

改进的 Fibonacci 双置乱图像加密算法

孙劲光 汪 洁 孟祥福

(辽宁工程技术大学电子与信息工程学院 葫芦岛 125105)

摘 要 图像置乱是实现图像加密的重要手段之一,其最终目的是改变图像像素的位置关系或者灰度值信息,改变图像的统计信息,从而达到图像加密的目的。为提升图像置乱效果和置乱性能,从均匀分块的角度出发,提出了一种改进的 Fibonacci 双置乱图像加密算法。首先采用均匀分块算法对原图像进行分块,使每个分块图像内的所有像素充分扩散到其他各个图像块中,以有效地削弱图像相邻像素的相关性;然后对每个图像块利用 Fibonacci 算法做像素位置置乱,以解除图像块的空间相关性;最后对整幅图像采用 Fibonacci 算法做像素值置乱,解除图像的色彩相关性。实验结果表明,该算法从本质上降低了图像内部相邻像素的相关性,有较强的抵御裁剪和常见噪声攻击的能力,利用双密钥提高了加密系统的安全性。

关键词 图像置乱, Fibonacci 双置乱, 均匀分块, 相关性

中图法分类号 TP391.41 **文献标识码** A

Improved Image Encryption Algorithm Based on Double Scrambling of Fibonacci Transforms

SUN Jin-guang WANG Jie MENG Xiang-fu

(School of Electronic and Information Engineering, Liaoning Technical University, Huludao 125105, China)

Abstract Image scrambling is one of the important means to realize image encryption and the ultimate purpose of scrambling is to change the pixel position or the gray value, change the statistic information of the image, so as to achieve the purpose of image encryption. To enhance the effect and performance of images scrambling, from the perspective of uniform blocking, a kind of improved double scrambling algorithm of Fibonacci transforms was put forward. At first, plain image was carried out, using uniform blocking algorithm, and each sub-block pixel was fully diffused to other sub-blocks in turn to weaken the image correlation between adjacent pixels effectively. Next, scrambling algorithm shuffled the pixels' position of each blocks to weaken the image spatial correlation by using Fibonacci. Finally, scrambling algorithm shuffled the pixels' value of the whole image to weaken the image color correlation by using Fibonacci. The experimental results demonstrate that this algorithm can not only reduce the correlation of image adjacent pixels in essence but also has strong ability against shearing and common noise attacks in some degree, and it improves the encryption system's security by utilizing dual-key cipher.

Keywords Image scrambling, Double scrambling algorithm of Fibonacci transformation, Uniform block, Relevance

1 引言

随着网络信息化的普及,信息在 Internet 上的传播变得日益频繁,保证敏感信息在传播过程中的安全性已成为近年来的研究热点。由于存储技术和网络通信技术的发展,数字图像在网络通信中占有越来越多的比率,图像加密技术的研究正处于蓬勃发展之中。

图像置乱技术是图像加密的一种常用方法,目前常作为数字水印的预处理技术。在图像置乱领域中,国内外很多专家学者提出了各自不同的理论体系,其目的都是想研究一种更为安全的加密方法。图像置乱的目的是通过某种变换算法,使加密图像与原图像的统计信息完全不同,从而保密原图像的真实内容。

现已总结的图像置乱方案可以分3类:(1)基于位置空间的置乱算法;(2)基于色彩空间的置乱算法;(3)基于位置和色彩空间的置乱算法。针对第一类方案,专家学者们提出了很多经典算法,如 Arnold 变换、幻方变换、Fibonacci 变换、面包师变换、Hilbert 曲线法、Tangram 算法、IFS 模型、混沌等。这类算法不改变图像灰度值,无论算法设计如何精妙,都无法改变图像基本统计特征(如直方图等),易引起攻击者的注意;针对图像色彩空间的置乱,常常采用经典的 Gray 码变换等。胡春强^[1]等人基于 Logistic 和标准映射设计了一种置乱变换系统,其通过替代变换改变图像像素值并产生互相依赖,这样加密算法具有置乱、替代和扩散等加密系统的基本要素。第二类方案极大程度地改变了数字图像的统计信息,但算法自身具有局限性,加密效果不佳,应用不广;与前两类方案相比,

