文章编号:1001 - 9081(2008)04 - 0888 - 04

花托自同构映射及其逆变换分析

李新路,黄廷祝
(电子科技大学 应用数学学院,成都 610054)
(xinluli@163.com)

摘 要:花托自同构映射是一种变换技术,尤其多被用于数字图像置乱。由于花托自同构映射变换在一定条件下具有周期性,使得通过控制变换的次数可以实现还原。目前关于该变换的还原大都利用周期性进行,但由于周期的无规律性以及还原过程的时间代价过高,使得花托自同构映射的应用及推广受到很大限制。对花托变换的逆映射进行了研究:首先证明了变换是双射,由此可知必然存在它的逆变换;接着给出了一般情况下的逆变换表达式;最后通过图形实验验证了逆变换还原对于周期性还原的优越性。

关键词:数字图像;置乱;花托变换;周期
中图分类号:TP309.7 **文献标志码**:A

Toral automorphisms mapping and anti-toral transformation analysis

LI Xin-lu, HUANG Ting-zhu
(*College of Applied Mathematics, University of Electronic Science and Technology of China, Chengdu Sichuan* 610054, *China*)

Abstract: Toral automorphisms mapping is a transform technology widely applied in digital image scramble. On certain condition the result can be reverted by controlling the transformation time because of the periodicity of the toral automorphisms transformation. In methods to this transformation, its application and generalization are mostly confined to the scrambling of the period and the huge time cost of the reverting. Therefore, the anti-toral transformation was studied. At first the transformation was proved to be bijective, and then the common expression of the anti-toral transformation was given. In the end, the experiment testifies that anti-transformation reverting is better than the periodicity reverting.

Key words: digital image; scramble; toral transformation; period

0 引言

随着网络技术和数字技术的发展,人们体会到网络时代带来的便捷,但同时,网络上的私人信息的安全性也受到威胁,于是信息安全被提上了日程,成为研究的热门,数字图像安全是其中的一大主题。数字图像置乱是一种图像加密的手段,有分形 Hilbert 曲线[1]、IFS 模型[2]、广义 Gray 码变换[3]、Arnold 变换[4]等方法。Arnold 变换是一种周期变换,因此可以应用于图像置乱,对于其周期的研究较多[4,5],但是计算周期并非容易的事,对于周期与图像的阶数 N 到目前还没有给出准确的函数关系。尽管在文献[4,5]中给出了一些特殊情况,但周期较长时,用周期性还原耗时较多,这就给图像还原带来了一定的难度。孔涛等人[6]提出了一种求 Arnold 逆变换的方法,通过解方程组求得逆变换,计算量比较大。花托自同构映射[7,8]是一种混沌映射,具有周期性,其中 Arnold 变换是它的一种特殊情况。比起 Arnold 变换,普通的花托自同构映射有更好的加密性,但是周期也更加难求。如果能求出它的逆映射,就可以利用逆映射还原图像,无需再计算周期。

本文证明了花托自同构映射的可逆性,并给出了逆。试验结果表明,其可操作性强,计算速度快,明显优于已有的周期性还原方法。

1 花托自同构映射

花托自同构映射是一种变换,一个二维的花托自同构是平面内的空域变换,可以定义为:

$$F: \Omega \to \Omega,\ \Omega = [0,1) \times [0,1) \subset R^2 \tag{1}$$

即:

$$\begin{pmatrix} x_{i+1} \\ y_{i+1} \end{pmatrix} = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \begin{pmatrix} x_i \\ y_i \end{pmatrix} (\mathrm{mod}\ 1) \tag{2}$$

记:$\boldsymbol{A} = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$ (3)

其中 $a_{ij} \in Z$, $i, j = 1, 2$, $|\boldsymbol{A}| = 1$ 且它的特征值 λ_1, $\lambda_2 \notin \{-1, 0, 1\}$,其相应的整数格映射为:

$$F_N: L_N \to L_N \tag{4}$$

其中:

$$L_N = \{(x, y) \mid 0 \leqslant x, y \leqslant N-1\} \tag{5}$$

是一个整数网格。较为常用的整数格映射为:

$$F_N(k): F_N \to F_N,$$

$$\begin{pmatrix} x_{i+1} \\ y_{i+1} \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ k & k+1 \end{pmatrix} \begin{pmatrix} x_i \\ y_i \end{pmatrix} (\mathrm{mod}\ N) \tag{6}$$

