基于改进的 Arnold 变换的数字图像置乱

司银女,康宝生
(西北大学 信息科学与技术学院,陕西 西安 710069)

摘 要:随着网络和现代通信技术的飞速发展,数字化多媒体信息的安全问题正日益成为人们关注的焦点,对信息的安全传输提出了更高的要求。信息隐藏成为信息技术领域的一大研究热点。改进了传统的 Arnold 变换。采用改进的 Arnold 变换对数字图像进行双向置乱,提高了置乱算法的效率,改善了置乱效果。通过在置乱算法中加入密钥,提高了算法的安全性。算法简单易行,可作为数字图像信息隐藏的预处理工具。

关键词:Arnold 变换;数字图像置乱;数字图像隐藏;密钥;峰值信噪比
中图分类号:TN911 **文献标识码**:A **文章编号**:1673-629X(2008)02-0074-03

Digital Image Scrambling Based on Improved Arnold Transformation

SI Yin-nü, KANG Bao-sheng
(School of Information Science and Technology, Northwest University, Xi'an 710069, China)

Abstract: With the rapid development of Internet and the modern telecommunication technology, digital information security has increasingly been cared, a higher request has been raised for information transmission safety. Information hiding has become a hot field in the society of information science and technology. The Arnold transformation is always being used in one direction. In this thesis, a modification has been given on Arnold transformation. While the modified Arnold transformation is used to scramble a digital image in two directions, the computing cost are reduced notably and the result of scrambling has a more improvement. By using secret key in scrambling, the security of the algorithm is increased. The approaches are easy to realize, and can be used as the preprocessing for the digital image information hiding.

Key words: Arnold transformation; digital image scrambling; digital image hiding; secret key; peak signal to noise ratio

0 引 言

置乱在数字化的今天已经不再是一个新名词。数字图像置乱是将一幅图像经过变换,使其成为面目全非的另一幅没有明显意义的混乱图像。置乱是在信息隐藏中对数字图像所做的预处理,也叫做信息伪装。数字图像置乱过程实质上是一类图像编码和解码的过程。数字图像置乱[1]可以在位置空间、色彩空间及频率空间上进行,其基本思想可以追溯到高卢战争时期凯撒大帝使用的凯撒暗码,即将原信息中的某个字母,按照某种固定的规则,依次用另外的字母代替。这种字母的替换可以看作是一种一维数据流的值替换,将之扩展到二维情形,从而可以得到对数字图像的位置或灰度等级做变换,使图像变得"面目全非",从而在一定程度上达到迷惑第三者的目的。

许多学者就数字图像置乱问题进行了研究,提出了大量的数字图像置乱方法。丁伟等[2]提出了基于 Arnold 变换的数字图像置乱;闫伟齐等[3]给出了基于 DES 的数字图像置乱;邹建成[4]提出了基于原根的数字图像置乱;李国富[5]研究了基于正交拉丁方的数字图像置乱;齐东旭[6]讨论了 FASS 曲线数字图像置乱;柏森等[7]提出了基于行列式的图像置乱;邹建成等[8]进一步提出了基于 Gray 的数字图像置乱。

基于 Arnold 变换的置乱的研究[2]仅局限于在一个方向上对图像进行置乱,效果并不是很好,且没有恢复的过程,其安全性由算法来决定,当知道所采用算法时恢复是很简单的。对于一个置乱算法,如果对图像进行加密,不仅可以提高算法的安全性,而且可以提高置乱的效果。

文中通过改进传统 Arnold 变换,给出一种新的图

收稿日期:2007-05-13
基金项目:陕西省自然科学基金(2005A14)
作者简介:司银女(1981-),女,陕西西安人,硕士研究生,研究方向为计算机辅助几何设计、数字图像处理;康宝生,教授,博士生导师,研究方向为计算机辅助几何设计、数字图像处理。