到稿日期:2012-03-26 返修日期:2012-07-04 本文受国家青年科学基金(61003162)资助。

孙劲光(1962—),女,教授,博士生导师,主要研究领域为图形和图像处理与人脸识别;汪 洁(1987—),女,硕士生,主要研究领域为图像处理与数字水印;孟祥福(1981—),男,博士,讲师,主要研究领域为 Web 数据库柔性查询与优化、信息安全。

第三类方案扩展了算法的密钥空间,将像素位置置乱和像素值置乱相结合^[2-9],从而弥补了相互的缺陷是图像置乱的发展方向。例如卢辉斌和孙艳^[10]基于混沌系统复杂的非线性行为,提出了一种基于四维超混沌系统的图像加密算法。Thomas Penvy, Patrick Bas, Jessica Fridrich^[11]等人提出一种 LSB 匹配检测算法,即利用消除像素邻接矩阵(SPAM)的方法实现图像加密。Vishal Monga, M. Kivanc Mihcak^[12]提出通过非负矩阵分解实现安全鲁棒的图像哈希算法,这些算法既改变了图像的像素位置,又改变了图像像素值。

本文采用一种改进的 Fibonacci 双置乱图像加密算法,即将待加密的图像分块,然后依次对每个图像块进行位置置乱,最后对块置乱后的图像采用像素值置乱。实验数据表明,本文的图像加密算法改变了图像的统计信息,置乱效果均匀,抵御裁剪和噪声攻击的能力强,具有重要的理论意义和实用价值。

2 Fibonacci 加密算法

2.1 Fibonacci 像素位置变换

Fibonacci 的变换矩阵如式(1)、式(2)所示。

$$F = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \quad (1)$$

$$F^n = \underbrace{\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}}_{n \text{ 个 } F \text{ 矩阵相乘}} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^n \quad (2)$$

图像像素的位置矩阵表示为 $p = (x, y)^H$, 二维 Fibonacci 位置变换表达式为:

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = F \cdot p = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} x \\ y \end{pmatrix} \pmod{N} \quad (3)$$

对图像做 n 次 Fibonacci 位置变换的表达式为:

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = F^n \cdot p = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^n \cdot \begin{pmatrix} x \\ y \end{pmatrix} \pmod{N} \quad (4)$$

$x, y, x', y' \in \{0, 1, \dots, N-1\}$, N 为数字图像矩阵的阶数; (x, y) 和 (x', y') 分别是原图像和置乱后图像像素的位置。

2.2 Fibonacci 像素值变换

无论位置置乱还是像素值置乱,其二维 Fibonacci 变换矩阵相同,都如式(1)、式(2)所示。与位置置乱不同, h 表示任意像素值模纵坐标的十六进制,不再是像素的位置坐标。对图像像素值 h 变换一次的表示形式如下:

$$\begin{pmatrix} h_1' \\ h_2' \end{pmatrix} = F \cdot h = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} h_1 \\ h_2 \end{pmatrix} \pmod{16} \quad (5)$$

则对图像像素值 h 变换 n 次的表示形式为:

$$\begin{pmatrix} h_1' \\ h_2' \end{pmatrix} = F^n \cdot h = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^n \cdot \begin{pmatrix} h_1 \\ h_2 \end{pmatrix} \pmod{16} \quad (6)$$

式中, $h = (h_1, h_2)^H$, $h_i, h_i' \in \{1, 2, \dots, n\}$, $i = 1, 2$, 则 $h' = (h_1', h_2')^H$ 是对每个像素值 h 置乱后对应的像素值。

2.3 Fibonacci 双置乱

Fibonacci 双置乱算法的主要思想是利用图像矩阵左乘二维 Fibonacci 变换矩阵,先改变图像像素位置,再改变像素的灰度值,算法分两步进行:

(1)对图像的像素进行 k_1 次位置置乱,削弱图像的空间相关性。

(2)对图像的像素进行 k_2 次灰度值置乱,削弱图像的色彩相关性。

最终得到随机生成的密钥序列,具体的置乱流程如图 1 所示。

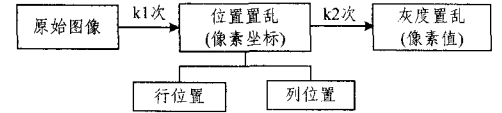


图 1 Fibonacci 双密钥置乱算法流程图

3 均匀分块算法

3.1 图像均匀分块原理

图像能够传达信息是因为图像的像素值之间具有差异性,图像位置置乱的目的是分散“相邻像素点”,从而最大程度地破坏像素之间的相关性。从信息论角度,图像置乱的目的降低图像相邻像素的相关性,使图像像素由最大确定性变换为不确定性的过程,即增加图像信息量的过程。首先提出图像位置熵的定义:

$$H(R) = \sum_{k=1}^B H_k(P) \quad (7)$$

式中, B 为图像分块区域个数; $H_k(P)$ 为第 k 个分块区域的信息熵,即第 k 个分块区域平均位置信息量,可表示如下:

$$H_k(P) = \sum_j P(i, j) \log \frac{1}{P(i, j)} \quad (8)$$

式中, $P(i, j)$ 为原始图像坐标为 (i, j) 的像素在置乱后图像第 k 个分块区域出现的概率。则当 $P(i, j)$ 等概率时熵函数 $H_k(P)$ 最大,从而位置熵 $H(R)$ 最大。

理想的置乱状态是置乱图像中任意分块区域内的点来自原始图像各个位置的概率都相等,或者说原始图像同一分块区域内的点分布到置乱图像不同分块区域的概率相等,则置乱后图像信源的平均信息量最大,置乱效果最好。为达到理想的置乱效果,提出如下均匀置乱方法:若原始图像中每块含有 $n \times n$ 个点,如果这些点分别出现在置乱后图像的 $n \times n$ 个图像块中,不管这些点在置乱后图像各块中出现的顺序如何,只要保证每块中各含有一个点,就称为均匀置乱。

3.2 图像的块置乱

假设图像的尺寸为 $M \times N$, 以 $f(i, j)$ ($1 \leq i \leq M, 1 \leq j \leq N$) 为中心的 $m \times n$ ($0 \leq m \leq M, 0 \leq n \leq N$) 个相邻像素组成的一个邻域,称为图像块。

(1)先将图像做分块处理,通常正方形在图像加密的研究中最有代表意义。图像分块需做如下约束:

①图像行数等于列数,而且是 2 的指数;

②图像平均分成若干块,每块的行数都等于列数。具体的分块过程如下:

根据文献[13],将原始图像分成 M_1 块,每块含有 N_1 个点,置乱后图像分成 M_2 块,每块含有 N_2 个点,那么实现原始图像各块中像素点间的距离由“最近”到“最远”,如图 2 所示,要保证该块中所有像素点被分到置乱后图像的不同块中,则 $M_2 \geq N_1$; 同理,实现原始图像各块中像素点间的距离由“最远”到“最近”,就必须保证在原始图像所有块中各取的一点,都能分到置乱后图像的同一块中,则 $N_2 \geq M_1$ 。因为 $M_2 \geq N_1, N_2 \geq M_1$, 则 $M_2 N_2 \geq N_1 N_2 \geq M_1 N_1$, 已知 $M_2 N_2 = M_1 N_1$, 那么 $M_2 = N_1, M_1 = N_2$ 。