当 $k = 1$ 时,这个整数格映射被称为猫映射,或称为 Arnold 变换,可以表述成矩阵形式:

$$\begin{pmatrix} x_{i+1} \\ y_{i+1} \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} x_i \\ y_i \end{pmatrix} (\mathrm{mod}\ N) \tag{7}$$

收稿日期:2007 - 10 - 21;**修回日期**:2007 - 12 - 14。
基金项目:四川省应用基础研究项目(05JY029-068-2);电子科技大学"中青年学术带头人 + 创新团队"项目。
作者简介:李新路(1983 -),男,河南焦作人,硕士研究生,主要研究方向:数值代数在图像分析中的应用; 黄廷祝(1964 -),男,四川成都人,教授,博士生导师,主要研究方向:矩阵计算及在信息科学中的应用。

2　花托自同构映射的讨论

上一章阐述了花托自同构的原理，那么用式(1)将图像像素位置进行变换，会不会变换生成相同的坐标呢? 也就是映射是否为单射? 这是我们所关心的问题。当然，如果产生坐标冲突，我们可以用数据结构中的方法解决，而事实上，它不会产生冲突。

定理 1　对任意的$(x_1, y_1), (x_2, y_2) \in L_N$，其中$L_N = \{0, 1, 2, \cdots, N-1\} \times \{0, 1, 2, \cdots, N-1\}$，若满足$(x_1, y_1) \neq (x_2, y_2)$(即$x_1 \neq x_2$或$y_1 \neq y_2$)，则经过映射(6)变换后得到的坐标$(\hat{x}_1, \hat{y}_1)$，$(\hat{x}_2, \hat{y}_2)$也满足$(\hat{x}_1, \hat{y}_1) \neq (\hat{x}_2, \hat{y}_2)$，即该映射是单射。

证明　设$(x_1, y_1), (x_2, y_2) \in L_N$，$(x_1, y_1) \neq (x_2, y_2)$。对$(x_1, y_1)$，$(x_2, y_2)$用式(6)进行变换，即：

$$\begin{pmatrix}\hat{x}_1\\ \hat{y}_1\end{pmatrix} = \begin{pmatrix}1 & 1\\ k & k+1\end{pmatrix}\begin{pmatrix}x_1\\ y_1\end{pmatrix} (\bmod N)$$
$$\begin{pmatrix}\hat{x}_2\\ \hat{y}_2\end{pmatrix} = \begin{pmatrix}1 & 1\\ k & k+1\end{pmatrix}\begin{pmatrix}x_2\\ y_2\end{pmatrix} (\bmod N) \tag{8}$$

那么存在$n_1, n_2, m_1, m_2 \in Z$，使得：

$$\begin{cases}\hat{x}_1 = x_1 + y_1 - n_1 N\\ \hat{y}_1 = kx_1 + (k+1)y_1 - m_1 N = \\ \qquad k(x_1 + y_1) + y_1 - m_1 N\\ \hat{x}_2 = x_2 + y_2 - n_2 N\\ \hat{y}_2 = kx_2 + (k+1)y_2 - m_2 N = \\ \qquad k(x_2 + y_2) + y_2 - m_2 N\end{cases} \tag{9}$$

成立。又因为$x_1 + y_1 < 2N$，$x_2 + y_2 < 2N$，$k(x_1 + y_1) + y_1 < (2k+1)N$，$k(x_2 + y_2) + y_2 < (2k+1)N$，所以$n_1, n_2 \in \{0, 1\}$，$m_1, m_2 \in \{0, 1, 2, \cdots, 2k+1\}$。

下面我们用反证法来证明。假设$(\hat{x}_1, \hat{y}_1) = (\hat{x}_2, \hat{y}_2)$，那么：

$$\begin{cases}x_1 + y_1 - n_1 N = x_2 + y_2 - n_2 N\\ kx_1 + (k+1)y_1 - m_1 N = \\ \qquad k(x_2 + y_2) + y_2 - m_2 N\end{cases} \tag{10}$$

即：

$$x_1 + y_1 = x_2 + y_2 + (n_1 - n_2)N \tag{11}$$
$$k(x_1 + y_1) + y_1 = k(x_2 + y_2) + y_2 - (m_1 - m_2)N \tag{12}$$

