Arnold 反变换的一种新算法*

孔 涛+, 张 亶

(浙江大学 数学系,浙江 杭州 310027)

A New Anti- Arnold Transformation Algorithm

KONG Tao+, ZHANG Dan

(Department of Mathematics, Zhejiang University, Hangzhou 310027, China)

+ Corresponding author: E-mail: kongtao2002@eyou.com, http://www.zju.edu.cn

Received 2003-12-16; Accepted 2004-04-27

Kong T. A new Anti-Arnold transformation algorithm. *Journal of Software*, 2004,15(10):1558~1564.
http://www.jos.org.cn/1000-9825/15/1558.htm

Abstract: Arnold transformation is applied widely in digital image encryption because of its periodicity. But if its periodicity is used in the course of image decryption, it will waste lots of time. So this paper offers a new anti-Arnold transformation algorithm. The algorithm gets anti-Arnold transformation by solving equation groups. The application of Arnold transformation from square image to rectangle image is generalized and its application on image encryption expanded. At the same time, the anti-Arnold transformation from 2-dimension to *m*-dimension is also generalized.

Key words: digital image; image encryption; image scramble; Arnold transformation; digital watermark

摘 要: Arnold 变换因其具有周期性,在图像加密方面得到了广泛的应用.但在解密过程中,若要利用其周期性,则显得很费时,因此提出了一种新的 Arnold 反变换算法.该算法通过求解方程组来求得反变换.在此基础上,把二维 Arnold 变换用在正方形图像的情形推广到一般的矩形图像,即图像矩阵不是方阵的情况,扩大了其在图像加密中的应用.同时,从理论上又把二维 Arnold 反变换推广到了 *m* 维 Arnold 反变换.

关键词: 数字图像;图像加密;图像置乱;Arnold 变换;数字水印

中图法分类号: TP309 **文献标识码**: A

在数字图像的加密过程中,一般是先将原图像进行置乱变换.图像置乱技术是一种重要的图像加密技术[1].人们用得较多的置乱技术是基于 Arnold 变换、幻方变换、分形 Hilbert 曲线[2]、Tangram 算法、IFS 模型[3]、Conway 游戏、Gray 码变换、广义 Gray 码变换[4]等方法.随着数字水印技术的兴起[5~9],置乱技术在通过置乱来分散错误比特的分布从而提高数字水印的鲁棒性方面又有了新的应用.其中 Arnold 变换算法简单且具有周期性[10~13],所以在数字水印方面得到了很好的应用[14](Arnold 变换是 V.I. Arnold 在研究环面上的自同态时提出的,后来把它应用到数字图像上).Arnold 变换的周期性是一个很好的性质,当反复应用 Arnold 变换时,在某一时刻

* Supported by the National Natural Science Foundation of China under Grant No.60202002 (国家自然科学基金)

作者简介: 孔涛(1979－)男,山东曲阜人,硕士,主要研究领域为小波分析及偏微分方程在图像中的应用,图像加密.张亶(1971－)男,博士,副教授,主要研究领域为偏微分方程在图像中的应用.

© 中国科学院软件研究所 http://www.jos.org.cn

就能恢复原图.因为Arnold变换的周期性与图像大小有关[11],如果我们利用它的周期性来恢复原图,势必要等很长时间.一般图像阶数与 Arnold 变换的周期并不成正比[11],而在实际中,把 Arnold 变换应用在数字水印方面时,应尽量减少它所带来的花费(时间和计算量),希望 Arnold 变换的周期越短越好.因此,在设计数字水印图像大小时,应尽量选择 Arnold 变换周期较小的图像阶数,这就限制了数字水印图像的选择范围,而且选择前还需先计算出它们的周期[12],非常麻烦.这就促使我们去寻找Arnold变换的反变换.与此有关的是通过引入遍历矩阵的概念来进行图像解密[15].本文提供了一种推导 Arnold 反变换的方法,该方法基于数学的严谨推理.如果原图像通过 Arnold 变换达到某一置乱状态时需要迭代 N 步,则用该算法随时都能从该置乱状态迭代同样的步数来很快地恢复出明文(即要传输的原图像),无须计算该图像的周期.最后,在此基础上把二维 Arnold 反变换推广到了 m 维反 Arnold 变换.

