一种基于分块和混沌网的图像置乱方法

田 岩[1] 谢玉波[1] 李 涛[2] 柳 健[1,2]

[1](华中科技大学电子与信息工程系，武汉 430074) [2](华中科技大学图像识别与人工智能研究所，武汉 430074)

摘 要 图像置乱是实现图像加密的重要手段之一。由于混沌系统具有非周期性、遍历性、伪随机性和对初值的高度敏感性，因而已被广泛应用于图像置乱。为提升图像置乱效果和置乱性能，现提出了一种图像分块与混沌网相结合的图像置乱方法。该方法首先利用一种分块思想将图像进行置乱，进而构造一种混沌网，并将其应用于分块置乱的结果。实验结果表明，该方法不仅可取得良好的置乱效果，并具有较强的抗攻击性能。

关键词 图像置乱 混沌系统 图像分块

中图法分类号：TP309 **文献标识码**：A **文章编号**：1006-8961(2007)01-0056-05

An Image Scrambling Method Based on Image Blocking and Chaos System

TIAN Yan[1], XIE Yu-bo[1], LI Tao[2], LIU Jian[1,2]

[1](*Department of Electronic and Information Engineering, Huazhong University of Science and Technology, Wuhan* 430074)

[2](*Institute for Pattern Recognition and Artificial Intelligence, Huazhong University of Science and Technology, Wuhan* 430074)

Abstract Image scrambling is an available means for image encryption. Since chaos system is extremely sensitive for initial value, ergodic and aperiod, it was widely applied for image encryption. Because there are certain techniques to decode the encryption method based merely on chaos system, a novel scrambling method based on image blocking and chaos system is presented in this paper. The rough idea of this method is that an image is scrambled by a blocking method, and then the result is further scrambled by a modulating way provided by chaos system. The experimental result proves that the new method is effective.

Keywords image scrambling, chaos system, image blocking

1 引 言

随着计算机网络和多媒体的迅速发展，数字图像信息安全的保障问题日益凸显，因此，图像加密技术近年来成为图像处理中的一个非常重要的研究方向。作为图像加密的常见手段之一——图像置乱目前已得到广泛的关注。所谓图像置乱就是旨在通过某种变换使得原始图像的内容变得杂乱无章，且无从理解和辨识，从而达到保护图像真实内容的目的。

目前关于图像置乱的研究已开展了许多工作，其中包括 Arnold 变换、Peanon 曲线和幻方变换等等[1,2]。众所周知，混沌现象是出现在非线性动态系统中的伪随机过程，由于它具有非周期性、遍历性、伪随机性和对初值高度敏感等特点，使其具有天然的信息隐藏能力，因而广泛用于信息置乱[3,4]。在基于混沌系统的图像置乱研究方面，Shi 和 Bhargava 提出了一种参数化的 2 维混沌方法用来置乱图像的像素[5]；在文献[6]中，利用混沌系统，孙鑫等人提出了基于混沌系统的在空域和频域构造置乱矩阵来置乱图像的方法。然而另有研究表明，一些单纯建立在混沌系统上的置乱方法已有了破解方法，如 Seshan 等已经发现基于混沌覆盖或是混沌调制的编码方案可以利用非线性多步预测方法来解

基金项目：国家自然科学基金项目(60572048)

收稿日期：2005-07-06；**改回日期**：2006-02-13

第一作者简介：田岩(1970～)，男，副教授。2000 年获武汉大学理学博士学位，2000～2002 年于华中科技大学控制科学与工程博士后流动站工作，2003～2004 年于香港理工大学做访问学者。主要从事图像处理、机器视觉、非线性分析等方面的研究。E-mail：tianyan2000@126.com