令原图像由 16×16 个像素点组成,每块中有 2×2 个点,共分成 8×8 块,置乱后的图像为每块中有 8×8 个像素点,共

分成 2×2 块,如图 2 所示。

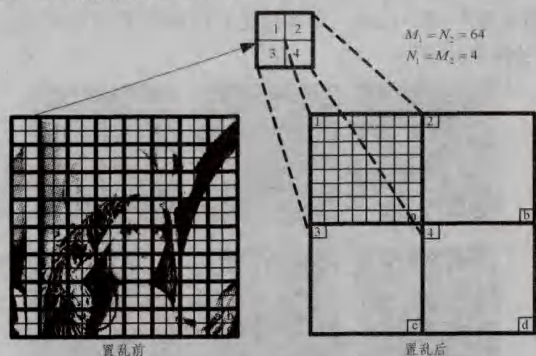


图 2 图像均匀分块原理

(2) 分别将置乱后的每个图像块按式(4)做 Fibonacci 位置变换,图像的加密流程如图 3 所示。其中 OriImage 是原始图像,ScrImage 是加密图像。

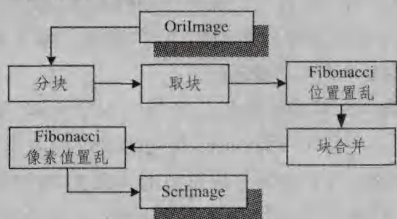


图 3 图像加密流程

图像的解密是加密的逆过程。即利用已知密钥,首先将加密图像做 Fibonacci 反变换,对图像的像素值置乱进行恢复,然后按照加密时块置乱的规律采用均匀分块算法,最后对图像块做 Fibonacci 反变换,对图像块的像素位置置乱进行恢复,就能将原始图像还原。

4 实验效果与分析

4.1 相邻像素相关性分析

图像的本质特征决定了图像中相邻像素间具有很大的相关性,利用该性质的统计攻击方法来分析图像的加密算法就成为可能,因此用相关系数来衡量加密算法破坏相邻像素相关性的能力。首先,从图像中随机选取 1000 对相邻像素点(水平、垂直和对角),然后利用以下公式进行计算。

$$E(x) = \frac{1}{N} \sum_{i=1}^N x_i \quad (9)$$

$$D(x) = \frac{1}{N} \sum_{i=1}^N [x_i - E(x)]^2 \quad (10)$$

$$Cov(x, y) = \frac{1}{N} \sum_{i=1}^N [x_i - E(x)][y_i - E(y)] \quad (11)$$

$$r = \frac{Cov(x, y)}{\sqrt{D(x)} \sqrt{D(y)}} \quad (12)$$

式中, x 和 y 分别表示相邻两个像素的像素值, $E(\cdot)$ 、 $D(\cdot)$ 和 $Cov(\cdot)$ 分别是期望、方差和协方差, r 是相邻两像素的相关系数,其值接近 1 的程度越高,相邻像素的相关性越高。将 Lenna 图像分别采用传统的整体 Fibonacci 置乱算法与本文算法进行相邻像素相关性对比实验,比较图像在 3 个方向的相邻像素相关性。通过表 1 的计算结果可见,原始图像的相邻像素是高度相关的,相关系数接近于 1,密图的像素相关性接近于 0,而且利用本文算法能更大程度地降低相邻像素的相关性,几乎达到了 0 相关。可见采用改进的双置乱加密算

法明显优于传统的 Fibonacci 置乱算法。

表 1 相邻像素的相关系数对比

方向	Lenna		
	原始图像	传统 Fibonacci	本文算法
水平方向	0.95690	0.06921	0.00061
垂直方向	0.89190	0.05007	0.00400
对角线方向	0.92230	0.08832	0.00570

4.2 置乱效果比较

图像置乱包括位置置乱和像素值置乱,置乱的最终目的是实现最大程度的混乱和扩散,对位置置乱而言,如果原始图像任意小的部分都能在加密之后的图像中呈均匀分布,那么可将其看作理想状态;对像素值置乱而言,如果加密之后的像素值能在(0~255)范围内呈均匀分布,即将灰度直方图的均匀分布看作理想状态。从图 4 可见,传统的置乱算法多数是对图像整体进行位置置乱,加密多次才能达到理想效果;而且单纯的位置置乱即使迭代多次,其灰度直方图也达不到均匀分布的状态,没有削弱图像像素的相关性;然而采用双置乱算法可以在较少的置乱次数下达到混乱和扩散的理想效果,有效削弱了图像像素的相关性。

