乱的要求是置乱后的图像具有较低的可懂度;置乱后的图像要有一定的安全性,能抵抗一定程度的破译攻击;解密后的图像能准确地表达原始图像的内容。

文献[3]作者提出用仿射变换的方法实现图像加密,还将 Fibonacci 变换的均匀性和周期性分析应用到图像置乱[4]中。在图像置乱研究中,Arnold 变换及其扩展方法得到了较多的应用[5-6],但需要多次迭代计算才能得到一幅置乱图像,效率较低。文献[7]作者提出一种基于位交换的置乱算法,通过位分解,互换奇数列和偶数列位置,提高了运算速度,但密钥空间小。文献[8]作者提出一种基于混沌序列的置乱算法,将图像的奇行和偶行分别与不同的混沌序列异或,密钥空间较大,也不需迭代,但加密后像素分布不均匀。

基于上述分析,本文提出一种新的基于混沌序列和位交换的图像置乱算法。该算法利用混沌序列和图像本身的自相关性进行加密,不需迭代,经过一次运算即可得到加密图像。与传统方法相比,该算法能有效地提高运算速度和保密性,像素分布均匀,置乱效果好。

1 Logistic 混沌序列和图像像素的位分解

Logistic 映射是一种简单但广泛应用的混沌序列生成器,混沌系统表述为:

$$x_{k+1} = \mu x_k(1 - x_k) \tag{1}$$

其中,$3.569\,946\,5 \leqslant \mu \leqslant 4$,$x \in (0,1)$,本文取 $\mu = 4$。这样,Logistic 映射可以定义在(0,1)上,相应地得到定义在(0,1)上的伪随机序列$\{x_k, k = 1,2,\cdots\}$。对其进行非线性离散化如下:设$\{s_k, k = 1,2,\cdots\}$为由混沌序列$\{x_k, k = 1,2,\cdots\}$经离散化得到的0,1序列。当 $k = 1$ 时,s_1 的值由 x_1 和0.5比较而得:当 $x_1 < 0.5$ 时,$s_1 = 0$;当 $x_1 \geqslant 0.5$ 时,$s_1 = 1$。当 $k > 1$ 时,s_k 的值由 x_k 和 x_{k-1} 比较而得:当 $x_k < x_{k-1}$ 时,$s_k = 0$;当 $x_k \geqslant x_{k-1}$ 时,$s_k = 1$。本文中,为了增强加密效果,要求舍弃序列的前 t

收稿日期:2009 - 04 - 01;**修回日期**:2009 - 06 - 08。 **基金项目**:陕西省自然科学基金资助项目(FC06121)。

作者简介:袁玲(1979 -),女,河南新野人,讲师,硕士研究生,主要研究方向:计算机图形学、图形图像、多媒体技术; 康宝生(1961 -),男,陕西礼泉人,教授,博士生导师,主要研究方向:计算机辅助几何设计、图形图像、多媒体技术。

项。t 作为密钥,其值由用户指定。

对一幅 $M \times N$ 的 L bit 图像 X 进行位分解得到 L 个位平面,每个像素在每一位平面对应 0 或 1。第 n 行第 m 列像素为 $C(m,n)$。令 $B^l(\cdot)$ 为位分解算子,则 $C(m,n)$ 的第 l 位为:

$$C^l(m,n) = B^l[C(m,n)] = \begin{cases} 1, \left[\frac{C(m,n)}{2^l}\right] \bmod 2 = 1 \\ 0, \text{其他} \end{cases} \tag{2}$$

2 算法原理

2.1 按位异或和混沌序列

按位异或是将两个二进制位的操作数从低位到高位依次对齐后,每位求异或的结果是只有两位不相同时,结果为 1,否则结果为 0。假设 $A = \{0110\}$,$B = \{0011\}$,xor 为异或运算符,记 A,B 的异或运算值为 C,即 A xor $B = C$,则 $C = \{0101\}$;反之,C xor $B = A$,C xor $A = B$。若 A 为秘密数据,B 为由密钥唯一生成的序列,则 C 可以看成是秘密数据 A 的置乱。通过 C 与 B 的异或运算,可准确地还原出秘密数据。