码[7],例如文献[8]提出应用神经网络来破解低维的混沌密钥切换系统。因而,必须通过提高混沌系统的维数或是与其他置乱方法相结合来提高混沌系统的图像置乱性能。

鉴于混沌置乱以上的优缺点,本文提出一种基于混沌网和图像分块的置乱方法。该方法首先利用一种分块置乱方法来置乱一幅图像;然后,再用构造的混沌网将上一步所得的结果进行置乱。本文方法简洁易行,实验结果表明,该方法不仅置乱性能良好,且抗攻击性强。

2　混沌系统

前面已经提到,混沌系统来源于非线性动态系统的伪随机过程。1 维的动态系统可以表示为

$$s_{k+1} = \mu F(s_k) \tag{1}$$

其中,μ 是系统参数,$s_k \in \boldsymbol{V}(k=0,1,2,\cdots)$ 为状态,非线性映射 $F:\boldsymbol{V}\to\boldsymbol{V},\boldsymbol{V}\subset\boldsymbol{R}$ 就是将目前状态 s_k 映射到下一个状态 s_{k+1}。

Logistic 映射是一种非常简单同时也非常实用的动态系统,其定义如下:

$$s_{k+1} = \mu s_k(1-s_k) \tag{2}$$

其中,$0\leqslant\mu\leqslant 4$ 是系统参数,$s_k\in(0,1)$。当 $3.569\,945\cdots<\mu\leqslant 4$,则该系统处于混沌状态。通过简单的变量代换,Logistic 映射可以定义在区间 $(-1,1)$ 中,并可以表示为

$$s_{k+1} = 1-\mu s_k^2 \tag{3}$$

这里 $\mu\in[0,2]$。Chebyshev 映射是另外一种形式简单的映射方式,而具有 k 阶的 Chebyshev 映射则可表示为

$$F(s_{k+1}) = \cos(n(\arccos s_k)) \tag{4}$$

其中,$s_k\in(-1,1)$,如果式(3)中参数 $\mu=2$,则 Logistic 映射为一满射,此时 Logistic 映射和 Chebyshev 映射互为拓扑共轭。

给定初值 s_0 及混沌序列的其他密钥后,就可由式(1)得到一个混沌序列,再通过混沌序列调制图像的像素便可实现图像的置乱。一般情况而言,混沌序列的密钥包含系统类型 F、系统参数 μ 和初值 s_0 等 3 个部分,这是因为不同的混沌系统可以产生不同的随机序列,而相同的混沌系统类型,不同参数产生的混沌序列也不相同,即便对于相同的系统类型和相同的系统参数,不同的初值也能产生截然不同的随机序列,故而混沌序列产生的密钥可以表示成 $K(F,\mu,s_0)$ 的形式。

3　基于图像分块和混沌网的图像置乱

为了提升混沌序列的置乱性能和抗攻击性,首先介绍一种基于图像分块的空域置乱方法,并将其与构建的混沌网相结合进一步置乱图像,此即本文提出的基于分块和混沌网的置乱方法。该方法本质上是多个方法的结合,由于在混沌置乱之前添加了空间置乱,因此新的置乱方法的性能无疑被加强。

下面给出本文方法的具体实现步骤(为了简单起见,在以下步骤中,被置乱图像的大小假设为 $2m\times 2n, m,n\in\boldsymbol{N}$)。

(1) 将原图像等分为 4 部分,按照左上、右上、左下和右下 4 个方向,将这些子图像分别记为 $f_1^{(1)}(x,y)$,$f_2^{(1)}(x,y)$,$f_3^{(1)}(x,y)$ 和 $f_4^{(1)}(x,y)$;

