

幻方群在图像置乱中的应用

刘颖, 刘健波

(四川大学视觉合成图形图像技术国家重点学科实验室, 四川成都 610064)

摘要: 为了提高幻方置乱图像的加密效果和增大密钥空间, 提出了一种新的基于幻方群的图像置乱算法。首先利用镶边法构造一组同心幻方并将其生成幻方群, 然后对幻方群内的每个同心幻方进行变换, 再对幻方群整体进行变换, 最后用变换后的矩阵对图像进行迭代置乱, 充分打乱图像各像素点的相关性。仿真实验表明, 该算法对传统幻方置乱图像的连续性问题的改进, 且置乱效果明显好于传统幻方置乱图像算法。该算法是一个实用的、有效的图像加密算法。

关键词: 镶边法; 同心幻方; 幻方群; 图像置乱; 迭代

中图分类号: TP309.7

文献标识码: A

文章编号: 1673-629X(2012)09-0119-04

Study and Application of Magic Square Group in Process of Image Scrambling

LIU Ying, LIU Jian-bo

(National Key Laboratory of Fundamental Science on Synthetic Vision, Sichuan University, Chengdu 610064, China)

Abstract: To improve the effect of magic square scrambling algorithm and increase key space, a new digital image encryption algorithm based on magic square group was presented. first the algorithm generated magic square group using a set of concentric magic-squares constructed by edging method. Then the correlation of each digital image pixel positions was disrupted by using magic square group composed of concentric magic-squares which had been transformed. Consequently, dual iteration of pixel position was completed and the encryption algorithm of image scrambling based on traditional magic square was improved. Experimental results show that the effect of the proposed method outperformed the image encryption algorithm based on traditional magic square in continuity of digital image pixel dots and has better consequence; It is a very useful and effective image encryption algorithm.

Key words: edging method; concentric magic square; magic square group; image scrambling; iterative

0 引言

图像置乱是图像加密的主要技术之一, 其目的是将图像噪声化, 使加密后的图像成为对视觉无意义的信号。图像置乱既可单独作为图像加密的方法, 也可与其他加密方法结合构建更为复杂的加密算法, 因而值得深入研究。基于数学的图像置乱方法主要有: 幻方变换、Arnold 变换、FASS 曲线、Gray 代码、生命模型等^[1~5]。其中, 幻方变换是一种经典的方法, 它的本质是对图像矩阵进行有限次初等矩阵变换, 打乱各像素点的位置, 实现图像加密的效果。实际上, 幻方与组合数学、群论等分支有许多关联, 它的潜在价值有待于人们继续探索和发现。

传统幻方置乱图像的算法主要存在两点不足:

(1) 置乱时变换的参数较少使得加密密钥空间很小;

(2) 传统幻方的构造特点决定了加密后的图像上下和左右具有一定的连续性, 即图像上(左)方与图像下(右)方的相邻像素相关性很大。

为减小置乱后图像各像素点相关性, 加大密钥空间, 提高置乱效果, 文中提出了一种新的基于幻方群的图像置乱算法。算法本质上对图像进行了双重的幻方迭代, 使密钥空间得到明显改善, 同时对传统幻方置乱图像的连续性进行了极大的改进。

1 幻方及算法原理

1.1 幻方定义

幻方是组合数学的经典内容, 这里首先给出它的基本定义:

定义1^[6] 幻方(magic square)就是在 $n \times n$ 的方阵中, 放入自然数 $1 \sim n^2$, 使其在一定的布局下各行、各列和两对角线上的数字之和正好都相等。这个和叫做“幻方常数”或“幻和”。对于任意 n 阶幻方, 其幻方常数 H_n 和方阵阶数 n 的关系是: $H_n = \frac{1}{2}n(n^2 + 1)$ 。

收稿日期: 2011-12-27; 修回日期: 2012-03-29

作者简介: 刘颖(1986-), 女, 硕士, 研究方向为信息安全; 刘健波, 博士, 教授, 研究方向为多源数据融合、信息安全等。

定义 2^[7] 如果一个 n 阶方阵满足通常的幻方性质,即各行、各列和两对角线上诸数之和都相等,但其中各数不必是从 1 开始的 n^2 个自然数,则称为广义幻方。

1.2 传统幻方置乱图像的基本原理

将未置乱的数字图像对应的 n 阶数字矩阵记为 Q ,构造一个 n 阶幻方记为 P ,使 Q 与 P 的元素 q_{ij} 与 p_{ij} 一一对应。对于 n 阶幻方 P 中的元素作一次幻方置乱变换:将元素 1 的位置移动至元素 2 所在的位置,将元素 2 的位置移动至元素 3 所在的位置...将元素 $n^2 - 1$ 的位置移动至元素 n^2 所在的位置,最后,将元素 n^2 的位置移动至元素 1 所在的位置。