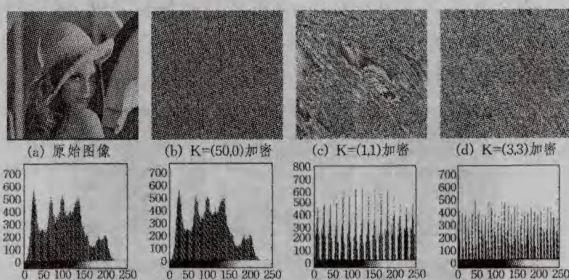


图 4 原始图像和加密图像的直方图分析

传统分块方法分 3 步进行:

①将图像进行分块,假设图像大小为 256×256 ,分块数为 32×32 ,则计算每个图像块中像素点的个数为 $(256 \times 256) \div (32 \times 32) = 8 \times 8 = 64$ 。

②对含有 64 个像素点的块进行位置置乱。

③采用幻方变换对图像整体进行加密。

第一行和第二行分别是采用传统分块算法和本文算法由不同分块数目获得的加密效果,如图 5 所示。

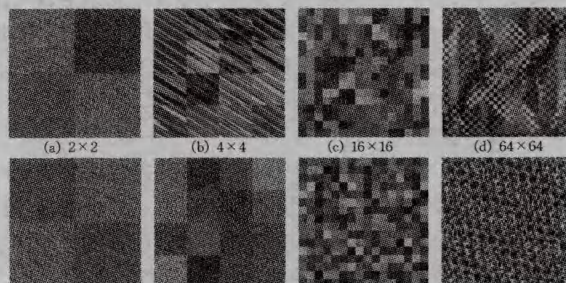


图 5 传统分块方法与改进分块方法比较

从图 5 可见,传统的分块方法具有一定的置乱效果,但随着分块数目的增加,原始图像信息逐渐从加密图像中显现出来,所以传统的分块算法有一定的局限性;而改进的分块方法分块数目越多,置乱效果越好,这是因为改进的方法采用均匀分块思想能够将图像像素均匀打乱,所以改进分块方法在图像加密中更具有实际的应用价值。

4.3 抗剪切实验

衡量图像加密性能一般采用误码率 BER、归一化相关系数 NC 和信噪比 SNR 3 个指标,它们的定义如下:

$$BER = \frac{M}{N} \times 100\% \quad (13)$$

$$NC = \frac{\sum_i \sum_j w(i,j)w_1(i,j)}{\sqrt{\sum_i \sum_j w^2(i,j)} \sqrt{\sum_i \sum_j w_1^2(i,j)}} \quad (14)$$

$$SNR = -10 \cdot \lg(\sum |A-A'|^2 / \sum |A|^2) \quad (15)$$

式中, M 和 N 分别为错误比特数和总比特数, $w(i,j)$ 和 $w_1(i,j)$ 分别为原始图像和对加密图像进行裁剪后恢复图像的数据量; A 和 A' 分别是原始图像和加密图像的方差。表 2 给出图像对随机裁剪攻击的鲁棒性实验结果。

表 2 随机裁剪攻击

裁剪大小/%	NC	BER/%
10	0.9802	5.66
25	0.9244	14.90
50	0.7886	38.27
70	0.5503	49.17
90	0.3796	72.80

首先采用本文算法对 Lena 图像进行加密处理,然后利用 Adobe photoshop 软件对加密图像按图 6 的方案裁剪,图 6(d)~(f)分别是对图 6(a)~(c)裁剪攻击恢复的效果图。