用 Logistic 序列生成器和密钥 μ, x_0 产生一个混沌序列,并用前述方法对其二值化,得到一个二值混沌序列 s。由用户指定密钥 t,舍弃序列 s 的前 t 项,取 $s = \{s_{t+1}, s_{t+2}, \cdots, s_{t+M+N+L}\}$,为方便起见,记为 $s = \{s_1, s_2, \cdots, s_{M+N+L}\}$,其中 M 和 N 为待加密图像的大小,L 为待加密图像中每个像素的位平面数。

2.2 加密方法

用式(2) 对图像的每个像素进行位分解,使每个像素变为 L 位二进制数,并在序列 s 中,根据每个像素点的位置选取子序列 $sp = \{s_{m+n}, s_{m+n+1}, \cdots, s_{m+n+L}\}$,其中 m,n 为像素点的坐标。对像素点 $C(m,n)(m \in [0,M-1), n \in [0,N-1))$,若 $m+n$ 是奇数时,用 $C(m,n)$ 的二进制序列按位异或序列 sp,并交换高位和低位序列的位置。以 $L = 8$ 为例,即第 8 位和第 4 位交换,第 7 位和第 3 位交换 …… 第 5 位和第 1 位交换;若 $m+n$ 为偶数时,则先交换高位和低位序列,再与序列 sp 异或。

2.3 算法步骤

1) 输入原始图像 C;

2) 输入密钥 μ、x_0 和 t,用式(1) 产生需要的序列 s;

3) 根据式(2) 对图像中的像素点 $C(m,n)(m \in [0,M-1), n \in [0,N-1))$ 进行位分解;

4) 根据 $C(m,n)$ 的位置,即 m,n 的值,选取 s 的子序列 $sp = \{s_{m+n}, s_{m+n+1}, \cdots, s_{m+n+L}\}$。若 $m+n$ 为奇数,则用 $C(m,n)$ 异或 sp,再交换高位和低位的位置;否则先交换位置,再与 sp 序列异或,得到新的数字 Y,Y 即为置乱后该点的像素值;

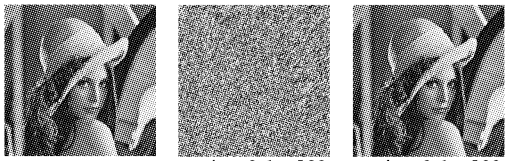
5) 重复执行 4),直到图像中每个像素点均被处理为止。

2.4 解密

解密时先对像素进行位分解,再根据密钥 μ、x_0 和 t 得到序列 $s = \{s_1, s_2, \cdots, s_{t+M+N+L}\}$。对每个像素点 $C(m,n)(m \in [0,M-1), n \in [0,N-1))$,根据 m 和 n 的值确定子序 $sp = \{s_{m+n}, s_{m+n+1}, \cdots, s_{m+n+L}\}$。若 $m+n$ 为奇数,则先交换高低位,再与 sp 序列异或;否则就先与 sp 序列异或,再交换奇偶位。

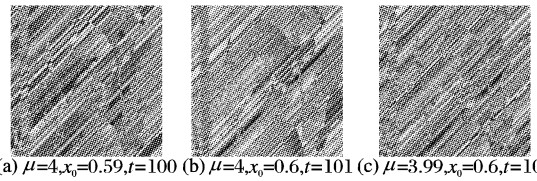
3 实验结果与分析

为验证算法的有效性和安全性,对其进行仿真实验,实验结果如图 1 ~ 6 和表 1 ~ 2 所示。其中,μ、x_0 为混沌初值,t 为舍弃混沌序列的项数。



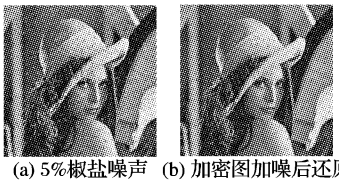
(a) 原图 (b) μ=4,x_0=0.6,t=100 置乱图片 (c) μ=4,x_0=0.6,t=100 正确解密