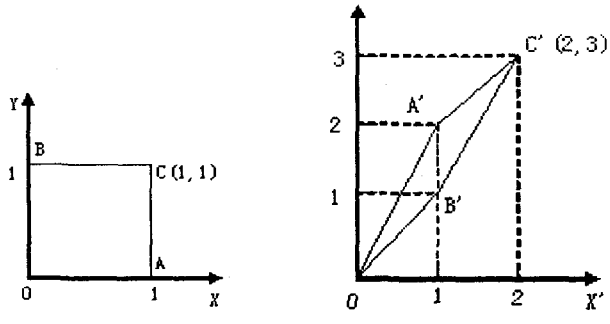
像置乱算法。所给算法对一幅灰度图像在两个方向上进行基于改进的 Arnold 变换,以及基于改进的 Arnold 变换的加密来实现图像的置乱和恢复。在所提出的算法中,加密是可以在置乱的整个过程中的任何一步进行的,且不对结果造成任何影响,同时解密也可以在置乱的整个过程中的任何一步进行且不对结果造成任何影响。

1　Arnold 变换

Arnold 变换是 Arnold 在遍历理论研究中提出的一种变换,又称为猫脸变换[6]。设想在平面单位正方形内绘制一个猫脸图像,通过下述变换,猫脸图像将由清晰变模糊。用矩阵表示即为:

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \bmod 2 \qquad (1)$$

其图形表示如图 1 所示。



(a) 原始图形　　(b) 变换后的图像

图 1　Arnold 变换

如果把其中的线段 OA、OB、OC 看成向量,则 Arnold 变换其实是对向量 OA、OB、OC 做了一个缩放和旋转变换。这种变换是一一对应的,且可以迭代地做下去。类似的变换可以参看面包师变换。

2　基于 Arnold 变换的数字图像置乱及恢复

一幅数字图像可看作是在二维连续曲面上按照某一间隔和某种策略进行采样所得的一个二维离散点阵,所以将图像表示为矩阵形式,矩阵中的元素即为图像对应点处的灰度值或者 RGB 颜色分量值。对于正方形数字图像,离散化的 Arnold 变换如下:

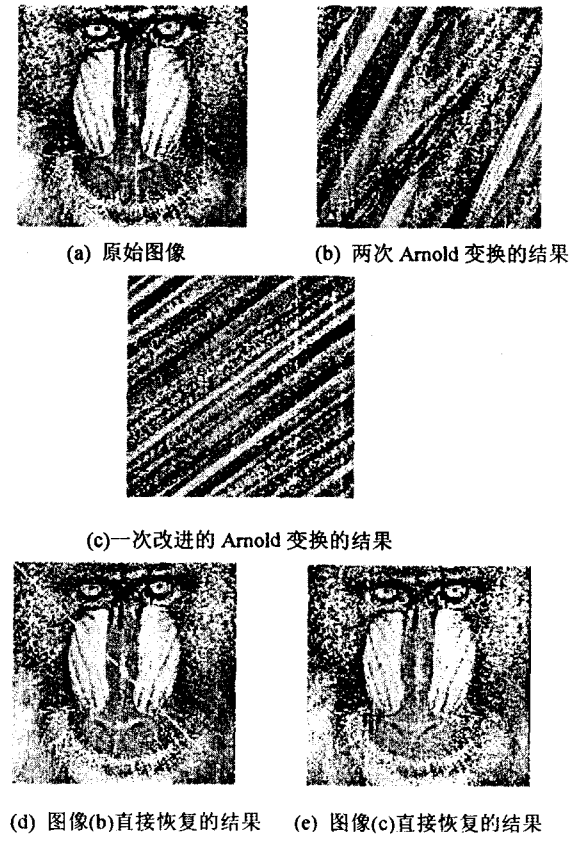
$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \bmod N; x, y \in \{0, 1, \cdots, N-1\} \qquad (2)$$