将经过上述一次幻方置乱后的矩阵记为 $P^{(1)}$,同理,将 $P^{(1)}$ 经过上述变换得到二次幻方置乱的矩阵记为 $P^{(2)}$,...,将 $P^{(k-1)}$ 经过上述变换得到的 k 次幻方置乱矩阵记为 $P^{(k)}$,此时 $k \in \{2,3,\dots, n^2 - 1\}$ 。接下来,将 Q 中的元素作相同的变换,可得到对应的 $Q^{(1)}$, $Q^{(2)}$,..., $Q^{(k)}$,这里 $Q^{(k)}$ 即为经过 k 次幻方变换后得到的最终置乱图像。因为幻方方阵中元素的排列具有相对较大的混乱性,所以经过 k 次幻方变换可以打乱图像中各个像素的位置,从而实现图像加密。

2 镶边法、幻方群及改进后的算法

2.1 镶边法构造同心幻方

镶边法是 17 世纪法国数学家弗兰尼克经过苦心研究的一种可以构造任意阶同心幻方的方法。这里首先给出同心幻方的定义:

定义 3^[7] 如果一个 n 阶幻方,不论去掉外层的一圈或者数圈,所得的 m 阶方阵(2 阶方阵除外)都是由自然数 1 至 n^2 的中间的 m^2 个数(即 $\frac{1}{2}(n^2 - m^2)$ 至 $\frac{1}{2}(n^2 + m^2)$)构成的广义幻方(见定义 2),则称此幻方为同心迭加幻方,简称同心幻方。

镶边法构造同心幻方的主要思想是:构造任意 n 阶幻方,首先将原始的 $n - 2$ 阶幻方的每个数加 $2(n - 1)$,然后在其四周镶一条边,填入余下的数使之成为幻方^[6]。这样由 3 阶幻方,可依次构造 5 阶、7 阶、9 阶...幻方;由 4 阶幻方可依次构造 6 阶、8 阶、10 阶...幻方。如图 1 所示:用镶边法构造 7 阶幻方,中间的 5 阶幻方的数本来应是 1 ~ 25,现均加上 $2(7 - 1) = 12$,变为 13 ~ 37。这样标准的 5 阶幻方就变成幻和为 $\frac{1}{2}n(n^2 + 1) + 2n(n + 1) = 125$ 的广义幻方。中间 $(n - 2)$ 阶方阵确

定后,将 1 ~ $2(n - 1)$ 和与之互补的 $n^2 \sim (n^2 - 2n + 3)$ 填入外层的方格,使内层 $(n - 2)$ 阶幻方的每行每列和两主对角线的角上各是一对互补数,并且这些方向的数字和恰为幻和 $\frac{1}{2}n(n^2 + 1)$,同时外层行列上数字和也等于幻和。

46	1	2	3	42	41	40
45	35	13	14	32	31	5
44	34	28	21	26	16	6
7	17	23	25	27	33	43
12	20	24	29	22	30	38
11	19	37	36	18	15	39
10	49	48	47	8	9	4

图 1 用镶边法构造 7 阶同心幻方

2.2 幻方群

首先给出幻方群的定义:

定义 4^[7] 由若干个小的广义幻方组成的大幻方,叫做幻方群。

以图 2 为例说明幻方群的一般作法。图 2 是由 9 个 4 阶广义幻方构成的 12 阶幻方,这种幻方叫做 4 阶 3 级幻方群。把 1 ~ 144 这些数按序每 16 个数作一个 4 阶广义幻方。把第 g 组数作成的广义幻方当成 g 作 3 阶幻方,则得 4 阶 3 级幻方群。一般的,要做 r 阶 s 级幻方群,先把 $1 \sim (rs)^2$ 的自然数按顺序分成 s^2 组,每组 r^2 个数。第 g 组数是 $(g - 1)r^2 + 1, \dots, (g - 1)r^2 + gr^2 - 1, gr^2$ 此时 $g \in \{1,2,\dots, s^2\}$ 。然后,先把每组数作成 一个 r 阶广义幻方,再把第 g 组数作成的广义幻方当成 g 作 s 阶幻方,就可以得到 r 阶 s 级幻方群。

