DOI:10.13374/j.issn1001-053x.2012.12.017

第34卷 第12期　北京科技大学学报　Vol. 34 No. 12
2012年 12月　Journal of University of Science and Technology Beijing　Dec. 2012

基于三维仿射变换的数字图像置乱算法

文昌辞[1)] ✉　王沁[1)]　丁华[2)]　苗晓宁[3)]　陶春生[4)]

1) 北京科技大学计算机与通信工程学院，北京 100083　2) 二炮692厂军代室，泸州 646605
3) 空军二院283厂军代室，北京 100854　4) 空军218厂军代室，北京 100009
✉通信作者，E-mail: wenchangci@126.com

摘　要　针对数字图像的特点，基于有限整数域上的二维置乱变换、仿射变换和整数提升变换，提出了适用于任意大小、任意长宽比图像的三维置乱加密算法. 考虑了变换矩阵中部分参数取负整数或小数的可行性，明确给出了参数的具体设置方法. 该算法引入实数作为参数，扩展了参数选择范围; 置乱像素位置的同时改变像素值，改善了置乱效果，加大了置乱周期，提高了数字图像的安全性.

关键词　密码术; 算法; 图像处理; 三维; 仿射变换
分类号　TP309.7

Image scrambling algorithm based on three-dimensional affine transformations

WEN Chang-ci[1)] ✉, *WANG Qin*[1)], *DING Hua*[2)], *MIAO Xiao-ning*[3)], *TAO Chun-sheng*[4)]

1) School of Computer and Communication Engineering, University of Science and Technology Beijing, Beijing 100083, China
2) Second Artillery 692 Factory Office, Luzhou 646605, China　3) Air Force 283 Factory Office, Beijing 100854, China
4) Air Force 218 Factory Office, Beijing 100009, China
✉Corresponding author, E-mail: wenchangci@126.com

ABSTRACT　According to the features of digital images, a kind of three-dimensional scrambling and encryption algorithm was proposed based on two-dimensional scrambling transformations in a finite integer domain, affine transformations, and integer lifting transformations. This algorithm applies to images with any length and width or at any length-to-width ratio. The feasibility that some parameters of the transformation matrix are negative integers or decimals is taken into account, and the method of parameter setting is explicitly shown. Real number is used in the algorithm, which expands the space of parameters, scrambles the pixel positions and changes their values, makes the scrambling result better, increases the periodicity of scrambling, and improves the security of digital image transformations.

KEY WORDS　cryptography; algorithms; image processing; three-dimensional; affine transformations

传统加密算法如DES(数据加密标准)、IDEA(国际数据加密算法)和AES(高级加密标准)，针对一维数据流而设计，没有考虑数字图像具有数据量大、相关性强和冗余度高的特点，加密效率不高，不适用于加密数字图像. 在实际加密中，像素置乱是一种很高效的办法，它可以快速地破坏图像中原有的空间有序性和局部相关性，把图像变得杂乱无章、无法识别. 目前的置乱方法有猫映射变换[1-4]及其扩展[5-6]、二维非等长置乱变换[7]、面包师变换、幻方变换、魔方变换[8]、基于骑士巡游的置乱、基于随机数排序的置乱[9]、基于象素值排序的自适应置乱、基于线映射的置乱[10]、基于队列变换的置乱等. 以猫映射变换和二维非等长置乱变换为代表的矩阵变换能快速地将相邻像素分散开，像素的移动具有混沌特性，而且耗费的计算量很小. 基于猫映射变换、幻方变换和骑士巡游的置乱对图像的长宽比例有限制，这使得它们的适用范围有限. 文献[11]提出有限整数域上的拟仿射变换，在实现时用多个置乱变换相级联，实际上相当于进行多轮的普通置乱，它的优势是采用的仿射变换形式使得所有的像素点

收稿日期: 2011-11-24
基金项目: 装备预研重点基金资助项目(9140A04040308DZ1002)

均可能变换了位置,而猫映射变换和二维非等长置乱变换没有改变(0,0)处像素的位置,这可能成为包含置乱操作在内的整个算法的安全漏洞. 基于排序的置乱算法时间复杂度较高,而且为了存储对应的像素位置,可能还需要额外的存储空间,所以空间复杂度也较高.

1　置乱变换

基于有限整数域上的二维非等长置乱变换[7]、仿射变换和整数提升变换[11],提出一种新的置乱变换,记为三维类仿射变换.