其中,N 为图像的宽度和高度;x,y 为坐标点(x, y)的两个坐标分量。

式(2)的置乱是对图像在一个方向上进行置乱,完全可以考虑在两个方向上同时对一幅图像做置乱,即对图像做如下的变换:

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 3 & 2 \\ 4 & 3 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \bmod N \qquad (3)$$

对于数字化图像来说,所做的灰度值或者 RGB 颜色值的移动,可看作是将原图像中的(x, y)点处对应的值移动到新图像中的点(x', y')处。重复进行这一过程,直到所生成的图像符合对图像的"面目全非"的要求,即实现了一幅图像的置乱,图 2 是对一幅 128×128 的灰度图像采用上述两种方法分别进行置乱的结果。



(a) 原始图像　　(b) 两次 Arnold 变换的结果

(c)一次改进的 Arnold 变换的结果

(d) 图像(b)直接恢复的结果　　(e) 图像(c)直接恢复的结果

图 2　Arnold 变换与改进的 Arnold 变换的置乱结果

应用 Arnold 变换对图像进行的置乱是一个位置置乱,无论做几次变换,无论是采用原变换还是采用改进后的变换,其置乱后的直方图都和原图像的直方图没有区别,所以下面只对恢复后的图像进行峰值信噪比的比较。采用 Arnold 变换两次所得图像之恢复图像的峰值信噪比为 PSNR = 28.9026,而采用一次改进的 Arnold 变换后,其结果图像之恢复图像的峰值信噪比则为 PSNR = 29.8983。

采用 Arnold 变换对图像置乱的恢复很简单,只需告诉接受方采用的是改进的 Arnold 变换就可以了。恢复的结果如图 2(e) 所示。

Arnold 变换具有周期性,当迭代到某一步时,将重复得到原始图像。Dyson 和 Falk 分析了离散 Arnold 变

换的周期性[6]，对于任意给定的正整数 $N > 2$，Arnold 变换的周期 $T_N \leqslant N^2/2$，这也是现在能得到的最好的结果了。

3 密钥的应用

基于 Arnold 变换的数字图像置乱方法能够实现对图像的置乱处理，但其安全性由算法保证。如果非法者得到或者猜想到实现图像置乱的方法，则很容易恢复出原始图像。因此，该方法在实际应用中具有很大的局限性。为此，通过加入密钥来提高系统的安全性。

将数字图像 $\boldsymbol{F}$ 看作是等间隔离散点上的采样矩阵，矩阵的每个元素对应图像上的一个采样点。该采样矩阵可以表示为：

$$\boldsymbol{F} = \begin{pmatrix} F_{00} & F_{10} & \cdots & F_{N-1,0} \\ F_{01} & F_{11} & \cdots & F_{N-1,1} \\ \vdots & \vdots & \vdots & \vdots \\ F_{0,N-1} & F_{1,N-1} & \cdots & F_{N-1,N-1} \end{pmatrix}$$

其中 $F_{x,y} = 0,1,\cdots,255$。

首先选取从 2 开始的顺序 N 个素数，对其做模 N 运算，即可得到一个没有周期且没有规律的整数序列，写成向量形式记为：

$$F_w = (F_w^1, F_w^2, \cdots, F_w^N)$$

做

$$F_w^i \times (F_{i0}, F_{i1}, \cdots, F_{i,N-1})$$

即对图像每行进行加密。

其次，选取从 4 开始的 N 个合数序列，并对其做模 N 运算，同样可以得到一个没有周期且没有规律的整数序列：

$$F_h = (F_h^1, F_h^2, \cdots, F_h^N)$$

做

$$F_h^i \times (F_{0i}, F_{1i}, \cdots, F_{N-1,i})$$

即对图像每列进行加密。

将 F_h、F_w 作为私钥通过秘密信道传送给合法用户，将采用改进的 Arnold 变换置乱的图像作为公钥从普通信道传送给合法用户。图 3 是对加密图像采用改进的 Arnold 变换置乱和恢复的结果，恢复图像的峰值信噪比为 PSNR = 29.8983。