1 算法推导过程

该算法建立在数学推理的基础上,通过求 Arnold 变换的反函数从而求得 Arnold 反变换.Arnold 变换的定义为

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} (\mathrm{mod}\, n),$$

其中,(x,y)是原图像的像素点,(x',y')是变换后新图像的像素点,n 是图像阶数,即图像的大小,一般考虑正方形图像.下面就是我们推导正方形图像 Arnold 反变换的过程.在该过程中,(x',y')和 n 是已知的,(x,y)是未知的,即我们所要求的.Arnold 变换的等价形式可以写成:

$$\begin{cases} x' = (x+y)(\mathrm{mod}\, n) \\ y' = (x+2y)(\mathrm{mod}\, n) \end{cases}.$$

这意味着 $\exists p,q \in \mathrm{Z}$ (Z 为整数),有

$$\begin{cases} \dfrac{x+y-x'}{n} = p \\ \dfrac{x+2y-y'}{n} = q \end{cases},$$

即

$$\begin{cases} x+y = np+x' \\ x+2y = nq+y' \end{cases} \tag{1}$$

本来这是个病态方程组,但是在图像处理的背景下,却能得到它的唯一解,因为隐含着这样的条件(这样写是为了与编程语言数组表示方法相一致,同时也不失一般性):

$$\begin{cases} 0 \le x \le n-1 \\ 0 \le y \le n-1 \\ 0 \le x' \le n-1 \\ 0 \le y' \le n-1 \end{cases} \tag{2}$$

由上面的条件可得到:

$$\begin{cases} 0 \le x+y \le 2n-2 \\ 0 \le x+2y \le 3n-3 \end{cases} (x',y'),$$

由不等式的性质,有

$$\begin{cases} 0 \le x+y-x' \le 2n-2 \\ 0 \le x+2y-y' \le 3n-3 \end{cases},$$

即

$$\begin{cases} 0 \le np \le 2n-2 \\ 0 \le nq \le 3n-3 \end{cases},$$

所以 p 只能取 0 和 1,q 只能取 0,1,2.由此得到了 $C_2^1 \times C_3^1 = 6$ 个方程组.如果把这 6 种情况全都罗列出来并进行逐

© 中国科学院软件研究所 http://www.jos.org.cn

一求解,则是非常麻烦的,尤其对于更高维情况更是繁琐,所以应充分利用条件来具体确定 p 和 q 的值.下面是分析求解过程.

第 1 种情况:当 $p=0$ 时,由式(1)得 $x+y=x'$,所以 $0\le x+y=x'\le n-1$,进一步由不等式的性质和式(2),得到 $0\le x+y+y\le 2n-2$.又因为 $x+2y=nq+y'$,并且 $0\le y'\le n-1$,所以 q 只能取 0 和 1,不能取到 2.因此得到两个方程组,它们分别是

$$\begin{cases}x+y=x'\\ x+2y=y'\end{cases},\ \begin{cases}x+y=x'\\ x+2y=n+y'\end{cases}.$$

解这两个二元一次方程组就可得到 x,y 的值,即在此 x,y 是未知的,而 n,x',y' 是已知的.所得到的解集只是反变换解集的子集,所以还应考虑另一种情况.

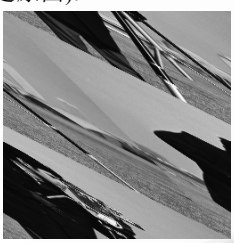
第 2 种情况:当 $p=1$ 时,由式(1)得 $x+y=n+x'$,所以 $n\le n+x'=x+y\le 2n-1$,进一步我们得到 $n\le x+y+y\le 3n-2$.又因为 $x+2y=nq+y'$ 并且 $0\le y'\le n-1$,所以 q 只能取 1 和 2,不能取到 0.因此又得到两个方程组,它们分别是

$$\begin{cases}x+y=n+x'\\ x+2y=n+y'\end{cases},\ \begin{cases}x+y=n+x'\\ x+2y=2n+y'\end{cases}.$$

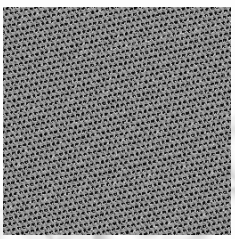
解这两个二元一次方程组就可以得到 x,y 的值.两种情况解集的并就是所求的反变换.在计算机上具体实现的时候,只需用 if 语句进行判断,使上面 4 个方程组的解在 $0\sim n-1$ 之间.我们不必担心所得到的解会逸出原来图像支集的范围,因为 Arnold 变换是一个双射,是可逆的,而我们所求的正是它的逆映射.归根结底,都是因为它有很好的代数结构,有严谨的数学理论做保证.因为正、反变换是相对的,所以可以把本文算法定义为 Arnold 变换,把原来的 Arnold 变换当作 Arnold 反变换.