定义 1　二维非等长仿射变换. 设 $x \in [0, M-1]$, $y \in [0, N-1]$, 若 (x, y) 映射为 (x', y') 满足 $\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix} + \begin{pmatrix} e \\ f \end{pmatrix} \bmod \begin{pmatrix} M \\ N \end{pmatrix}$, 其中 a、b、c、d、e 和 f 为非负整数且 $\begin{vmatrix} a & b \\ c & d \end{vmatrix} \neq 0$, 则称为二维非等长仿射变换. 特别地当 e 和 f 为 0 时,称为二维非等长置乱变换.

定义 2　三维类仿射变换. 设 x、y 和 z 为整数且 $x \in [0, M-1]$, $y \in [0, N-1]$, $z \in [0, L-1]$, 定义 (x, y, z) 映射为 (x', y', z') 的如下运算

$$\begin{pmatrix} x' \\ y' \\ z' \end{pmatrix} = \begin{pmatrix} a & b & c \\ d & e & f \\ g & h & l \end{pmatrix}\begin{pmatrix} x \\ y \\ z \end{pmatrix} + \begin{pmatrix} r \\ s \\ t \end{pmatrix} \bmod \begin{pmatrix} M \\ N \\ L \end{pmatrix} =$$

$$\begin{pmatrix} \lfloor ax + by + cz + 0.5 \rfloor \\ \lfloor dx + ey + fz + 0.5 \rfloor \\ \lfloor gx + hy + lz + 0.5 \rfloor \end{pmatrix} + \begin{pmatrix} \lfloor r + 0.5 \rfloor \\ \lfloor s + 0.5 \rfloor \\ \lfloor t + 0.5 \rfloor \end{pmatrix} \bmod \begin{pmatrix} M \\ N \\ L \end{pmatrix}$$

为三维类仿射变换,其中 a、b、c、d、e、f、g、h、l、r、s 和 t 为实数, M、N 和 L 为正整数, $\lfloor\ \rfloor$ 表示取整.

1.1　置乱参数设置

要将三维类仿射变换用于图像的置乱加密,必须使其为一一映射. 对参数进行适当设置,可分别得到以下四个式子:

$$\begin{pmatrix} x' \\ y' \\ z' \end{pmatrix} = \begin{pmatrix} a & 0 & 0 \\ c & e & 0 \\ g & h & l \end{pmatrix}\begin{pmatrix} x \\ y \\ z \end{pmatrix} + \begin{pmatrix} r \\ s \\ t \end{pmatrix} \bmod \begin{pmatrix} M \\ N \\ L \end{pmatrix}, \tag{1}$$

$$\begin{pmatrix} x' \\ y' \\ z' \end{pmatrix} = \begin{pmatrix} a & c & 0 \\ 0 & e & 0 \\ g & h & l \end{pmatrix}\begin{pmatrix} x \\ y \\ z \end{pmatrix} + \begin{pmatrix} r \\ s \\ t \end{pmatrix} \bmod \begin{pmatrix} M \\ N \\ L \end{pmatrix}, \tag{2}$$

$$\begin{pmatrix} x' \\ y' \\ z' \end{pmatrix} = \begin{pmatrix} 1+dnq & nq & 0 \\ d & 1 & 0 \\ g & h & l \end{pmatrix}\begin{pmatrix} x \\ y \\ z \end{pmatrix} + \begin{pmatrix} r \\ s \\ t \end{pmatrix} \bmod \begin{pmatrix} M \\ N \\ L \end{pmatrix}, \tag{3}$$

$$\begin{pmatrix} x' \\ y' \\ z' \end{pmatrix} = \begin{pmatrix} 1 & b & 0 \\ np & 1+bnp & 0 \\ g & h & l \end{pmatrix}\begin{pmatrix} x \\ y \\ z \end{pmatrix} + \begin{pmatrix} r \\ s \\ t \end{pmatrix} \bmod \begin{pmatrix} M \\ N \\ L \end{pmatrix}. \tag{4}$$

式中: a、e 和 l 为非零整数且 $\gcd(a, M) = \gcd(e, N) = \gcd(l, L) = 1$, c、g、h、r、s 和 t 为任意实数, n、b、d 为任意正整数; $\gcd(\ )$ 为求最大公因子; $q = M/\gcd(M, N)$, $p = N/\gcd(M, N)$.