将式(11)代入式(12)得：

$$y_1 = y_2 + [m_1 - m_2 - k(n_1 - n_2)]N \tag{13}$$

令$l = m_1 - m_2 - k(n_1 - n_2)$，我们有：

$$y_1 = y_2 + lN \tag{14}$$

若$y_1 = y_2$，则由式(11)得$x_1 = x_2 + (n_1 - n_2)N$。由条件可知$x_1 \neq x_2$，因此$n_1 - n_2 \neq 0$，这与$0 \leqslant x_1, x_2 \leqslant N-1$矛盾，所以$y_1 \neq y_2$。那么由式(14)知，$l \neq 0$，这与$0 \leqslant y_1, y_2 \leqslant N-1$矛盾，所以$(\hat{x}_1, \hat{y}_1) \neq (\hat{x}_2, \hat{y}_2)$，定理得证。

3　二维花托映射的逆变换分析

从花托自同构这个名字来看，我们就知道该映射为双射。上面我们已经证明了它是单射，而映射(6)的定义域和值域都是有限可数集合，且等势，那么它必然是满射。所以存在逆映射，下面我们对其进行求解。这里有必要先给出整数模的定义。

定义 1　n对于N的整数模定义为：

$$n \bmod N = \begin{cases}n - qN, & 0 \leqslant n - qN \leqslant N, \ n \geqslant 0\\ n + qN, & 0 \leqslant n + qN \leqslant N, \ n < 0\end{cases} \tag{15}$$

其中N，q为正整数，n为整数。

设$\boldsymbol{A} = \begin{pmatrix}1 & 1\\ k & k+1\end{pmatrix}$，则容易求出矩阵$\boldsymbol{A}$的逆：

$$\boldsymbol{A}^{-1} = \begin{pmatrix}1 + k & -1\\ -k & 1\end{pmatrix} \tag{16}$$

那么有如下定理成立：

定理 2　对于上述的$\boldsymbol{A}$，(x, y)，$(\hat{x}, \hat{y}) \in L_N$：

$$\begin{pmatrix}\hat{x}\\ \hat{y}\end{pmatrix} = \boldsymbol{A}\begin{pmatrix}x\\ y\end{pmatrix} (\bmod N) \tag{17}$$

成立的充要条件是：

$$\begin{pmatrix}x\\ y\end{pmatrix} = \boldsymbol{A}^{-1}\begin{pmatrix}\hat{x}\\ \hat{y}\end{pmatrix} (\bmod N) \tag{18}$$

成立。

证明　由式(17)，存在整数p_1，q_1使得：

$$\begin{pmatrix}\hat{x}\\ \hat{y}\end{pmatrix} = \boldsymbol{A}\begin{pmatrix}x\\ y\end{pmatrix} + N\begin{pmatrix}p_1\\ q_1\end{pmatrix} \tag{19}$$

成立。继而，我们可以解出：

$$\begin{pmatrix}x\\ y\end{pmatrix} = \boldsymbol{A}^{-1}\begin{pmatrix}\hat{x}\\ \hat{y}\end{pmatrix} - \boldsymbol{A}^{-1}\begin{pmatrix}p_1\\ q_1\end{pmatrix}N \tag{20}$$

令：

$$\begin{pmatrix}p_2\\ q_2\end{pmatrix} = -\boldsymbol{A}^{-1}\begin{pmatrix}p_1\\ q_1\end{pmatrix} \tag{21}$$

也就是$p_2 = -(k+1)p_1 + q_1$，$q_2 = kp_1 - q_1$，显然p_2，q_2为整数，所以式(18)成立。同理，我们可以从式(18)推导出式(17)，式(18)就是花托自同构整数格映射(6)的逆映射。

4　高维花托自同构映射的逆映射

现在我们来研究高维花托自同构映射及其逆映射。定义m维花托自同构映射如下：

$$\begin{pmatrix}\hat{x}_1\\ \hat{x}_2\\ \vdots\\ \hat{x}_m\end{pmatrix} = \boldsymbol{A}\begin{pmatrix}x_1\\ x_2\\ \vdots\\ x_m\end{pmatrix} (\bmod N) \tag{22}$$

其中：

$$\boldsymbol{A} = \begin{pmatrix}1 & 1 & \cdots & 1\\ k & k+1 & \cdots & k+1\\ \vdots & \vdots & & \vdots\\ k & k+1 & \cdots & k+m-1\end{pmatrix} \tag{23}$$