图 1 正确解密



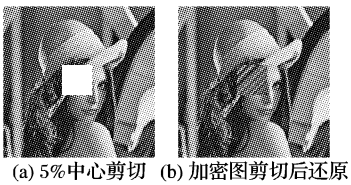
(a) μ=4,x_0=0.59,t=100 (b) μ=4,x_0=0.6,t=101 (c) μ=3.99,x_0=0.6,t=100

图 2 错误解密(解密方法正确,但其中一个参数错误)



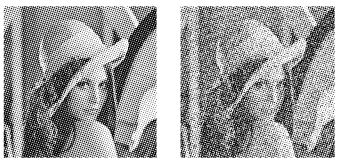
(a) 5%椒盐噪声 (b) 加密图加噪后还原

图 3 椒盐噪声影响



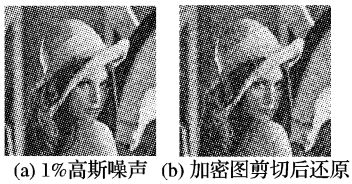
(a) 5%中心剪切 (b) 加密图剪切后还原

图 4 剪切攻击影响



(a) 5%加性噪声 (b) 加密图加噪后还原

图 5 加性噪声影响



(a) 1%高斯噪声 (b) 加密图剪切后还原

图 6 高斯白噪声影响

表 1 峰值信噪比(PNSR)数据比对

原始图像	PSNR	椒盐噪声	块裁剪	高斯噪声
	PSNR1	43.773	43.931	42.573
	PSNR2	43.326	42.203	41.947
	PSNR1	44.251	34.184	37.322
	PSNR2	29.806	39.052	36.548
	PSNR1	43.854	38.079	41.417
	PSNR2	44.086	40.975	38.108
	PSNR1	43.922	38.431	40.746
	PSNR2	43.761	43.052	41.063

表 1 中:在块裁剪时,本文不论原图大小,均裁剪原图中任意位置50 像素 ×50像素的图像块。PNSR1 为公开图像受

攻击后的 PNSR;PNSR2 为置乱后图像受攻击的 PNSR。

本文置乱算法属于空间域置乱算法,结合了位交换和混沌序列,混沌序列的初值敏感性和随机性使算法有了很高的安全性。而把每个像素的位分离,进行位交换,使得一个像素点 的可操作范围扩大到8位。此外,在加密过程中,对像素点不是单纯的分奇偶行或者奇偶列进行加密,而是对同一条对角线上的元素采用相同的加密方法。对混沌序列的选取,也采用了中间截取的方式。在同一幅图像中,截取的每一个混沌序列,只与两个像素点异或,使得该算法的安全性大大增加。

表 2　本文算法与其他算法比较

算法	效率	加密效果	安全性	算法特点
本文算法	一次迭代,效率高	像素分布均匀	可以抵抗一定噪声攻击和已知选择明文攻击	效率,加密效果和安全性均较好,能原样恢复加密图像
Arnold 类算法	多次迭代,效率低	像素分布均匀	不能抵抗已知选择明文攻击	效率较低,安全性较差,加密效果好,实现容易
文献[8]算法	一次迭代,效率高	像素分布不均匀	不能抵抗已知选择明文攻击	效率高,加密效果和安全性差
文献[9]算法	一次迭代,效率高	像素分布均匀	不能抵抗已知选择明文攻击	效率和加密效果较好,但安全性较差
文献[10]算法	一次迭代,效率高	像素分布均匀	安全性好,可以抵抗各种攻击	效率效果和安全性均较好,但解密图不能原样恢复

在其他空间域算法中,Arnold 变换具有周期性,对于 $N \times N$ 的图像,在连续变换 T_N 次之后可以恢复原始图像。据文献[3]的分析,对于任意 $N > 2$ 的图像,Arnold 变换的周期为 $T_N \leqslant N^2/2$。由此可知,对于 Arnold 变换,图像越大,其变换周期越长,相应的加密和解密效率也就越低。其他基于混沌序列的空间域加密算法,都是依靠混沌序列的伪随机性来达到加密图像的目的。因此加密过程一般不需要迭代,算法质量的好坏,主要取决于加密算法的安全性以及加密图像的效果。文献[8]中同时使用两种混沌序列,分别与图像的奇数行和偶数行异或,密钥空间比较大,但是加密图像素分布不均匀,加密效果不太理想,不能抵抗已知选择明文攻击。CKBA 算法[9]也采用了混沌序列与图像异或的方法。但和文献[8]一样,算法中选取的与图像异或的混沌序列是一定的,由异或运算的性质可知,该算法同样不能抵抗已知选择明文攻击。而对于本文提出的算法,其混沌序列的选取以及加密方法的选择,是和图像自身的性质紧密联系,不同图像,甚至同一图像中不同像素位置的加密方法均不同,使得攻击者不能进行已知选择明文攻击,大大提高了算法的安全性。