1.2　一一映射证明

引理[7]　二维非等长置乱一一映射定理. 对于二维非等长置乱变换,如果对于所有不同为 0 的整数 l_1 和 l_2, 若以下两式不同时成立,则二维非等长置乱变换为一一映射.

$$|l_1 dM - l_2 bN| / |ad - bc| < M,$$
$$(ad - bc) \mid (l_1 dM - l_2 bN); \tag{5}$$
$$|l_1 cM - l_2 aN| / |ad - bc| < N,$$
$$(ad - bc) \mid (l_1 dM - l_2 bN). \tag{6}$$

定理 1　三维类仿射变换的一一映射定理. 如果把式(1)~(4)用于图像的置乱变换,其中 (x, y, z) 和 (x', y', z') 分别代表置乱前、置乱后的像素坐标和像素值,那么该置乱变换是一一映射.

证明:

(1) 对于式(1),任取两个不同位置的像素 (x_1, y_1, z_1) 和 (x_2, y_2, z_2), 只有两种情况: ① $x_1 \neq x_2$; ② $x_1 = x_2$ 但是 $y_1 \neq y_2$.

①当 $x_1 \neq x_2$ 时,因为 $\gcd(a, M) = 1$, 所以 $(ax_1 + \lfloor r + 0.5 \rfloor) \bmod M \neq (\lfloor r + 0.5 \rfloor + ax_2) \bmod M$, 因此 $(x_1', y_1') \neq (x_2', y_2')$, 即像素的坐标位置是一一映射.

②当 $x_1 = x_2$ 但 $y_1 \neq y_2$ 时, $y_1' = (ey_1 \bmod N + \lfloor cx_2 + 0.5 \rfloor + \lfloor s + 0.5 \rfloor) \bmod N$, $y_2' = (ey_2 \bmod N + \lfloor cx_2 + 0.5 \rfloor + \lfloor s + 0.5 \rfloor) \bmod N$. 因为 $\gcd(e, N) = 1$, 所以 $y_1' \neq y_2'$, 即像素坐标位置是一一映射.

③在 $(x, y) \to (x', y')$ 计算可逆的情况下,因为 $\gcd(l, L) = 1$, 所以 $z = (z' - \lfloor t + 0.5 \rfloor - \lfloor gx + hy + 0.5 \rfloor) \times l^{-1} \bmod L$, l^{-1} 为 l 在剩余类域 Z_L 中的模 L 乘法逆元,即像素值的计算也可逆.

综合①、②和③,可得出式(1)是一一映射. 同理可证,式(2)也是一一映射.

(2) 对于式(3),改变坐标位置的变换矩阵为以下二维非等长置乱变换:

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} 1+dnq & nq \\ d & 1 \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix} + \begin{pmatrix} r \\ s \end{pmatrix} \bmod \begin{pmatrix} M \\ N \end{pmatrix}.$$

对应于此时的二维非等长置乱变换,上文中的式(5)和式(6)可变换为

$$|l_1 - l_2 nqN/M| < 1, \tag{7}$$

$$|l_1 dM/N - l_2(1 + dnq)| < 1. \tag{8}$$

当 $l_1 = 0, l_2 \neq 0$ 时,式(8)不成立. 当 $l_1 \neq 0, l_2 = 0$ 时,式(7)不成立. 当 $l_1 \neq 0, l_2 \neq 0$ 时,如果 $l_1 = l_2 nqN/M$,则代入式(8)得 $|l_2| < 1$,显然不成立;如果 $l_1 \neq l_2 nqN/M$,则式(7)不成立. 所以对于所有不同为 0 的整数 l_1 和 l_2,式(7)和式(8)不同时成立,该二维非等长置乱变换是一一映射. 进一步容易得出:式(3)是一一映射. 同理,式(4)也是一一映射.

由(1)和(2)可知,上述四种置乱形式均是一一映射.

1.3 反置乱

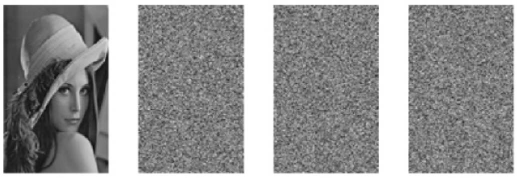
反置乱时不需要计算置乱恢复矩阵,只需要逐个像素根据坐标(x,y)正向计算出(x',y'),然后根据 $z = (z' - \lfloor t + 0.5 \rfloor - \lfloor gx + hy + 0.5 \rfloor) \times l^{-1} \bmod L$ 计算出密图中点(x',y')对应的原始像素值 z,就得到了(x,y,z)与(x',y',z')的一一对应关系.