2 实验结果

我们分两种情况来进行对比实验.第 1 种情况:先把原来的 Arnold 变换当做 Arnold 正变换进行实验,迭代了 50 次,抽取两幅图,如图 1 所示(其中原图是 256 的正方形图像),其中,图 1(a)为第 1 次迭代所得到的图像,图 1(b)为第 31 次迭代所得到的图像.接着,我们以第 50 次迭代后的图像为第 1 幅图像,用本文的算法进行迭代来恢复原图,抽取两幅图,如图 2 所示.其中,图 2(a)为第 49 次迭代所得到的图像,图 2(b)为第 50 次迭代恢复的图像(实际上是原图).



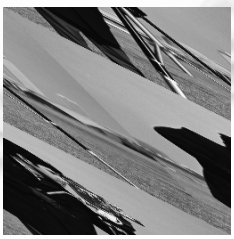
(a)



(b)

Fig.1

图 1



(a)

(b)

Fig.2

图 2

由上面的实验图可以看出,正变换的第 1 次迭代所得到的图像就是反变换的第 49 次迭代所得到的图像.由此可以得出一个有趣的结论:对一幅图像迭代 m 次后,在这过程中随机抽出第 r $(0\le r\le m)$ 次迭代后的图像,该图像正好是以原图迭代 m 次后作为原图进行反变换,其中第 k 次迭代后的图像,并且 $k+r=m$,也就是说,正变换的第 r 次迭代后的图像正好是反变换的第 $m-r$ 次迭代后的图像.

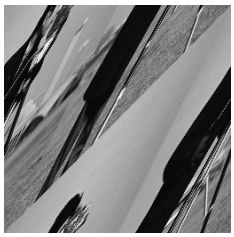
第 2 种情况:以本文的算法作为 Arnold 正变换,以原来的 Arnold 变换作为反变换进行迭代恢复原图.先是 Arnold 正变换的过程,迭代了 50 次,在这个过程中抽出了两幅,如图 3 所示,其中图 3(a)为第 1 次迭代所得到的图像,图 3(b)为第 31 次迭代所得到的图像.

以第 50 次迭代后所得到的图像为第 1 幅图像,用原来的 Arnold 变换作为反变换进行迭代来恢复原图.第

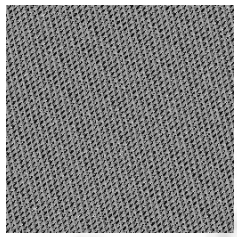
© 中国科学院软件研究所 http://www.jos.org.cn

49 次迭代所得到的图像即为图 3(a).第 50 次迭代后的图像即为原图,也就是图 2(b),在此不再显示.由上面的对比实验可以看出,虽然两种情况下对应的实验图像是不同的,但哪一个作为正变换并不重要,重要的是我们都能把它们其中任意一个用于置乱,另一个用于反置乱,并成功地恢复原图.同时也可以从上面的实验中看出,它们分别作为正变换时第 1 次迭代是不一样的,即图 1(a)与图 3(a)不同.但在同一情况下,却印证了第 1 种情况下的结论,例如图 1(a)与图 2(a)是一样的.

一般地,都是对正方形图像进行 Arnold 变换,现在把它推广到 $m\times n$ 的矩形图像,即图像的长度和宽度不相等,如图 4 所示(该图大小为 176×260).



(a)



(b)

Fig.3

图 3

Fig.4

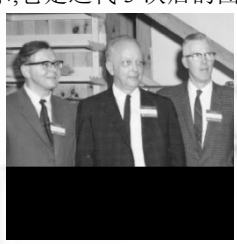
图 4

此时,可以把二维 Arnold 变换写成:

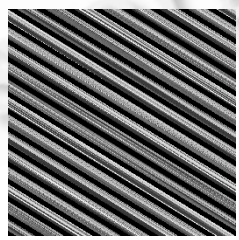
$$\begin{cases} x+y=mp_1+x' \\ x+2y=np_2+y' \end{cases},$$

其中 $m\neq n, p_1, p_2\in Z$ (Z 是整数).