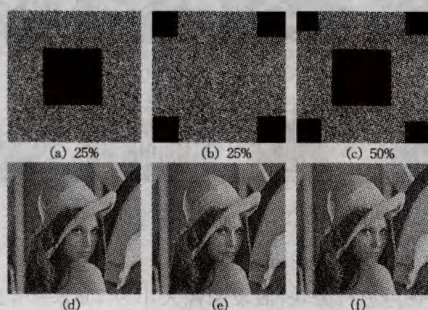


图 6 抗裁剪攻击实验

由裁剪攻击实验得知,对裁剪后的图像进行恢复会存在一定程度的失真,但是要辨认图像所传达的信息并不困难。通过该实验发现,加密图像恢复的效果与裁剪的位置几乎无关,主要因为改进的双置乱算法采用了均匀分块和图像块置乱的思想,使得每个图像块的像素都均匀分布到其他各个图像块,即“广泛分布”,而非“集中分布”,从本质上削弱了图像内部相邻像素的相关性,所以该算法能有效地抵抗裁剪攻击,一定程度的裁剪对图像的恢复影响不大。

4.4 抗噪声实验

图像数据一般用于网络传输,因此不可避免地会受到一些噪声或信道干扰。借此,采用实验验证本文算法抵御噪声攻击的能力是必要的,根据式(13)~式(15)计算加密图像在不同的 Gauss 噪声攻击下的性能,如表 3 所列。

表 3 Gauss 噪声攻击

σ^2	NC	BER	SNR/dB
1	1.0000	00.00	26.7760
100	1.0000	00.00	26.3410
200	1.0000	00.00	25.1006
400	0.9845	04.60	23.5619
600	0.6290	55.47	20.8892

在加密图像中加入不同程度的高斯白噪声,其中参数 m

和 σ 分别代表均值和均方差。加入均值 $m=0$,均方差 σ 不同的高斯噪声,图 7(d)~(f)分别是利用解密算法对图 7(a)~(c)的恢复效果图。

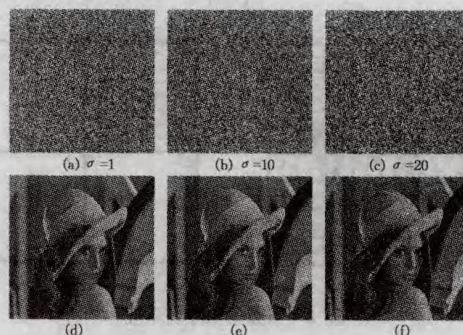


图 7 抗噪声分析结果

通过采用不同参数对密图进行噪声攻击的实验可以看出,当图像受到一定程度的噪声污染时基本能恢复原图像,总体上并不会影响图像所展现的内容,证明了本文算法在一定程度上抵御噪声的性能较强。

结束语 针对传统图像加密技术安全性差、效率低等问题,提出了一种基于 Fibonacci 变换的改进的双置乱方法,其在二维 Fibonacci 和均匀分块思想的基础上,首先将原图像均匀分块,然后对每个图像块进行 Fibonacci 位置置乱,再对块置乱后的图像进行 Fibonacci 像素值置乱,用双密钥决定置乱的次数,增强了加密系统的安全性。实验表明,该算法置乱效率高、置乱效果均匀,相邻像素的相关性小,改变了图像的统计信息,抵御裁剪和噪声攻击的能力较强,是一种实用而有效的图像加密算法。

参考文献

- [1] 胡春强,邓绍江,秦明甫,等. 基于 Logistic 与标准映射的数字图像加密算法[J]. 计算机科学,2010,37(12):57-59
- [2] Singh N, Sinha A. Optical image encryption using Hartley transform and Logistic map [J]. Optics Communications, 2009, 282(6):1104-1109
- [3] Patidar V, Pareek N K, Sud K K. A new substitution-diffusion based image cipher using chaotic standard and logistic maps [J]. Communications in Nonlinear Science and Numerical Simulation, 2009, 14(7):3056-3075
- [4] 陈艳峰,李义方. 交替分段相互置乱的双混沌序列图像加密算法[J]. 华南理工大学学报:自然科学版,2010,38(5):27-33
- [5] Gmbss K, Chandrasekaran V. A novel image encryption scheme using Lorenz attractor[C]// Proceedings of the 4th IEEE Conference on Industrial Electronics and Applications, 2009:3662-3666
- [6] Al-Hamdani Wasim A. Cryptography based access control in healthcare Web systems[C]// Proceedings of Information Security Curriculum Development Conference, New York: ACM, 2010: 66-79
- [7] Luo Wei-qí, Huang Fang-jun, Huang Ji-wu. Edge adaptive image steganography based on LSB matching revisited [J]. IEEE Transaction on Information Forensics and Security, 2010, 5(2): 201-214
- [8] Zhu Zhi-ling, Zhang Wei, Wong Kwok-wo, et al. A chaos-based symmetric image encryption scheme using a bit-level permutation