(2) 分别将图像 $f_2^{(1)}(x,y)$ 和 $f_4^{(1)}(x,y)$ 中的像素均匀地散布到图像 $f_1^{(1)}(x,y)$ 和 $f_3^{(1)}(x,y)$ 中,然后将所获得的结果 $f_1(x,y)$ 再按步骤(1)中的方法进行分块,并将子图像分别表示为 $f_1^{(2)}(x,y)$,$f_2^{(2)}(x,y)$,$f_3^{(2)}(x,y)$ 和 $f_4^{(2)}(x,y)$,进行分块置乱时,方法并不唯一,也可以将图像 $f_2^{(1)}(x,y)$ 和 $f_1^{(1)}(x,y)$ 中的像素均匀地散布到图像 $f_3^{(1)}(x,y)$ 和 $f_4^{(1)}(x,y)$ 中去(对对角方向的子图像进行置乱),或是其他组合,双方约定以后,就可作为密钥的一部分;

(3) 分别将 $f_1^{(2)}(x,y)$ 和 $f_2^{(2)}(x,y)$ 中的像素均匀的散布到 $f_3^{(2)}(x,y)$ 和 $f_4^{(2)}(x,y)$ 中,其置乱结果表示为 $\hat{f}_0(x)$,或者可以将 $f_1^{(2)}(x,y)$ 和 $f_2^{(2)}(x,y)$ 中的像素均匀地散布到 $f_4^{(2)}(x,y)$ 和 $f_3^{(2)}(x,y)$ 中去;

(4) 构造 2 维混沌网。通过设定混沌类型、混沌参数及其初值 $s_0^{(1)}$ 和 $s_0^{(2)}$,即可得到长度分别为 m 和 n 的混沌序列 $\boldsymbol{L}_1=\{l_1^1,l_1^2,\cdots,l_1^m\}$ 和 $\boldsymbol{L}_2=\{l_2^1,l_2^2,\cdots,l_2^n\}$,进而构造的混沌网为

$$\boldsymbol{C} = (l_1^1,l_1^2,\cdots,l_1^m)^{\mathrm{T}}(l_2^1,l_2^2,\cdots,l_2^n) = \begin{bmatrix} l_1^1l_2^1 & l_1^1l_2^2 & \cdots & l_1^1l_2^{n-1} & l_1^1l_2^n \\ l_1^2l_2^1 & l_1^2l_2^2 & \cdots & l_1^2l_2^{n-1} & l_1^2l_2^n \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ l_1^ml_2^1 & l_1^ml_2^2 & \cdots & l_1^ml_2^{n-1} & l_1^ml_2^n \end{bmatrix}$$

利用上述混沌网调制图像 $\hat{f}_0(x,y)$ 即可得到置乱后的图像 $f_1(x,y)$;

(5) 重复步骤(1)到步骤(4)过程,直到得到满意的置乱结果为止。

下面给出上述算法的说明:

① 步骤(2)的目的是将一个子图像 $\boldsymbol{P}=(p_{l,k})_{m\times n}$ 均匀地散布到另一个子图像 $\boldsymbol{Q}=(q_{l,k})_{m\times n}$ 中去,现可以用下式描述

$$\pi_{i,j}=\begin{cases}p_{i,j/2} & \text{如果 } j \text{ 为偶数}\\ q_{i,(j+1)/2} & \text{如果 } j \text{ 为奇数}\end{cases} \tag{5}$$

$\boldsymbol{\Pi}=(\pi_{i,j})_{m\times 2n}$ 是置乱后的图像。

② 在步骤(3)中,将一个子图像 $\hat{\boldsymbol{P}}=(\hat{p}_{l,k})_{m\times n}$ 均匀分散到另一子图像 $\hat{\boldsymbol{Q}}=(\hat{q}_{l,k})_{m\times n}$ 中去,可以用式(6)来描述:

$$\hat{\pi}_{i,j}=\begin{cases}\hat{p}_{i/2,j} & \text{如果 } i \text{ 为偶数}\\ \hat{q}_{i/2,j} & \text{如果 } i \text{ 为奇数}\end{cases} \tag{6}$$