如果按照上面对正方形图像情况的算法直接先进行求解将会出现错误.这是因为长度和宽度不相等,分别对长度和宽度的模运算就不一样了,且此处的 Arnold 变换不再是一一映射,因而不可逆.可以举反例来证明,比如 5×8 的矩形图像.因此,在这里我们把矩形图像转换成正方形图像,其基本思想是:把原来的矩形图像扩充成正方形图像,然后再按照已经讨论过的正方形图像的情况做.如果长度大于宽度,则按长度的大小扩充成正方形图像;如果宽度大于长度,则按宽度的大小扩充成正方形图像;如果宽度等于长度,则是上面讨论过的正方形图像.图 4 的宽度大于长度,因此把该图像扩展成了 260×260 的正方形图像,如图 5(a)所示.我们进行了 17 次迭代,从中抽取了 1 幅,如图 5(b)所示,它是迭代 3 次后的图像.



(a)



(b)

Fig.5

图 5

用本文的方法进行反变换,在这一步可以直接利用已经编好的正方形图像情况下的反变换的源程序,以上面迭代 17 次后的图像为初始图像进行迭代,迭代 17 次后即为上面的扩展成正方形后的图像(图 5(a)),再经过显示的后处理(即不显示图像的扩展部分),即为原图(图 4).该程序用 MATLAB 比用 VC++实现容易些,但应注意 MATLAB 中矩阵的第 1 个元素的位置是(1,1)不是(0,0),这与 VC++有所不同.最后还有一个问题,为什么扩展的图像下面全是以黑色显示,用其他的可以吗?完全可以,比如全是白色的也可以.只要扩展的像素值被赋予 0~255 之间,并且各不相同都可以.因为最终恢复得到的图像与这些像素无关,当然,中间得到的置乱图像与这些像素是有关的,这也在我们的想象之中.对于长度大于宽度的情形类似,不再演示.最后再将该算法应用于数字水印

© 中国科学院软件研究所 http://www.jos.org.cn

系统,此时的实验不再演示.

3 推广的 Arnold 反变换

现在我们把二维 Arnold 反变换推广到三维.定义三维 Arnold 变换[11]如下:

$$\begin{pmatrix} x' \\ y' \\ z' \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 2 & 2 \\ 1 & 2 & 3 \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix} (\mathrm{mod}\, n),$$

其中,(x,y,z) 是原三维图像的像素点,(x',y',z') 是变换后新三维图像的像素点,n 是图像阶数.三维 Arnold 变换等价于 $\exists p_1, p_2, p_3 \in \mathrm{Z}$,(Z 是整数),满足:

$$\begin{cases} x+y+z = np_1 + x' \\ x+2y+2z = np_2 + y' \\ x+2y+3z = np_3 + z' \end{cases} \tag{3}$$

此时,(x',y',z') 和 n 是已知的,(x,y,z) 是未知的,并且式(3)满足隐含条件:

$$\begin{cases} 0 \le x \le n-1, 0 \le x' \le n-1 \\ 0 \le y \le n-1, 0 \le y' \le n-1 \\ 0 \le z \le n-1, 0 \le z' \le n-1 \end{cases},$$

由条件和不等式性质,有

$$\begin{cases} 0 \le x+y+z-x' \le 3n-3 \\ 0 \le x+2y+2z-y' \le 5n-5 \\ 0 \le x+2y+3z-z' \le 6n-6 \end{cases},$$

即

$$\begin{cases} 0 \le np_1 \le 3n-3 \\ 0 \le np_2 \le 5n-5 \\ 0 \le np_3 \le 6n-6 \end{cases}.$$

所以,有

$$\begin{cases} p_1 = 0,1,2 \\ p_2 = 0,1,2,3,4 \\ p_3 = 0,1,2,3,4,5 \end{cases}.$$

所以,共有 $C_3^1 C_5^1 C_6^1 = 90$ 个方程组,要解这 90 个三元一次方程组是相当繁琐的,所以和二维一样,先分类讨论再求解,这样能减少很多计算量.具体操作如下:

第 1 种情况:当 $p_1 = 0$ 时,由(3)式得: $0 \le x+y+z = x' \le n-1$,由条件和不等式的性质得:

$$\begin{cases} 0 \le x+2y+2z-y' \le 3n-3 \\ 0 \le x+2y+3z-z' \le 4n-4 \end{cases},$$

即

$$\begin{cases} 0 \le np_2 \le 3n-3 \\ 0 \le np_3 \le 4n-4 \end{cases},$$

所以

$$\begin{cases} p_2 = 0,1,2 \\ p_3 = 0,1,2,3 \end{cases}.$$

第 2 种情况:当 $p_1 = 1$ 时,由式(3)得: $n \le x+y+z = n+x' \le 2n-1$,由条件和不等式的性质得:

$$\begin{cases} n \le x+2y+2z-y' \le 4n-3 \\ n \le x+2y+3z-z' \le 5n-4 \end{cases},$$

即

$$\begin{cases} n \le np_2 \le 4n-3 \\ n \le np_3 \le 5n-4 \end{cases},$$

所以

$$\begin{cases} p_2 = 1,2,3 \\ p_3 = 1,2,3,4 \end{cases}.$$

© 中国科学院软件研究所 http://www.jos.org.cn

第 3 种情况:当 $p_1=2$ 时,由式(3)得: $2n\le x+y+z=2n+x'\le 3n-1$,由条件和不等式的性质得:

$$\begin{cases}2n\le x+2y+2z-y'\le 5n-3\\ 2n\le x+2y+3z-z'\le 6n-4\end{cases},$$

即

$$\begin{cases}2n\le np_2\le 5n-3\\ 2n\le np_3\le 6n-4\end{cases},$$

所以

$$\begin{cases}p_2=2,3,4\\ p_3=2,3,4,5\end{cases}.$$

这 $3C_3^1C_4^1=36$ 个三元一次方程组解的并即为所求.

现在,进一步把它推广到 m 维的情况,定义 m 维 Arnold 变换[11]如下:

$$\begin{pmatrix}x_1'\\ x_2'\\ x_3'\\ \dots\\ x_{m-1}'\\ x_m'\end{pmatrix}=\begin{pmatrix}1&1&1&\dots&1&1\\ 1&2&2&\dots&2&2\\ 1&2&3&\dots&3&3\\ \dots&\dots&\dots&\dots&\dots&\dots\\ 1&2&3&\dots&m-1&m-1\\ 1&2&3&\dots&m-1&m\end{pmatrix}\begin{pmatrix}x_1\\ x_2\\ x_3\\ \dots\\ x_{m-1}\\ x_m\end{pmatrix}(\mathrm{mod}\,n),$$

即 $\exists p_1,p_2,\dots p_m\in \mathrm{Z}$,(Z 为整数),满足:

$$\begin{cases}x_1+x_2+x_3+\dots+x_{m-1}+x_m=np_1+x_1'\\ x_1+2x_2+2x_3+\dots+2x_{m-1}+2x_m=np_2+x_2'\\ x_1+2x_2+3x_3+\dots+3x_{m-1}+3x_m=np_3+x_3'\\ \dots\\ x_1+2x_2+3x_3+\dots+(m-1)x_{m-1}+(m-1)x_m=np_{m-1}+x_{m-1}'\\ x_1+2x_2+3x_3+\dots+(m-1)x_{m-1}+mx_m=np_m+x_m'\end{cases}.$$

由条件和不等式的性质,有

$$0\le np_i\le (n-1)\sum_{k=0}^{i-1}(m-k)\ ,\ i=1,2,\dots,m\ .$$

所以

$$p_i=0,1,2,\dots,\left(\sum_{k=0}^{i-1}(m-k)\right)-1\ ,i=1,2,\dots,m.$$

具体解这 $\prod_{i=1}^{m}C_{\sum_{k=0}^{i-1}(m-k)}^{1}$ 个方程组时,方法和二维或三维的一样.最后所得到的 m 元一次方程组可采用高斯消元法或 Crame 法则来求,所有解的并即为所求.由于结果繁琐,在此不再写出,有兴趣的读者可具体求解.