125	124	120	113	13	12	8	1	93	92	88	81
114	119	123	126	2	7	11	14	82	87	91	94
115	118	122	127	3	6	10	15	83	86	90	95
128	121	117	116	16	9	5	4	96	89	85	84
45	44	40	33	77	76	72	65	109	108	104	97
34	39	43	46	66	71	75	78	98	103	107	110
35	38	42	47	67	70	74	79	99	102	106	111
48	41	37	26	80	73	69	68	112	105	101	100
61	60	56	49	141	140	136	129	29	28	24	17
50	55	59	62	130	135	139	142	18	23	27	30
51	54	58	63	131	134	138	143	19	22	26	31
64	57	53	52	144	137	133	132	32	25	21	20

图 2 4 阶 3 级幻方群

由上述方法所作的 r 阶 s 级幻方群可以看成 一个 $r \times s$ 阶方阵,易证明,这个方阵也是一个大的幻方^[6]。

证明:记第 g 组广义幻方的每行每列和对角线上

的 r 个数的和为 $\frac{1}{r} \{ [(g-1)r^2 + 1] + \dots + gr^2 \} = gr^3 - \frac{1}{2}r^3 + \frac{1}{2}r$, 任取 $r \times s$ 阶大方阵的一行或一列或一对角线, 设其上的数属于第 g_1, g_2, \dots, g_s 组, 则 $\sum_{i=1}^s g_i = H_s = \frac{1}{2}s(s^2 + 1)$ 。于是可得各数之和为: $\sum_{i=1}^s (g_i r^3 - \frac{1}{2}r^3 + \frac{1}{2}r) = \frac{1}{2}s(s^2 + 1)r^3 - \frac{1}{2}sr^3 + \frac{1}{2}sr = \frac{1}{2}sr(s^2 r^2 + 1) = H_{sr}$ 。

综上所述可以看出, 首先用镶边法构造的仍意阶同心幻方在去掉一圈或者数圈后仍然是个同心幻方, 因此用镶边法构造的幻方较为稳定, 且避免了文献[8~11]中传统幻方构造方法导致的问题, 即传统幻方变换后上下和左右的元素连续性使得置乱的图像像素相关性较大。其次用 s^2 个 r 阶同心幻方构造的 r 阶 s 级幻方群也可以看成是一个幻和为 $\frac{1}{2}sr(s^2 r^2 + 1)$ 的大广义幻方, 下面将根据这个基本算法设计相关算法。

2.3 改进后的算法

文中对传统幻方图像置乱算法作出的改进主要基于两点: 第一, 对传统幻方构造时导致的特性进行了改进, 文中采用镶边法构造同心幻方, 避免了传统幻方构造时产生的元素位置的连续性, 而这种连续性恰好给攻击者提供了破译的理论基础; 第二, 文中采用幻方群的做法, 增大了密钥空间, 并提高了置乱度。本质上, 文中用幻方群对图像进行置乱的算法相当于传统幻方对图像进行双重迭代置乱的效果。一方面, 文中构造的 r 阶 s 级幻方群可以看成是一个大的 s 阶同心幻方; 另一方面, 这个大幻方由 s^2 个 r 阶小同心幻方组成, 这样先对 s^2 个 r 阶同心幻方进行变换, 再对大的 s 阶同心幻方进行迭代变换, 最后对整个图像进行置乱, 形成双重迭代置乱。基于上述分析, 文中提出如下置乱算法。

加密算法步骤:

1. 记未置乱图像的数字矩阵为 $Q_{n \times n}$, 其中 $n = r \times s$; 用镶边法构造一个 r 阶 s 级的幻方群记为 $P_{n \times n}$, 使 Q 与 P 的元素一一对应, 即有 q_{ij} 与 p_{ij} 一一对应。对于上述幻方群 $P_{n \times n}$, 可以将其看成一个 s 阶幻方, 该幻方由

s^2 个 r 阶小幻方组成, 分别记为 g_1, g_2, \dots, g_{s^2} ;

2. 在 $P_{n \times n}$ 中, 对于 r 阶幻方 g_1 , 其中的任意元素 $g[i][j]$, $i = 0, 1, 2, \dots, r-1$, $j = 0, 1, 2, \dots, r-1$, 若 $g[i][j] = 1$, 则 $g[i][j] = r^2$, 否则 $g[i][j] = g[i][j] - 1$;

3. 对于 g_t , $t = 2, 3, \dots, s^2$, 按照第2步进行变换有, 若 $g[i][j] = (t-1)r^2$, 则 $g[i][j] = tr^2 - 1$; 记此时变换后的矩阵为 $P_{n \times n}^{(1)}$;