类似于定理 1，我们有如下定理：

定理 3　对于任意的$(x_1, x_2, \cdots, x_m)$，$(y_1, y_2, \cdots, y_m) \in \Omega_N = \{0, 1, \cdots, N-1\} \times \{0, 1, \cdots, N-1\} \times \cdots \times \{0, 1, \cdots, N-1\}$，若满足$(x_1, x_2, \cdots, x_m) \neq (y_1, y_2, \cdots, y_m)$，经过映射(22)变换后得到的坐标$(\hat{x}_1, \hat{x}_2, \cdots, \hat{x}_m)$，$(\hat{y}_1, \hat{y}_2, \cdots, \hat{y}_m)$也满足$(\hat{x}_1, \hat{x}_2, \cdots, \hat{x}_m) \neq (\hat{y}_1, \hat{y}_2, \cdots, \hat{y}_m)$，即该映射是单射。

证明　设$(x_1, x_2, \cdots, x_m)$，$(y_1, y_2, \cdots, y_m) \in \Omega_N$，且$(x_1, x_2, \cdots, x_m) \neq (y_1, y_2, \cdots, y_m)$，用式(22)进行变换，即：

$$\begin{pmatrix}\hat{x}_1\\ \hat{x}_2\\ \vdots\\ \hat{x}_m\end{pmatrix}=\begin{pmatrix}1 & 1 & \cdots & 1\\ k & k+1 & \cdots & k+1\\ \vdots & \vdots & & \vdots\\ k & k+1 & \cdots & k+m-1\end{pmatrix}\begin{pmatrix}x_1\\ x_2\\ \vdots\\ x_m\end{pmatrix}(\mathrm{mod}\ N)$$

$$\begin{pmatrix}\hat{y}_1\\ \hat{y}_2\\ \vdots\\ \hat{y}_m\end{pmatrix}=\begin{pmatrix}1 & 1 & \cdots & 1\\ k & k+1 & \cdots & k+1\\ \vdots & \vdots & & \vdots\\ k & k+1 & \cdots & k+m-1\end{pmatrix}\begin{pmatrix}y_1\\ y_2\\ \vdots\\ y_m\end{pmatrix}(\mathrm{mod}\ N) \tag{24}$$

那么 $\exists p_1, p_2, \cdots, p_m, q_1, q_2, \cdots, q_m \in Z$，使得：

$$\begin{cases}x_1+x_2+\cdots+x_m = Np_1+\hat{x}_1\\ kx_1+(k+1)x_2+\cdots+(k+1)x_m = Np_2+\hat{x}_2\\ \vdots\\ kx_1+(k+1)x_2+\cdots+(k+m-1)x_m = Np_m+\hat{x}_m\end{cases}$$

$$\begin{cases}y_1+y_2+\cdots+y_m = Nq_1+\hat{y}_1\\ ky_1+(k+1)y_2+\cdots+(k+1)y_m = Nq_2+\hat{y}_2\\ \vdots\\ ky_1+(k+1)y_2+\cdots+(k+m-1)y_m = Nq_m+\hat{y}_m\end{cases} \tag{25}$$

假设$(\hat{x}_1, \hat{x}_2, \cdots, \hat{x}_m) = (\hat{y}_1, \hat{y}_2, \cdots, \hat{y}_m)$，那么：

$$\begin{cases}x_1+x_2+\cdots+x_m-Np_1 = y_1+y_2+\cdots+y_m-Nq_1\\ kx_1+(k+1)x_2+\cdots+(k+1)x_m-Np_2 =\\ \quad ky_1+(k+1)y_2+\cdots+(k+1)y_m-Nq_2\\ \vdots\\ kx_1+(k+1)x_2+\cdots+(k+m-1)x_m-Np_m =\\ \quad ky_1+(k+1)y_2+\cdots+(k+m-1)y_m-Nq_m\end{cases} \tag{26}$$

其中，前两个式子可以变为：

$$\sum_{i=1}^{m}x_i = \sum_{i=1}^{m}y_i+(p_1-q_1)N \tag{27}$$

$$(k+1)\sum_{i=1}^{m}x_i-x_1 = (k+1)\sum_{i=1}^{m}y_i-y_1+(p_2-q_2)N \tag{28}$$

将式(27)代入式(28)，得：$(k+1)(p_1-q_1)N = x_1-y_1+(p_2-q_2)N$，即 $x_1 = y_1+[(k+1)(p_1-q_1)-(p_2-q_2)]N$。