4 结 论

在图像置乱技术中,Arnold 变换具有很好的特性.但由于 Arnold 变换的周期性与图像阶有关,对于一幅置乱后比较大的图像,要想利用它的周期性来恢复原图,需要很长时间.本文提出的 Arnold 反变换的算法,使我们在 Arnold 变换后的任意时刻都能随时很快地恢复原图,大大节省了时间.另外,在此基础上把 Arnold 变换应用在正方形图像的情形推广到了矩形图像的情形,拓宽了 Arnold 变换的应用范围,丰富了 Arnold 变换在图像加密中的应用,最后又把二维 Arnold 反变换推广到了 m 维 Arnold 反变换.

References:

[1] Li CG, Han ZZ, Zhang HR. Image encryption techniques: A survey. Journal of Computer Research and Development, 2002,39(10): 1317~1324 (in Chinese with English abstract).

© 中国科学院软件研究所 http://www.jos.org.cn

[2] Ding W, Qi DX. Digital image transformation and information hiding and disguising technology. Chinese Journal of Computers, 1998,21(9):838~843 (in Chinese with English abstract).

[3] Qi DX. Matrix transformation and its application to image hiding. Journal of North China University of Technology, 1999,11(1):24~28 (in Chinese with English abstract).

[4] Zou JC, Li GF, Qi DX. Generalized Gray code and its application in the scrambling technology of digital images. Applied Mathematics (A), A Journal of Chinese Universities, 2002,17(3):363~370 (in Chinese with English abstract).

[5] Bender W, Gruhl D, Morimto N. Techniques for data hiding. IBM System Journal, 1996,35(3-4):313~335.

[6] Chin SS, Hsiang CH, Feng HW, Jeng SP. Genetic watermarking based on transform-domain techniques. The Journal of the Pattern Recognition Society, 2004,37(3):555~565.

[7] Voyatzis G, Pitas I. The use of watermark in the protection of digital multimedia products. Proc. of the IEEE, 1999,87(7): 1197~1207.

[8] Su JK, Girod B. Power-spectrum condition for energy-efficient watermarking. IEEE Trans. on Multimedia, 2002,4(4):551~560.

[9] Moulin P, vanovic A. The zero-rate spread-spectrum watermarking game. IEEE Trans. on Signal Processing, 2003,51(4): 1098~1117

[10] Sun W. The periodicity of Arnold transformation. Journal of North China University of Technology, 1999,11(1):29~32 (in Chinese with English abstract).

[11] Qi DX, Zou JC, Han XY. A new scramble transformation and its application to image hiding. Science in China (Series E), 2000, 30(5):440~447 (in Chinese with English abstract).

[12] Zou JC, Tie XY. Arnold transformation of digital image with two dimensions and its periodicity. Journal of North China University of Technology, 2000,12(1):10~14 (in Chinese with English abstract).

[13] Zhao H. Arnold Transformation of *n* Dimensions and its Periodicity. Journal of North China University of Technology, 2002, 14(1):21~25 (in Chinese with English abstract).

[14] Zhang HX, Qiu PL. Application of Shuffling Techniques within Watermarking. Journal of Circuits and Systems, 2001,6(3):32~36 (in Chinese with English abstract).

[15] Zhao XY, Chen G. Ergodic matrix in image encryption. SPIE, 2002,4875:394~401.

附中文参考文献:

[1] 李昌刚,韩正之,张浩然.图像加密技术综述.计算机研究与发展,2002,39(10):1317~1324.

[2] 丁玮,齐东旭.数字图像变换及信息隐藏与伪装技术.计算机学报,1998,21(9):838~843.

[3] 齐东旭.矩阵变换及其在图像信息隐藏中的应用研究.北方工业大学学报,1999,11(1):24~28.

[4] 邹建成,李国富,齐东旭.广义 Gray 码及其在数字图像置乱中的应用.高校应用数学学报(A 辑),2002,17(3):363~370.

[10] 孙伟.关于 Arnold 变换的周期性.北方工业大学学报,1999,11(1):29~32.

[11] 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藏中的应用.中国科学(E 辑),2000,30(5):440~447.

[12] 邹建成,铁小匀.数字图像的二维 Arnold 变换及周期性.北方工业大学学报,2000,12(1):10~14.

[13] 赵慧.*n* 维 Arnold 变换及其周期性.北方工业大学学报,2002,14(1):21~25.

[14] 张华熊,仇佩亮.置乱技术在数字水印中的应用.电路与系统学报,2001,6(3):32~36.

© 中国科学院软件研究所 http://www.jos.org.cn