4. 将 $P_{n \times n}^{(1)}$ 重复第2、3步 N_1 次, 其中 $N_1 \in \{1, 2, \dots, r^2 - 1\}$, 将经过此变换得到的矩阵记为 $P_{n \times n}^{(N_1)}$, 对 $Q_{n \times n}$ 做相同的变换; 则可得到与 $P_{n \times n}^{(N_1)}$ 相对应的 $Q_{n \times n}^{(N_1)}$;

5. 对于 $P_{n \times n}^{(N_1)}$ 的 g_t 组, 其中 $t = \{1, 2, \dots, s^2\}$, 若 $g_t = g_1$, 则 $g_t = g_{s^2}$, 否则 $g_t = g_{t-1}$;

6. 将步骤5重复 N_2 次, 其中 $N_2 \in \{1, 2, \dots, s^2 - 1\}$, 则经此步骤变换的数字矩阵记为 $P_{n \times n}^{(N_1 N_2)}$;

7. 对 $Q_{n \times n}^{(N_1)}$ 按步骤5、6做相同变换, 则得到与 $P_{n \times n}^{(N_1 N_2)}$ 对应的 $Q_{n \times n}^{(N_1 N_2)}$, 至此, 图像置乱完毕, 置乱后的图像即为 $Q_{n \times n}^{(N_1 N_2)}$ 。

解密算法步骤:

8. 将 $Q_{n \times n}^{(N_1 N_2)}$ 重复步骤7 总共 $(s^2 - N_2)$ 次, 即可得到 $Q_{n \times n}^{(N_1)}$;

9. 将 $Q_{n \times n}^{(N_1)}$ 重复步骤4 总共 $(r^2 - N_1)$ 次, 即可得到 $Q_{n \times n}$, 此时原始图像恢复。

3 实验结果及分析

文中针对标准 256×256 图像 Lena 进行仿真实验, 分别采用文中改进的算法和传统幻方置乱算法进行对比。结果如图3~5所示。

由实验结果可以看出, 图3是标准的Lena图像 (256×256), 图4是传统幻方置乱1024次的结果, 图5是改进的算法迭代 $N_1 + N_2 = 1024$ 次的结果。

由此可见, 在相同置乱次数下, 图4因为传统幻方构造时图片上下和左右像素点位置连续的特点可以依稀看到原图轮廓, 而图5对原算法置乱图像的连续性问题有了明显改进, 且置乱效果远好于传统幻方置乱



图3 原图

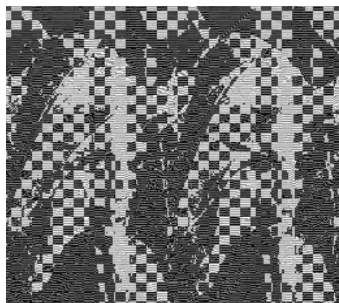


图4 原算法置乱1024次

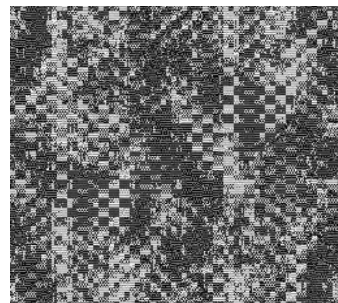


图5 改进算法 $N_1 = 13N_2 = 1011$

的效果。文中根据文献[12]中提出的图像置乱效果评价方法对图 4 和图 5 的置乱度进行了计算,结果如表 1 所示:

表 1 置乱度比较

传统幻方置乱算法置乱度	文中算法置乱度
0.679655	0.805802

从表中可以看出,文中算法的置乱度明显高于传统幻方算法的置乱度,说明本算法极大地降低了相邻像素间的相关性,并且扩散效果更好。在文献[7,8]等许多与幻方结合的加密算法中,基本都是采用传统的幻方置乱,如果能用本算法替换原有的传统幻方置乱算法,那加密效果应该更好。

4 安全性分析

文中算法分为两步:把幻方群看成 s^2 个 r 阶小同心幻方组成,这样先对 s^2 个 r 阶同心幻方进行变换,再对幻方群进行变换,然后用变换后的矩阵对图像进行双重迭代置乱。在还原图像时,不仅要知道构成 n 阶方阵的 (r,s) 构造的 r 阶和 s 阶幻方,而且还要知道置乱次数 N_1 和 N_2 。明显的,本算法构造 r 阶 s 级的幻方群时, r 与 s 的选择并不唯一,例如文中未加密图像为 256 阶方阵,其 (r,s) 可以选择有序对: $(4,64)$ 、 $(8,32)$ 、 $(16,16)$ 、 $(32,8)$ 、 $(64,4)$,设此时 m 为 (r,s) 可选择的有序对的个数。而文中 r 阶和 s 阶同心幻方的个数至少为 $(6(c_{2r-3}^{r-1})^2 + 2c_{2r-3}^{r-1}c_{2r-3}^r)(6(c_{2s-3}^{s-1})^2 + 2c_{2s-3}^{s-1}c_{2s-3}^s)^{[13]}$ 种。