令 $l_1 = (k+1)(p_1-q_1)-(p_2-q_2)$，则 $x_1 = y_1+l_1N$。

若 $x_1 \neq y_1$，则 $l_1 \neq 0$，这与 $0 \leqslant x_1, y_1 \leqslant N-1$ 矛盾。所以：

$$x_1 = y_1 \tag{29}$$

将式(29)代入式(26)，并去掉第二个等式，得到：

$$\begin{cases}x_2+\cdots+x_m-Np_1 = y_2+\cdots+y_m-Nq_1\\ (k+1)x_2+\cdots+(k+2)x_m-Np_3 =\\ \quad (k+1)y_2+\cdots+(k+2)y_m-Nq_3\\ \vdots\\ (k+1)x_2+\cdots+(k+m-1)x_m-Np_m =\\ \quad (k+1)y_2+\cdots+(k+m-1)y_m-Nq_m\end{cases} \tag{30}$$

再将第一个等式代入第二个，并且化简，得到 $x_2 = y_2+[(k+2)(p_1-q_1)-(p_3-q_3)]N$。

令 $l_2 = (k+2)(p_1-q_1)-(p_3-q_3)$，则 $x_2 = y_2+l_2N$。

若 $x_2 \neq y_2$，则 $l_2 \neq 0$，这与 $0 \leqslant x_2, y_2 \leqslant N-1$ 矛盾。所以：

$$x_2 = y_2 \tag{31}$$

同样，将式(31)代入式(30)，继续下去，可以得到 $x_3 = y_3$，$x_4 = y_4$，$\cdots$，$x_m = y_m$。

这与已知的$(x_1, x_2, \cdots, x_m) \neq (y_1, y_2, \cdots, y_m)$矛盾，故$(\hat{x}_1, \hat{x}_2, \cdots, \hat{x}_m) \neq (\hat{y}_1, \hat{y}_2, \cdots, \hat{y}_m)$，定理得证。

上述定理说明了变换公式(22)同样是双射，所以存在逆映射。容易求出矩阵 $\boldsymbol{A}$ 的逆：

$$\boldsymbol{A}^{-1} = \begin{pmatrix}k+1 & -1 & 0 & \cdots & 0 & 0\\ -k & 2 & -1 & \cdots & 0 & 0\\ 0 & -1 & 2 & \cdots & 0 & 0\\ \vdots & \vdots & \vdots & & \vdots & \vdots\\ 0 & 0 & 0 & \cdots & 2 & -1\\ 0 & 0 & 0 & \cdots & -1 & 1\end{pmatrix} \tag{32}$$

这就是花托自同构映射在 m 维空间上的逆变换。于是，对于花托自同构变换及其逆变换我们可以得到如下定理：

定理 4 对$(x_1, x_2, \cdots, x_m)$，$(\hat{x}_1, \hat{x}_2, \cdots, \hat{x}_m) \in \boldsymbol{\Omega}_N$，

$$\begin{pmatrix}\hat{x}_1\\ \hat{x}_2\\ \vdots\\ \hat{x}_m\end{pmatrix}=\boldsymbol{A}\begin{pmatrix}x_1\\ x_2\\ \vdots\\ x_m\end{pmatrix}(\mathrm{mod}\ N) \tag{33}$$

成立的充要条件是：

$$\begin{pmatrix}x_1\\ x_2\\ \vdots\\ x_m\end{pmatrix}=\boldsymbol{A}^{-1}\begin{pmatrix}\hat{x}_1\\ \hat{x}_2\\ \vdots\\ \hat{x}_m\end{pmatrix}(\mathrm{mod}\ N) \tag{34}$$

成立。

证明 证明过程类似于定理 2，此处不再赘述。

5 图形实验

基于式(22)的 m 维上花托自同构映射进行图像置乱以及图像去乱的整个过程可以描述为算法 1 和算法 2 两个算法。

算法 1 基于花托自同构映射的图像置乱算法

1）给定初始参数 k，变换次数 K 和图像大小 $N \times N$，其中 k，K 这两个参数都可以用作密钥。

2）对给定图像的每点像素坐标都用式(22)进行变换，得到新的坐标顺序。

3）重复 2）直到指定变换次数 K，得到新的坐标顺序。

4）将原图像素映射到新的坐标上，得到置乱图像。

算法 2 花托自同构映射图像置乱的还原算法

1）利用密钥 k，求出 $\boldsymbol{A}$ 的逆矩阵 $\boldsymbol{A}^{-1}$。

2）对给定的置乱元素坐标用式(34)进行变换，得到新的坐标顺序。

3）重复 2）直到密钥中的变换次数 K，得到新的坐标顺序。

4）将置乱元素映射到新的坐标上，得到原始元素。

对 Arnold 变换，首先我们将本文的方法与文献[6]的方法进行比较。取 $m = 3$，做三维上的图形实验，选取一个 $21 \times 21 \times 21$ 空间上的锥顶作为实验对象。结果表明文献[6]的方法耗时 2.781 250 s，而本文方法耗时仅 0.031 250 s，还原速度明显提高，实验结果如图 1 所示。改变 N 的值进行多次实