1.4 置乱分析

目前已有的置乱算法大都不改变像素值,通过对明密文的像素直接进行比对就可能发现置乱规律,安全性较低. 文献[8]在三维空间上通过魔方变换来旋转置乱像素的比特位,文献[10]将像素之间的比特位重新组合,这些三维置乱算法虽然改变了像素值,但是由于计算机在处理每个比特位时实际上需要对整个像素进行操作,所以总的计算量很大. 本文的三维置乱在改变像素位置的同时略微增加计算量就能达到非线性地混合像素值的目的,不仅像素的位置被充分打乱而且密图的灰度直方图趋向于均衡化,所以它能更有效地抵御已知明文攻击. 同别的置乱算法一样,它也可以嵌入到图像压缩编码的过程中,在 DCT 域或 DWT 域对量化后系数进行置乱,以达到加密并压缩的目的.

2 实验及算法评价

为了实验长宽不等图像的像素置乱效果,裁减 256 色的标准测试图像 lena(256×256)得到 244×178 的图 1(a),此时 $M = 244, N = 178, L = 256$. 用 VC++ 编写代码进行三维置乱,当 $a = 7$, $b = 0$, $c = 0$, $d = 21$, $e = 5$, $f = 0$, $g = 21$, $h = 37$, $l = 51$, $r = 36$, $s = 28$, $t = 71$ 时,置乱得到图 1(b). 当 $a = 7$, $b = 0$, $c = 0$, $d = 20.34568$, $e = 5$, $f = 0$, $g = 21.9537$, $h = 37.678763$, $l = 51$, $r = 36.557546$, $s = 28.459297$, $t = 71.554$ 时,置乱得到图 1(c). 当 $a = 7$, $b = 0$, $c = 0$, $d = 20.34568$, $e = 5$, $f = 0$, $g = 21.9537$, $h = 37.678763$, $l = 17$, $r = 36.557546$, $s = 28.459297$, $t = 72.6$ 时,置乱得到图 1(d). 继续裁减标准测试图像 lena(256×256)得到一系列新的图像,并使用下述设置进行置乱,置乱效果对比情况见表 1 和表 2.



(a)　(b)　(c)　(d)

图 1　像素置乱效果. (a) 明文; (b) 密文 1; (c) 密文 2; (d) 密文 3

Fig. 1　Effect of pixel scrambling: (a) plaintext; (b) Ciphertext 1; (c) Ciphertext 2; (d) Ciphertext 3

①设置二维非等长置乱变换参数:$a = 7, b = 0, c = 20, d = 5$,记为"二维置乱 1".

②设置二维非等长仿射变换参数:$a = 7, b = 0, c = 20, d = 5, e = 36, f = 28$,记为"二维置乱 2".

③设置三维类仿射变换参数:$a = 7, b = 0, c = 0, d = 20, e = 5, f = 0, g = 21, h = 37, l = 51, r = 36, s = 28, t = 71$,记为"三维置乱 1".

④设置三维类仿射变换参数:$a = 7, b = 0, c = 0, d = 20.34568, e = 5, f = 0, g = 21.9537, h = 37.678763, l = 51, r = 36.557546, s = 28.459292, t = 71.6$,记为"三维置乱 2".

2.1 置乱周期

图像中像素值的状态数是有限的,所以在置乱若干次以后,图像终究会回复到初始状态. 置乱次数可以作为图像加密算法的密钥之一,置乱周期越长,则用于图像加密的密钥空间就越大,算法抵御穷举攻击的能力就越强. 在 M 相同、N 也相同的情况下,由于二维矩阵置乱相当于在 $M \times N$ 的二维空间中进行置乱,而本文的三维算法在改变像素位置的同时还改变了像素值,相当于在 $M \times N \times L$ 的三维空间中进行置乱,这种置乱是在 $M \times N$ 二维空间中进行相同置乱的同时还伴随着另一维的置乱,所以置乱周期远大于二维置乱的周期. 持续置乱以恢复出原始图像所需的置乱次数可反映这一现象,二维置乱、三维置乱所需的置乱次数见表 1.