$\hat{\boldsymbol{\Pi}}=(\hat{\pi}_{i,j})_{2m\times n}$ 是垂直置乱后的图像。

注:图像分块的思想也可以用以下两种方式来实现:一种方式是将一幅图像划分成一系列的子图($k\times k, k\geq 3$);另一种方式就是先将一幅图像划分成 2×2 的部分,然后将图像按上面的方法进行置乱,最后将结果再次划分成 4×4 的部分…,依次类推。

解码算法是编码算法的逆过程,也就是

(1) 通过混沌系统、系统参数、系统初值和截取规则,即可得到混沌网置乱的恢复图像;

(2) 执行步骤(3)的逆过程;

(3) 执行步骤(2)的逆过程;

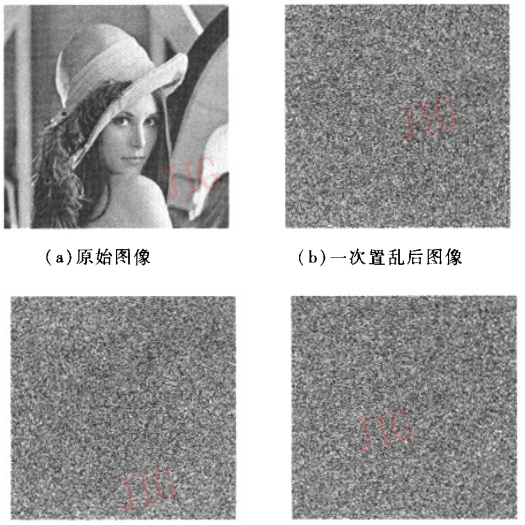
(4) 重复以上步骤,直到得到复原的图像。

4 试验结果及分析

为测试本文置乱算法的性能,本节设计了两组试验。第 1 组实验用来验证算法的置乱效果;第 2 组实验测试其抗攻击能力,考虑到 Arnold 算法具有较强的抗攻击能力,因此选取 Arnold 算法进行对比。

被测试图像如图 1(a)所示,图 1(b)、图 1(c)和图 1(d)分别是按本文算法置乱一次、两次,三次后所得到的结果。这里混沌网由式(3)生成的两个混沌序列来构造,系统参数 $\mu=2$,系统初值 $s_0^{(1)}=0.4$,$s_0^{(2)}=0.8$。