验，可知随着 N 的值越大，本文方法的优越性越明显，不同 N 值的对比如表 1 所示。

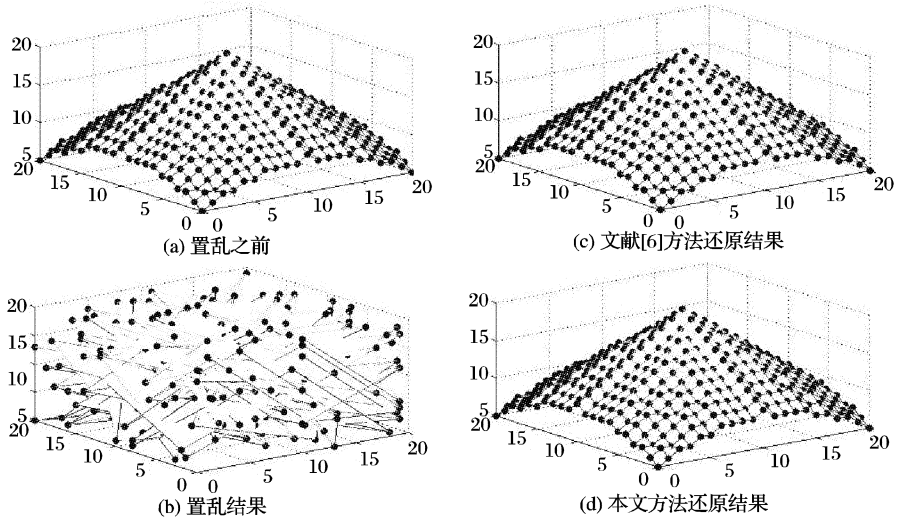

图 1　锥顶实验

表 1　不同 N 值对比

N 值	文献[6]方法耗时/s	本文方法耗时/s	速度比
20	2.781 250	0.031 250	89.000 0
30	7.453 125	0.062 500	119.250 0
40	17.109 375	0.125 000	136.875 0
50	30.578 125	0.187 500	163.083 3
60	51.078 125	0.250 000	204.312 5

然后对一般的花托变换，我们将本文的方法和文献[4]等提出的周期性方法还原进行对比。选取一个 $21 \times 21 \times 21$ 空间上的阈边帽作为实验对象，取 $k = 12$; $K = 12$ 进行实验，两种方法都可以达到去乱的效果。此时周期 $T = 76$，在相同的条件下，用周期还原需要时间 $t = 0.187500$ s，而用逆变换还原只需 $t = 0.031250$ s，实验的结果如图 2 所示。

接下来选取其他 k 和 K 值进行多次实验，结果表明本文提出的方法明显优于已有的周期性方法，两种方法的实验结果对比如表 2 所示。

若实验对象为 $a \times b \times c$ 的长方体，而不是 $N \times N \times N$ 的正方体，变换(22) 不再是一一映射，因而不可逆。为了进行置乱，我们把它扩展成正方体来做。具体思路如下：求出 a，b，c 中的最大值，设为 N，然后扩展成 $N \times N \times N$ 的正方体，扩展部分可任意取值，因为最终恢复得到的结果和这些点无关。对恢复后的结果我们只取前面的 $a \times b \times c$ 部分的值就得到了初始图形。

表 2　实验结果对比

k 值	K 值	周期 T	周期还原时间/s	逆变换还原时间/s
9	9	48	0.109 375	0.015 625
	15	48	0.093 750	0.031 250
	18	48	0.062 500	0.046 875
16	24	624	1.515 625	0.062 500
	64	624	1.390 625	0.156 250
	100	624	1.296 875	0.234 375
18	52	228	0.453 125	0.125 000
	72	228	0.406 250	0.171 875
	85	228	0.375 000	0.187 500