为了进一步提高置乱效果，只需重复进行置乱即可。每次置乱都可以加入密钥。

只要知道密钥和算法，基于改进的 Arnold 变换的图像置乱的恢复很简单。但是，不知道密钥或者算法，要恢复图像，其计算量是相当的大，基本上是不可能的。

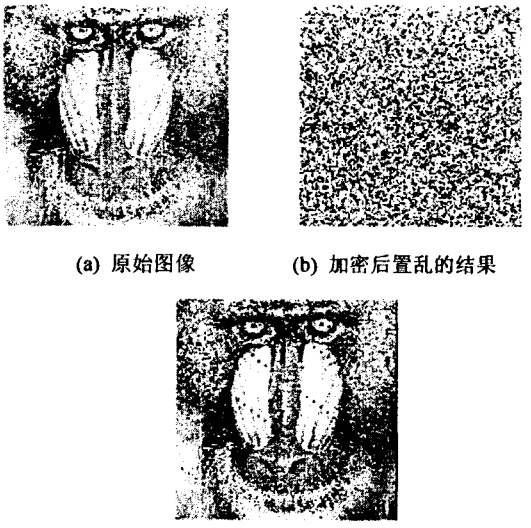
由图像置乱过程可知，恢复算法如下：

Step1 分别对置乱的图像每行的每个元素乘以给定的密钥 F_w 的相应的值；

Step2 分别对置乱的图像每列的每个元素乘以给定的密钥 F_h 的相应的值。

Step3 对 Step2 得到的结果进行逆 Arnold 变换，即可得到恢复图像。

采用改进的 Arnold 变换很容易推广到彩色图像，原理完全相同，这里不赘述。



(a) 原始图像 (b) 加密后置乱的结果

(c) 对(b)恢复的结果

图 3 加密后应用改进的 Arnold 变换的置乱和恢复结果

4 结 论

讨论了改进的 Arnold 变换，使得置乱的速度和质量都有很大的提高，且没有增加图像恢复的难度。实验结果表明，改进方法的恢复图像比原方法的恢复图像的峰值信噪比高。对原图像加密后，使得对于不知道密钥的非法截获者，要恢复出原始图像几乎不可能，从而提高了安全性。尽管改进方法的恢复效果优于原方法，但峰值信噪比仍然不高。对此，在以后的工作中将作进一步的研究，以提高恢复效果。

参考文献：

[1] 丁 伟，闫伟齐，齐东旭. 基于置乱与融合的数字图像隐藏技术及应用[J]. 中国图像图形学报，2000，8(5)：644 - 649.

[2] 丁 伟，闫伟齐，齐东旭. 基于 Arnold 变换的数字图像置乱技术[J]. 计算机辅助设计与图形学学报，2001，13(4)：338 - 341.

[3] 闫伟齐，邹建成，齐东旭. 一种基于 DES 的数字图像置乱

(下转第 79 页)

表 1　某一信息决策系统

U	a	b	c	e	d
1	0	0	0	0	0
2	1	0	1	1	1
3	1	1	0	0	0
4	0	2	0	1	1
5	1	2	0	0	1
6	1	0	0	0	0
7	1	2	1	1	1
8	0	0	1	1	1

表 2　表 1 的分辨矩阵

U	1	2	3	4	5	6	7	8
1	0	*ace*	*bce*	*be*	*ab*	0	*abce*	*ce*
2		0	*bce*	0	0	*ce*	0	0
3			0	*abe*	*b*	0	*bce*	*abce*
4				0	0	*abe*	0	0
5					0	*b*	0	0
6						0	*bce*	*ace*
7							0	0
8								0

① 计算。

$JH_a = \{1,2,3,4,5,6,7,8\}$,则 $POS_a(D) = \varnothing$

同理可得:

$POS_b(D) = \{3,4,5,7\}$

$POS_c(D) = \{2,7,8\}$

$POS_e(D) = \{2,4,7,8\}$

选择 b 或 e 加入到 $RED(R)$ 中,设 $RED(R) = \{e\}$

② 由于 $JH_{RED(R)} = \{1,3,5,6\}$,而 $JH_C = \varnothing$,$JH_{RED(R)} \neq JH_C$,故需要增加其它属性,以构成最小约简。

$POS_{RED(R)\cup\{a\}}(D) = \{1,2,4,5,7,8\}$

$POS_{RED(R)\cup\{b\}}(D) = \{1,2,3,4,5,6,7,8\}$

$POS_{RED(R)\cup\{c\}}(D) = \{2,4,7,8\}$

选择 b 加入到 $RED(R) = \{e,b\}$,此时 $JH_{RED(R)} = JH_C$

该决策表的一最小属性约简为 $\{e,b\}$。

3　基于新的属性约简的规则提取

文中提出的新的属性约简算法,通过计算相对正域的大小来选择属性加入到约简集中,相对正域越大,根据该条件属性组合(或单个属性)能够确定分类的对象就越多。故每次选择的属性可以作为决策树的结点,第一次选择的属性可以作为根结点,其后选择的属性可以作为叶子结点。根据新的属性约简算法对表 1 构建的决策树,如图 1 所示。

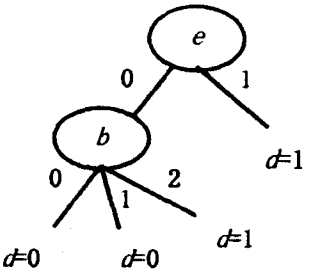


图 1　表 1 的决策树

由图 1 得出表 1 的 4 条规则如下:

$e = 0 \wedge b = 0 \rightarrow d = 0$; $e = 0 \wedge b = 1 \rightarrow d = 0$;

$e = 0 \wedge b = 2 \rightarrow d = 1$; $e = 1 \rightarrow d = 1$

4　结束语

文中提出计算不同的条件属性组合相对于决策属性的正域的方法,并给出计算核属性的新方法。利用分辨矩阵正域作为启发式知识,提出了一种基于分辨矩阵的核属性和非核属性同步选择的属性约简的算法,在该属性约简的基础上,能够简单地生成一棵决策树,进行规则提取。该算法的主要特点有:利用分辨矩阵的正域作为启发式知识;判断约简条件简单。最后通过例子分析,表明该算法是有效的。

参考文献:

[1] Pawlak Z. Vagueness and uncertainty: A Rough Set Prospective[J]. Inter J of Computer Intelligence, 1995, 11(2): 37 - 41.

[2] 王国胤. Rough 理论与知识获取[M]. 西安:西安交通大学出版社,2001.

[3] 李秀红,史开泉. 一种基于知识粒度的属性约简算法[J]. 计算机应用,2006,26(6):76 - 77.

[4] 李　珊,肖怀铁,付　强. 改进的粗集属性约简的启发式算法[J]. 电光与控制,2006,13(8):46 - 48.

[5] 王亚英,张春慨,邵惠鹤. 启发式知识约简算法的研究与应用[J]. 控制与决策,2001,16(6):886 - 889.

(上接第 76 页)

新方法[J]. 北方工业大学学报,2002,14(1):1 - 7.

[4] 邹建成. 基于原根的数字图像置乱技术[J]. 北方工业大学学报,2001,13(3):14 - 16.

[5] 李国富. 基于正交拉丁方的数字图像置乱方法[J]. 北方工业大学学报,2001,13(1):14 - 17.

[6] 齐东旭. 分形及其计算机生成[M]. 北京:科学出版社,1997.

[7] 柏　森,曹长修. 一类基于行列式计算思想的图像置乱加密算法[J]. 计算机工程与应用,2002,38(8):37 - 39.

[8] 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[J]. 高校应用数学学报 A 辑,2002,17(3):363 - 370.