tion[J]. Journal of Information Sciences, 2011, 181(6): 1171-1186

[9] Wang Qing, Song Ren-wang. Research on Transformation-Domain Digital Audio Blind Watermarking Combining Chaotic Encryption and Arnold Transformation[J]. SCI-TECH Information development and Economy, 2010, 20(17): 127-129

[10] 卢辉斌, 孙艳. 基于新的超混沌系统的图像加密方案[J]. 计算机科学, 2011, 38(6): 149-151

[11] Pevny T, Bas P, Fridrich J. Steganalysis by subtractive pixel adjacency matrix[J]. IEEE Transaction on Information Forensics and Security, 2010, 5(2): 215-224

[12] Monga V, Kivanc Mihcak M. Robust and secure image hashing via non-negative matrix factorization[J]. IEEE Trans on Information Forensics and Security, 2007, 2(3): 376-390

[13] 张健, 任洪娥, 陈宇. 基于均匀置乱的图像位置置乱衡量方法[J]. 计算机工程与应用, 2010, 46(11): 22-25

(上接第 211 页)

表 3 差分进化算法得到的最优解决方案

时间	P _{1t}	P _{2t}	P _{3t}	P _{4t}	P _{5t}	P _{6t}	P _{7t}	P _{8t}	P _{9t}	P _{10t}	P _{1t}	$\sum_{i=1}^{10} P_{it} - P_{Li}$
1	150.00	135.00	73.00	60.00	173.50	160.00	130.00	119.99	44.23	10.00	19.72	1036
2	150.00	135.00	73.00	81.04	174.39	160.00	130.00	120.00	71.61	37.50	22.53	1110
3	150.00	135.30	114.03	130.50	211.77	160.00	130.00	120.00	80.00	55.00	28.61	1258
4	150.00	146.88	176.22	180.50	243.00	160.00	130.00	120.00	80.00	55.00	35.61	1406
5	150.00	192.75	191.93	197.13	243.00	160.00	130.00	120.00	80.00	55.00	39.80	1480
6	169.59	233.34	246.61	239.23	243.00	160.00	130.00	120.00	80.00	55.00	48.77	1628
7	150.00	257.15	287.09	273.28	243.00	160.00	130.00	120.00	80.00	55.00	53.53	1702
8	183.38	244.19	335.84	283.18	243.00	160.00	130.00	120.00	80.00	55.00	58.59	1776
9	249.47	317.09	340.00	300.00	243.00	160.00	130.00	120.00	80.00	55.00	70.56	1924
10	307.38	366.16	340.00	300.00	243.00	160.00	130.00	120.00	80.00	55.00	79.54	2022
11	369.75	396.11	340.00	300.00	243.00	160.00	130.00	120.00	80.00	55.00	87.86	2106
12	397.97	416.49	340.00	300.00	243.00	160.00	130.00	120.00	80.00	55.00	92.46	2150
13	351.54	379.91	337.03	300.00	243.00	160.00	130.00	120.00	80.00	55.00	84.47	2072
14	284.10	306.32	318.08	298.32	243.00	160.00	130.00	120.00	80.00	55.00	70.83	1924
15	213.40	242.68	299.17	291.51	243.00	160.00	130.00	120.00	80.00	55.00	58.76	1776
16	150.00	162.68	252.85	244.13	243.00	160.00	130.00	120.00	80.00	55.00	43.66	1554
17	150.00	135.99	194.98	250.51	243.00	160.00	130.00	120.00	80.00	54.90	39.39	1480
18	181.48	204.94	252.83	249.36	243.00	160.00	130.00	120.00	80.00	55.00	48.60	1628
19	227.74	267.65	257.47	294.32	243.00	160.00	130.00	120.00	80.00	55.00	59.17	1776
20	287.80	340.00	331.91	299.26	243.00	160.00	130.00	120.00	80.00	55.00	74.97	1972
21	276.11	310.95	319.71	300.00	243.00	160.00	130.00	120.00	80.00	55.00	70.78	1924
22	196.11	231.40	239.90	250.79	227.11	160.00	129.80	120.00	79.88	41.97	48.97	1628
23	150.00	151.40	167.43	201.46	196.60	160.00	130.00	112.04	50.57	44.38	31.87	1332
24	150.00	135.00	87.61	154.77	174.62	160.00	129.50	109.71	62.92	45.18	25.31	1184
燃料消耗量 (\$)							2495003.0680					
污染物排放量 (lb)							306600.5398					
总的网络损耗 (MW)							1294.3545					