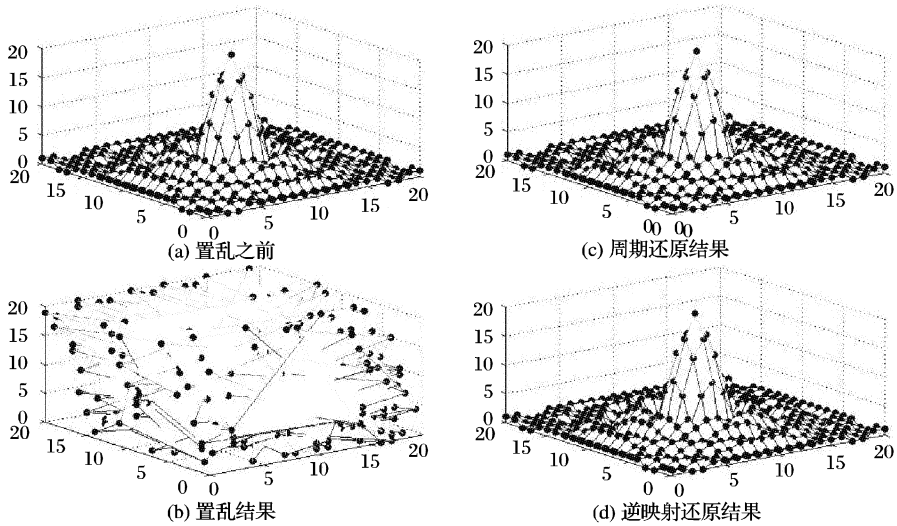

图 2　阈边帽实验

6　结语

在置乱变换的方法中，花托自同构映射有很好的特性，目前已有不少关于这方面的研究。尤其对于其中的 Arnold 变换，不仅有很多关于其周期性的研究结果，而且还有利用

(下转第 895 页)

露开销,故发送 ∅。至此,双方可生成各自的最小开销生成树,图2(d)给出了全局的最小开销生成树。10 到 14 处发送的消息是依据定义 3 自顶向下遍历最小开销生成树生成。15 到 20 处为实际的凭证披露,则是依据定义 3 自底向上遍历最小开销生成树生成。21 处发送 *Success*,协商成功结束,即高性能计算中心 M 将向张三以收费的方式提供网格计算资源 R。

3　性能分析

对于自动信任协商策略的性能分析一般从通信复杂度和时间复杂度两个方面进行。ATN 发生在网络中需要交互的两个实体之间,因此不可避免地给网络通信带来额外的负担;对于凭证的解锁、开销更新和最小开销生成树的遍历会加重本机处理器的运算量,将影响到本机其他进程的运行。

3.1　策略的通信复杂度

通信复杂度取决于消息的数量和消息的大小。策略包括七类的消息,主要考虑其中的 *NewlyUnlockSet*、*SolvedDisclose* 和 *FinalDisclose*,其余四类容易得出其通信复杂度为线性。对于 *NewlyUnlockSet*,在最坏的情况下,每个凭证均对应一条解锁的消息,其开销在每条访问控制策略下均更新一次,设访问控制策略数量为 m,则对应于 n 个凭证最多有 $O(nm)$ 条消息。设 *NewlyUnlockSet* 消息的大小为一常数,则 *NewlyUnlockSet* 的通信复杂度为 $O(nm)$。对于 *SolvedDisclose*,n 个凭证至多发送 n 条 *SolvedDisclose* 消息,消息内容为凭证描述,大小为常数,故通信复杂度不超过 $O(n)$。对于 *FinalDisclose*,消息的数量同 *SolvedDisclose*,但消息内容为真正的凭证,设每个凭证的大小不超过 $O(n)$,则复杂度为 $O(n^2)$。综上所述,在最坏的情况下,通信复杂度为 $O(mn+n^2)$,其中,若 $m \gg n$,则复杂度为 $O(mn)$;反之,若 $n \gg m$,则复杂度为 $O(n^2)$。

3.2　策略的计算复杂度

计算复杂度主要涉及到凭证的解锁、凭证披露开销的更新以及最小开销生成树的搜索。影响因素包括凭证的数量 n 和访问控制策略的数量 m。现考虑最复杂的情况,假设 $n-1$ 个凭证(至少有一个凭证除外,否则协商无法进行)均对应一条访问控制策略。在最坏的情况下,对每个凭证的解锁将遍历协商开销图的 m 个节点,凭证的披露开销的更新与解锁同时进行,故凭证的解锁和开销更新的计算复杂度不超过 $O(nm)$。最小开销生成树的节点数至多为 n 个,则生成 *SolvedDisclose* 和 *FinalDisclose* 消息时对最小开销生成树的搜索的复杂度不超过 $O(n)$。因此基于动态规划的协商策略的计算复杂度为 $O(nm)$。