从图 1 可以看到,原图(图 1(a))在一次置乱以后就完全不能被识别,可见本文方法具有较好的置乱性能。



(a)原始图像 (b)一次置乱后图像

(c)两次置乱后图像 (b)三次置乱后图像

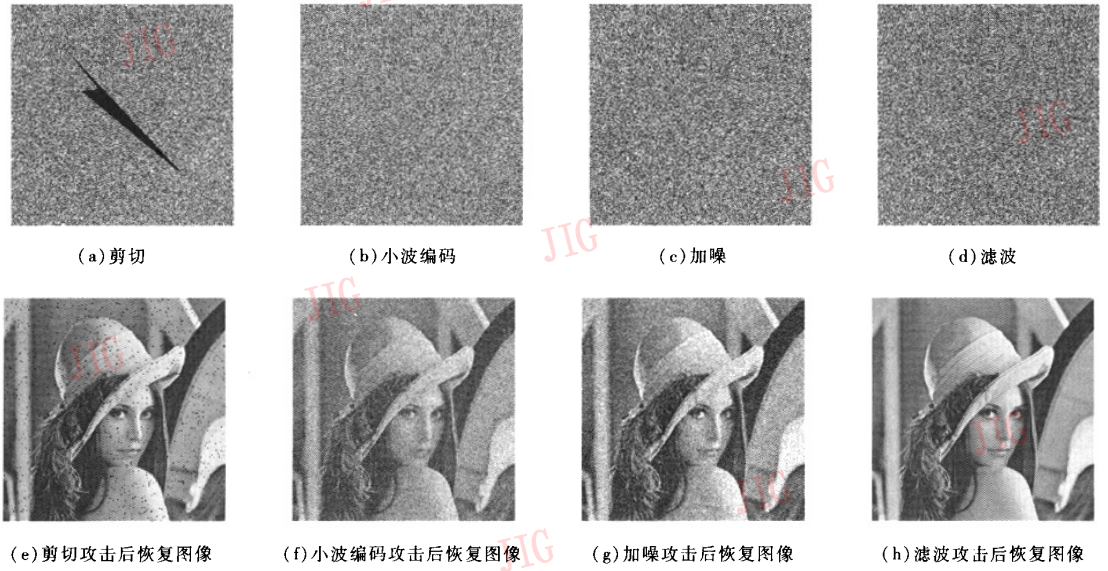
图 1 本文方法的置乱结果

Fig. 1 Scrambling results of the proposed method

为了测试本文算法的抗攻击能力,在这里采用了以下几种常用的攻击手段:几何攻击(剪切)、基于小波变换的编码、加噪和滤波。图 2(a)、图 2(b)、图 2(c)和图 2(d)分别是三次置乱后得到的图像遭受以上攻击手段后得到的图像。图 2(e)~图 2(h)是对应以上受攻击图像的恢复结果。本文实验添加的高斯噪声的方差为 0.01,滤波采用的是均值滤波。从图 2 的实验结果可以看到,原图能够得到较好的恢复,这表明该方法对常用的攻击手段具有较强的抵抗能力。图 3(a)、图 3(b)、图 3(c)和图 3(d)分别是对经 Arnold 变换 8 次置乱后的图像,同样采用几何剪切、基于小波变换的编码、加噪和滤波等 4 种攻击手段后得到的结果,图 3(e)~图 3(h)是对应的恢复结果。

通过对图 2、图 3 的对比可以看出,在抵抗编码、噪声和滤波方面的性能,本文方法和经典的 Arnold 方法的视觉效果几乎相当,但在抗几何攻击时,本文方法能够比较均匀地将剪切区域散布到整幅图像中去,使恢复的图像在很大程度上保持了原图像的信息,而 Arnold 方法在恢复时则带来明显的块状效应,使相当一部分图像信息丢失。另外,计算得到的各个恢复结果的均方根误差如表 1 所示。