2.2 峰值信噪比

把置乱加密看成是往明文图像上叠加噪声,计算峰值信噪比 PSNR,信噪比越小则置乱加密效果越好. $\mathrm{PSNR} = 10\lg(\psi_{\max}^2/\mathrm{MSE})$,其中 $\psi_{\max}$ 为像素的最大亮度值,$\mathrm{MSE} = (MN)^{-1} \sum \sum (p_{ij} - c_{ij})^2$,其中 p_{ij} 和 c_{ij} 分别为明密文像素点(i,j)的值. 计算得出的峰值信噪比见表 1. 从表中数据可以看出,相对于

表 1　置乱次数和峰值信噪比

Table 1　Scrambling number and peak signal-to-noise ratio

图像大小	置乱次数				峰值信噪比			
	二维置乱 1	二维置乱 2	三维置乱 1	三维置乱 2	二维置乱 1	二维置乱 2	三维置乱 1	三维置乱 2
244 × 178	660	660	84480	337920	10.7354	10.7805	8.4580	8.4307
193 × 161	264	264	473088	473088	10.9703	10.9873	8.5574	8.4872
251 × 251	125	125	16000	4016000	10.7774	10.7706	8.5921	8.5954
227 × 151	8475	8475	1084800	1084800	10.3306	10.3475	8.3665	8.4354
195 × 201	132	132	33792	101376	10.3763	10.3471	8.4003	8.3680
195 × 199	132	132	33792	33792	10.4197	10.3612	8.4163	8.3424

二维矩阵置乱,本文的三维置乱能获得更好的加密效果.

2.3　信息熵

设 v_i 表示 L 级灰度图像的第 i 个灰度值,$p(v_i)$ 表示图像中具有第 i 个灰度值的像素所占的比例,图像的信息熵 H 定义为 $H = -\sum p(v_i)\log_2 p(v_i)$. 信息熵可以度量图像中灰度值的分布情况,灰度分布越均匀,图像信息熵就越大,反之信息熵就越小. 计算得出的信息熵见表 2. 可以看出,二维矩阵置乱后信息熵不变,而本文的三维置乱非线性地改变了像素值,灰度直方图趋向于均衡化,导致密图的信息熵增大了,所以算法能更有效地抵抗已知明文攻击.

表 2　信息熵和明密文图像相似度

Table 2　Information entropy and similarity between two images

图像大小	信息熵				明密文图像相似度			
	二维置乱 1	二维置乱 2	三维置乱 1	三维置乱 2	二维置乱 1	二维置乱 2	三维置乱 1	三维置乱 2
244 × 178	7.5432	7.5432	7.5432	7.9952	0.5238	0.5288	0.1956	0.1905
193 × 161	7.5199	7.5199	7.5199	7.9940	0.5504	0.5521	0.2163	0.2035
251 × 251	7.5702	7.5702	7.5702	7.9966	0.5628	0.5621	0.2768	0.2774
227 × 151	7.5750	7.5750	7.5750	7.9941	0.5077	0.5096	0.2262	0.2384
195 × 201	7.5833	7.5833	7.5833	7.9949	0.5124	0.5091	0.2315	0.2257
195 × 199	7.5816	7.5816	7.5816	7.9948	0.5140	0.5075	0.2292	0.2160

2.4　明密文图像相似度

设明文图像为 $P(M \times N)$,密文图像为 $C(M \times N)$,则两幅图像的相似度为

$$\mathrm{XSD} = 1 - \sum\sum(c_{ij} - p_{ij})^2 / \sum\sum p_{ij}^2.$$

两幅图像的相似度越小则差别越大. 计算出的明密文图像相似度见表 2. 可以看到,本文三维置乱的明密文相似度比二维置乱的小.

从相邻像素相关性、图像自相关度、不动点比和灰度平均变化值的实验结果也可以看出,本文提出的三维置乱视觉效果优于二维置乱. 具体实验数据略.

2.5　计算复杂度

在实际中,可限制 g 和 h 小数部分的二进制形式取 00、01、10 或 11,r、s 和 t 小数部分的二进制形式取 0 或 1,使得置乱时乘积计算的复杂度相当于定点乘. 假设模运算比定点乘法和加法的计算量大得多,以模运算为基本操作. 对于 $M \times N$ 大小的图像,采用二维置乱时,平均时间复杂度为 $O(2MN)$; 用三维类仿射置乱进行置乱时,平均时间复杂度为 $O(3MN)$. 反置乱时不需要计算置乱恢复矩阵,也不需要考虑置乱周期的大小,较之于正向变换,仅多一个求逆元 l^{-1} 的过程,而且对一幅图像只需求一次. 因此反置乱的时间复杂度与置乱时近似相等.