4　结语

本文在定义披露开销的基础上,基于协商开销图建模,运用动态规划的思想,设计了一种能找到最小开销凭证披露序列的协商策略。该策略区分了凭证的解锁和披露,使协商过程实际上分成凭证披露序列确立和实际凭证披露两个阶段,有以下两个优点:1)凭证的先解锁后披露保证了协商过程的安全性;2)协商过程的前阶段只发送凭证描述,减小交互的消息大小,降低通信量,后阶段才实际披露凭证,提高了协商效率。经证明,该策略为高效的,其通信复杂度为 $O(mn+n^2)$,计算复杂度为 $O(nm)$,其中 n 为凭证的数量,m 为访问控制策略的数量。

本文提出的基于动态规划的协商策略还存在一些不足:该策略虽然确保最小开销生成树生成的一定是协商总开销最小的凭证披露序列,但却不是凭证披露数目最少的披露序列,如何均衡最小开销和最少数目将是下一步的研究方向;其次,本文尚未考虑访问控制策略的披露开销,对于实际的协商,访问访问控制策略本身也具有披露开销,我们将进一步开展这方面的研究;另外,该策略虽然未将访问控制策略的内容向对方披露,但对协商过程进行深入分析仍能得出部分访问控制策略,加强策略的安全性也是进一步的研究方向。

参考文献:

[1] WINSBOROUGH W H, SEAMONS K E, JONES V E. Automated trust negotiation[C]// DARPA Information Survivability Conference and Exposition. Washington D C, USA: IEEE Press, 2000: 88-102.

[2] 李建欣, 怀进鹏, 李先贤. 自动信任协商研究[J]. 软件学报, 2006, 17(1): 124-133.

[3] YU T, MA X, WINSLETT M. PRUNES: An efficient and complete strategy for trust negotiation over the Internet[C]// Proceedings of the 7th ACM Conference on Computer and Communications Security. New York: ACM Press, 2000: 210-219.

[4] CHEN W, CLARKE L, KUROSE J, *et al*. Optimizing cost-sensitive trust-negotiation protocols[C]// INFOCOM 2005. Washington DC: IEEE Computer and Communications Society, 2005, 2: 1431-1442.

[5] BELLMAN R E. Dynamic Programming[M]. Princeton, NJ: Princeton University Press, 1957.

(上接第 891 页)

反变换进行还原的研究。但是,由于变换的周期和图像的大小有关,当图像比较大的时候,利用周期性进行还原就显得不太现实。本文提出的逆变换算法不仅克服了这个问题,使得在图像被置乱任意多次后,能很快地进行恢复,而且对于更普遍的花托自同构映射同样可以进行操作,拓宽了它的应用范围。

参考文献:

[1] DING WEI, XU QI-DONG. Digital image transformation and information hiding and disguising technology[J]. Chinese Journal of Computers, 1998, 21(9): 838-843.

[2] XU QI-DONG. Matrix transformation and its application to image hiding[J]. Journal of North China University of Technology, 1999, 11(1): 24-28.

[3] ZOU JIAN-CHENG, LI GUO-FU, XU QI-DONG Generalized gray code and its application in the scrambling technology of digital images[J]. Applied Mathematics(A), A Journal of Chinese Universities, 2002, 17(3): 363-370.

[4] 黎罗罗. Arnold 型置乱变换周期分析[J]. 中山大学学报: 自然科学版, 2005, 44(2): 1-4.

[5] 李兵, 徐家伟. Arnold 变换的周期及其应用[J]. 中山大学学报: 自然科学版, 2004, 43(A02): 139-142.

[6] 孔涛, 张亶. Arnold 反变换的一种新算法[J]. 软件学报, 2004, 15(10): 1558-1564.

[7] VOYATZIS G, PITAS I. Applications of toral automorphisms in image watermarking[J]. IEEE International Conference on Image Processing. Washington DC: IEEE Computer Society, 1996, 2: 237-240.

[8] 孙圣和, 陆哲明, 牛夏牧. 数字水印技术及应用[M]. 北京: 科学出版社, 2004.