用传统幻方置乱 n 阶 $(n=r \times s)$ 数字矩阵的图像个数为 $n^2 - 1$,而本算法置乱图像的个数至少为 $m(s^2 - 1)(r^2 - 1)(6(c_{2r-3}^{r-1})^2 + 2c_{2r-3}^{r-1}c_{2r-3}^r)(6(c_{2s-3}^{s-1})^2 + 2c_{2s-3}^{s-1}c_{2s-3}^s)$,即密钥空间数量级达到 $O(N^4)$,远远大于传统幻方图像置乱算法的密钥空间 $O(N^2)$ 。由此可见,本算法的密钥随机性更大、安全性更高并且加密效果更好。

5 结束语

图像置乱是图像加密领域中重要的一个研究方

向,文中针对传统幻方置乱加算法存在的问题提出了基于幻方群的图像置乱算法。该算法首先用镶边法构造同心幻方,然后再用同心幻方构造幻方群,对图像进行双重迭代。

实验表明,本算法对传统幻方置乱图像的连续性问题有了明显的改进,同时密钥空间得到很大改善,且置乱效果更好。

文中算法没有考虑置乱时造成的块效应,这也是今后有待改进的地方。同时将该算法与其他算法有效地结合也将是未来的研究方向之一。

参考文献:

[1] 司银女,康宝生. 基于改进的 Arnold 变换的数字图像置乱[J]. 计算机技术与发展,2008,18(2):74-79.

[2] 丁伟,齐东旭. 数字图像变换及信息隐藏及伪装技术[J]. 计算机学报,1998(9):838-843.

[3] Ding Wei, Yan Weiqi, Qi Dongxu. Digital image scrambling[J]. Progress in Natural Science,2001,11(6):456-460.

[4] Zhang Meng, Wang Fanzhen. Chaotic Video Encryption Algorithm Based on Baker Map[J]. Journal of Image and Graphics,2006,11(9):1328-1333.

[5] Li Shujun, Zheng Xuan. On the security of an image encryption method[C]//Proc of IEEE ICIP. [s.l.]:[s.n.],2002.

[6] 吴鹤龄. 幻方及其他-娱乐数学经典名题[M]. 北京:科学出版社,2004.

[7] 舒文中. 幻方[M]. 广州:广东科技出版社,1991.

[8] 李太勇,吴江. 一种基于混沌序列和幻方变换的数字图像加密算法[J]. 网络安全技术与应用,2006(5):90-92.

[9] 陈巧琳,廖晓峰,陈勇,等. 改进的基于混沌序列的幻方变换图像加密[J]. 计算机工程与应用,2005(22):138-139.

[10] 王秀丽,宁正元. 基于奇幻方的数字图像加密算法[J]. 闽江学院学报(自然科学版),2006,27(2):57-59.

[11] 王冬梅. 奇数阶幻方变换数字图像的准周期[J]. 浙江工业大学学报,2005,33(2):292-294.

[12] 田红鹏. 图像置乱效果盲评价的灰色块分析方法[J]. 计算机工程与应用,2009,45(34):171-173.

[13] 郑格于. 同心幻方的历史、构造及特性[J]. 武当学刊(自然科学版),1993(2):1-13.

(上接第 118 页)

[10] Case J, Fedor M, Schoffstall M, et al. Simple network management protocol[S]. RFC 1157, IEIF, 1990.

[11] Shreedhar M, Varghese G. Efficient fair queueing using deficit round robin[C]//Proc. of ACM SIGCOMM 95. Cambridge, MAUSA:[s.n.],1995:231-242.

[12] 刘彪. NS-2 模拟器及其教育应用[J]. 计算机教育,2007(10):164-166.

[13] Man H Y, Xu L Y, Li Z J. End-to-End QoS Implement by DiffServ and MPLS[C]//Canadian Conference. Canadian:[s.n.],2004:641-644.

幻方群在图像置乱中的应用

作者: [刘颖](#), [刘健波](#)
作者单位: [四川大学 视觉合成图形图像技术国家重点学科实验室, 四川 成都 610064](#)
刊名: [计算机技术与发展](#)
英文刊名: [Computer Technology and Development](#)
年, 卷(期): 2012(9)

本文链接: http://d.g.wanfangdata.com.cn/Periodical_wjfz201209032.aspx