从表 1 可以看到,在抗几何剪切能力方面,两种方法效果相差无几,但在另外 3 种情形下,本文方法的优越性是显然的。

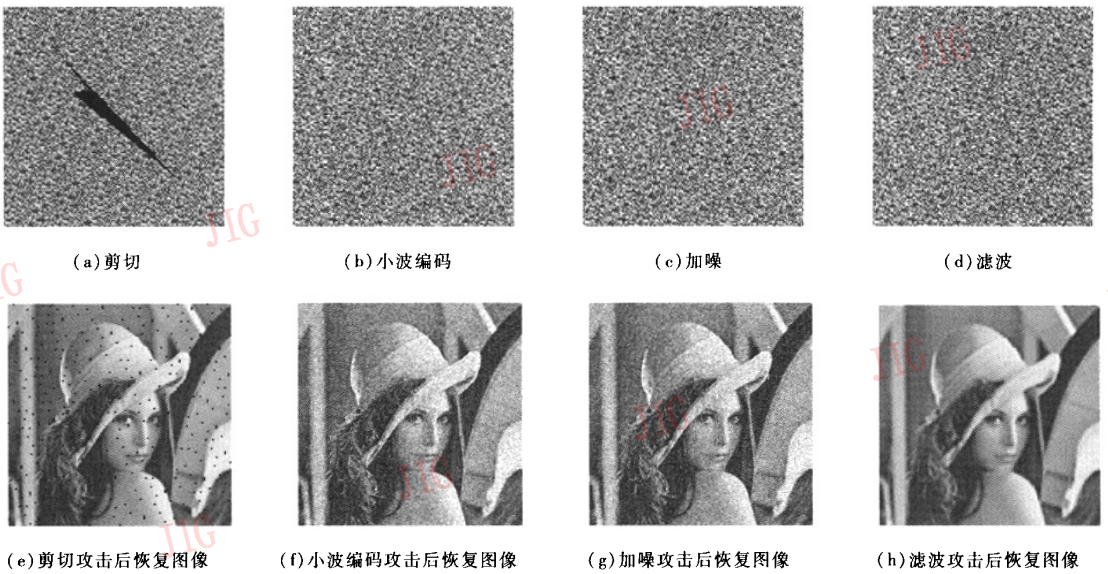


(a)剪切　(b)小波编码　(c)加噪　(d)滤波

(e)剪切攻击后恢复图像　(f)小波编码攻击后恢复图像　(g)加噪攻击后恢复图像　(h)滤波攻击后恢复图像

图 2　本文方法的抗攻击能力

Fig. 2　The anti-attack performance of the proposed method



(a)剪切　(b)小波编码　(c)加噪　(d)滤波

(e)剪切攻击后恢复图像　(f)小波编码攻击后恢复图像　(g)加噪攻击后恢复图像　(h)滤波攻击后恢复图像

图 3　Arnold 加密算法的抗攻击能力

Fig. 3　The anti-attack performance of the Arnold method

表 1　恢复图像的均方根误差

Tab. 1　The root square error of the restored results

	剪切	编码	加噪	滤波
本文算法	0.077 13	0.046 38	0.050 07	0.021 73
Arnold 算法	0.077 09	0.046 69	0.050 18	0.022 10

5　结　论

图像置乱是图像编码的一种有效手段,考虑到单纯的基于混沌系统的置乱方法有被破解的危险,本文首先提出一种图像分块的置乱方法,然后将此

与混沌系统相结合,提出了一种混合式的置乱方法。实验结果表明,本文方法不仅在图像置乱方面具有非常好的性能,同时具有良好的抗攻击能力。

参考文献(References)

1 Qi Dong-xu, Zhou Jian-cheng, Han Xiao-you. A new chaos transformation and its application in image information hiding[J]. Science In China(Series E), 2000, **30**(5): 304 ~ 312. [齐东旭, 邹建成, 韩效宥. 一类新的置乱变换及其在图像信息隐蔽中的应用[J]. 中国科学 E 辑, 2000, **30**(5): 304 ~ 312.]

2 Qi Dong-xu. Fractal and Its Generation for Computer[M]. Beijing: Science Press, 1994: 143 ~ 145. [齐东旭. 分形及其计算机生成[M]. 北京:科学出版社,1994: 143 ~ 145.]

3 Wu C W, Rul'kov N F. Studying chaos via 1-D maps—a tutorial [J]. IEEE Transactions on Circuits and Systems: Fundamental Theory and Applications, 1993, **40**(10):707 ~ 721.

4 Habustu T, Nishio Y, Sasase I. A secret key cryptosystem by iterating chaotic map[J]. LectNotes Computer Science, 1991, **547**: 127 ~ 140.

5 Shi C, Bhargava B. Light-weight MPEG video encryption algorithm [A]. In: Proceedings of the International Conference on Multimidia' 98[C], New Delhi, India, 1998: 55 ~ 61.

6 Sun Xin, Yi Kai-xiang, SunYou-xian. New image encryption algorithm based on chaos system[J]. Journal of Computer-Aided Design & Compute Rgraphics, 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.]

7 Seshan S, Balakrishan H, Katz R H. Handoffs in cellular wireless net-works: The daedalus implementation and experience[J]. Kluwer International Journal on Wireless Personal Communications, 1997, **4**(2):141 ~ 162.

8 Perkins C E, Wang K Y. Optimized smooth handoffs in mobile IP [A]. In: Proceedings of The Fourth IEEE Symposium on Computers and Communications[C], Red Sea, Egypt, 1999: 340 ~ 346.