结束语 本文提出基于差分进化算法和启发式策略的新方法,并将其应用于解决电力系统动态环境经济调度问题。动态环境经济调度问题是双目标优化问题,虽然研究人员已经提出很多双目标优化算法,但是对于高维的双目标优化问题那些算法不但效率低,而且往往得不到满意的解决方案。本文中,首先,采用代价惩罚因子将该双目标优化问题转化成单目标优化问题,该方法大大降低了问题的复杂性;然后,在优化的过程中通过启发式策略修正差分进化算法得到的解决方案,使其满足有功功率输出约束和爬坡约束;同时采用基于优先列表的启发式策略解决动态电力平衡约束条件。仿真实验结果显示,提出的新方法能够有效地解决电力系统动态环境经济调度问题。

参 考 文 献

[1] 荣芬,朱耀明,姚良忠,等. 节能发电调度研究综述[J]. 水电能源科学, 2011, 29(2): 178-181

[2] Zhao B, Cao Y J. Multiple objective particle swarm optimization technique for economic load dispatch[J]. Journal of Zhejiang University Science, 2005, 6A(5): 420-427

[3] 毛弋, 刘文春, 张鹏飞. 利用模糊算法对电力市场下纯火电系统多目标综合经济负荷进行分配[J]. 电力系统及其自动化学报, 2000, 12(6): 22-25

[4] 冯士刚, 艾芊. 火电站多目标负荷调度及其算法的研究[J]. 动力

工程, 2008, 28(3): 404-407

[5] Wang L F, Singh C. Environment/economic power dispatch using a fuzzified multi-objective particle swarm optimization algorithm[J]. Electric Power Systems Research, 2007, 77(12): 1654-1664

[6] Cai J J, Ma X Q, Li Q, et al. A multi-objective chaotic particle swarm optimization for environmental/economic dispatch[J]. Energy Conversion and Management, 2009, 50(5): 1318-1325

[7] Abido M A. Multiobjective particle swarm optimization for environmental/economic dispatch problem[J]. Electric Power System Research, 2009, 79(7): 1105-1113

[8] Wang L F, Singh C N. Reserve-constrained multiarea environmental/economic dispatch based on particle swarm optimization with local search[J]. Engineering Application of Artificial intelligence, 2009, 22(2): 298-307

[9] Wang L F, Singh C N. Stochastic economic emission load dispatch through a modified particle swarm optimization algorithm[J]. Electric Power Systems Research, 2008, 78(8): 1466-1476

[10] Palanichamy C, Sundar B N. Analytical solution for combined economic and emissions dispatch[J]. Electric Power Systems Research, 2008, 78(7): 1129-1137

[11] Basu M. Dynamic economic emission dispatch using nondominated sorted genetic algorithm-II[J]. Electrical Power and Energy Systems, 2008, 30(2): 140-149