进行二维置乱和反置乱时,需要一个同图像大小 $M \times N$ 相等的辅助空间用于存储置乱后的像素. 按本文的算法进行三维置乱和反置乱时,虽然是相当于在 $M \times N \times L$ 个像素的三维空间中进行置乱,但是也只需要 $M \times N$ 个像素的空间用于存储置乱结果,所以空间复杂度也为 $O(2MN)$.

3　结论

(1) 提出了一种适用于任意大小、任意宽高比

图像的三维置乱算法，考虑了变换矩阵中部分参数取负整数或小数的可行性，明确给出了参数的具体设置方法.

(2) 该算法引入实数作为参数，扩展了参数选择范围; 置乱前不需要将像素按三维的形式重新排列，运算量不大; 置乱像素位置的同时改变像素值，改善了置乱效果，扩大了置乱周期，提高了密文图像的安全性.

(3) 从置乱周期、峰值信噪比、信息熵、明密文图像相似度、计算复杂度等多个角度综合比较可以得出，本文提出的三维置乱优于二维置乱.

(4) 从原理设计上来说，由于该算法融合了二维非等长置乱变换和拟仿射变换的优点，同时没有基于排序的置乱复杂度高的缺点，并且还能快速地搅匀像素值，所以设计加密算法时应优先选用. 进一步的研究内容是将混沌系统与本置乱算法结合起来，增加代换和扩散操作.

参 考 文 献

[1] Shang Z W, Ren H E, Zhang J. A block location scrambling algorithm of digital image based on Arnold transformation // *The 9th International Conference for Young Computer Scientists*. Washington: IEEE Press, 2008: 2942

[2] Chen D M. A feasible chaotic encryption scheme for image // 2009 *International Workshop on Chaos-Fractals Theories and Applications*. Washington: IEEE Press, 2009: 172

[3] Xu J B, Liang W, Zhu L W, et al. A new non-linear cross-encryption method for video images // 2009 *International Forum on Information Technology and Applications*. Washington: IEEE Press, 2009: 239

[4] Zhang W, Zhu Z L, Yu H. An image encryption scheme based on chaotic maps // 2009 *International Workshop on Chaos-Fractals Theories and Applications*. Washington: IEEE Press, 2009: 195

[5] Zhai Y K, Lin S Y, Zhang Q. Improving image encryption using multi-chaotic map //2008 *Workshop on Power Electronics and Intelligent Transportation System*. Washington: IEEE Press, 2008: 143

[6] Fan J, Huang F. Fan transform in image scrambling encryption application // *International Conference on Wireless Communications & Signal Processing*. Washington: IEEE Press, 2009: article No. 5371644

[7] Shao L P, Qin Z, Gao H J, et al. 2-dimension non equilateral image scrambling transformation. *Acta Electron Sin*, 2007, 35(7): 1290
(邵利平，覃征，高洪江，等. 二维非等长图像置乱变换. 电子学报，2007，35(7): 1290)

[8] Zhao L L, Fang Z L, Gu Z C. A novel algorithm of digital image scrambling and encryption based on magic cube transformation. *J Optoelectron Laser*, 2008, 19(1): 131
(赵立龙，方志良，顾泽苍. 一种新的基于魔方变换的数字图像置乱加密算法. 光电子·激光，2008，19(1): 131)

[9] Liu T, Min L Q. Discussion of a chaotic image scrambling algorithm based on sort transformation. *J Univ Sci Technol Beijing*, 2010, 32(5): 673
(刘婷，闵乐泉. 对一种基于排序变换的混沌图像置乱算法的商榷. 北京科技大学学报，2010，32(5): 673)

[10] Li J, Feng Y, Yang X Q. An improved image encryption scheme based on line maps // *Fifth International Conference on Information Assurance and Security*. Washington: IEEE Press, 2009: 605

[11] Zhu G B, Cao C X, Hu Z Y, et al. An image scrambling and encryption algorithm based on affine transformation. *J Comput Aided Des Comput Graphics*,2003, 15(6): 711
(朱桂斌，曹长修，胡中豫，等. 基于仿射变换的数字图像置乱加密算法. 计算机辅助设计与图形学学报，2003，15(6): 711)