还有一类加密算法是在变换域进行的。文献[10]作者提出在加密算法中结合小波变换和混沌序列,在变换域对变换后的小波系数进行加密,使得对一个系数的修改会影响到图像中的每个像素,可以有效抵抗各种攻击,算法安全性好;但是在解密图的恢复上,不能原样恢复数据,使得解密图的质量下降,对算法的应用范围有所限制。

实验表明:使用本文算法置乱后的像素均匀分布,已不能分辨出原图信息;在解密过程中,如果有一个参数和密钥不一致,都不能得到正确的解密结果。

根据算法特点和实验结果,本算法对彩色图像也能得到较好的置乱效果。在对加密图像进行椒盐噪声攻击时,解密图能够较好地恢复,虽然可以看出噪声影响的痕迹,但程度已大大减轻(PSNR 值大于原图受攻击的 PSNR 值)。在对加密图进行裁剪攻击时,被裁剪的部位信息丢失,恢复时,对应位置不能正常恢复,但是其余位置的图像不受影响。对图像进行加性噪声、乘性噪声和高斯白噪声攻击时,会引起解密图像的降质,但是不影响图像内容的识别。通过仿真实验检验,该算法可以抵抗一定程度的攻击,具有一定的鲁棒性。

4　结语

本文所给的图像置乱算法,将像素位分为高四位和低四位,通过判断像素位置,在每个像素组内进行高低位交换打乱位值次序,并且与混沌序列异或操作,改变像素颜色实现图像加密,建立了替换像素和被替换像素的映射关系。由于执行 1 次就可以得到加密图,不需要反复迭代,所以该算法具有较高的效率。但是,二值图像只用一个 bit 表示像素值,不能进行位交换。所以,本算法不能用于二值图像的置乱。

参考文献:

[1] 王怀彬,孔德慧,王鹏涛. 一种新的信息加—解密技术的研究[J]. 光电子·激光, 2005, 16(12):1496 - 1499.

[2] 陈靖远,陶亮. 基于 Gabor 变换的一种有效的图像水印技术[J]. 光电子·激光, 2005, 16(11):1363 - 1367.

[3] ZOU J, TIE X, WARD R K, *et al.* Some novel image scrambling methods based on affine modular matrix transformation[J]. Journal of Information and Computational Science, 2005, 2(1):223 - 227.

[4] ZOU J, WARD R K, QI D. A new digital image scrambling method based on Fibonacci numbers[C]// Proceedings of the 2004 IEEE International Symposium on Circuits and Systems. [S. l.]: IEEE Press, 2004, 3:965 - 968.

[5] 丁玮, 闫伟齐, 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.

[6] YANG YA-LI, CAI NA, NI GUO-QIANG. Digital image scrambling technology based on the symmetry of Arnold transform[J]. Journal of Beijing Institute of Technology, 2006, 15(2):216 - 220.

[7] 唐振军,路兴,魏为民,等. 基于位交换的图像置乱[J]. 光电子·激光,2007,18(12):1486 - 1488, 1495.

[8] 赵玉霞. 数字水印关键技术研究及应用[D]. 西安: 西北大学, 2008.

[9] YEN JUI-CHENG, GUO JIUN-IN. A new chaotic key-based design for image encyption and decryption[C]// Proceedings of IEEE International Symposium on Circuits and Systems. Geveva: IEEE Press, 2000, 4:49 - 52.

[10] 穆秀春,张娜. 基于小波变换的混沌图像置乱加密算法[J]. 信息安全, 2008, 31(15):84 - 86, 90.