

Fibonacci 变换及其在数字图像水印中的应用^{*}

商艳红, 李 南, 邹建成

(北方工业大学 CAD 研究中心, 北京 100041)

摘 要: 基于 Fibonacci 变换具有均匀性的良好性质, 在一种基于 Fibonacci 变换的数字图像置乱方法的基础上, 给出了一种描述数字图像置乱程度的置乱度的定义, 并比较了 Arnold 变换和 Fibonacci 变换的置乱效果。实验表明 Fibonacci 变换的置乱效果比 Arnold 变换的置乱效果要好。还考虑了 Fibonacci 变换在数字图像水印中的应用, 并作了一些抗攻击实验, 取得了令人满意的结果。

关键词: Fibonacci 变换; 图像置乱; 数字水印

中图分类号: TP391.41 **文献标识码:** A **文章编号:** 0529-6579 (2004) S2-0148-05

近年来作为有效保护版权的数字水印技术得到了越来越多的关注。一般来说, 不管是何种数字产品的版权保护, 尤以表明产品版权信息的图像水印为主。这是因为提取出来的水印主要由人的视觉进行验证, 而图像水印由于人眼的分辨率有限, 即使多个像素错误也不会影响整体信息, 图像的鲁棒性较其他水印有明显优势。因此我们可以想到, 如果错误像素分散在整幅水印图像中, 则其对视觉的影响就更小, 即错误像素分散得越均匀抽取得到的水印效果越好。而数字图像的置乱技术用于水印预处理中恰恰能够做到这一点。

图像置乱技术作为一种图像加密技术, 已成为数字图像安全传输和保密存储的重要手段之一。该技术将原来有一定意义的图像数据, 通过一些变换, 将原始图像变换成一幅“杂乱无章”的新图像, 达到保护图像信息的目的^[1-7]。在数字水印技术中, 利用位置置乱可将错误像素的分布分散开来, 用于水印图像的预处理中, 可提高不可见水印的鲁棒性。在图像加密中, 置乱技术主要关心的是加密强度或解密难度。而在水印预处理中, 置乱技术更关心的是对错误像素分布的分散程度, 提高水印的视觉效果来增强其鲁棒性。因此在数字水印系统中置乱技术需要考虑: ①置乱算法的快速性; ②分散像素的均匀性。本文研究了基于 Fibonacci 变换的置乱效果及其在数字图像水印中的应用, 从理论分析和实验数据上显示, 该置乱算法置乱速度快, 同时使得水印像素得到了均匀分散, 非常适合

用于水印的预处理过程中, 此外, 该算法的抗裁剪攻击能力得到了进一步提高, 易于实现, 且对于空域和变换域的水印算法均可适用。

本文首先给出了 Fibonacci 变换的定义, 并介绍了几个性质, 然后分析了 Fibonacci 变换的置乱效果, 给出了一种描述数字图像置乱程度的置乱度的定义, 并比较了 Arnold 变换和 Fibonacci 变换的置乱效果。实验表明 Fibonacci 变换的置乱效果比 Arnold 变换的置乱效果要好。最后考虑了 Fibonacci 变换在数字图像水印中的应用, 并作了一些抗攻击实验, 取得了令人满意的结果。

1 Fibonacci 变换及其性质

数列 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, …… 是 Fibonacci 数列, 它是 1202 年意大利数学家斐波那契首先提出来的, 近百年来它的性质和应用引起了广泛的关注和探讨。本文结合一些文献, 利用该数列独特的良好性质, 将其应用在数字图像水印的研究中。下面给出 Fibonacci 数列和 Fibonacci 变换的精确数学定义。

定义 1^[8] 设 $F_0 = 1$, $F_1 = 1$, $F_n = F_{n-1} + F_{n-2}$, $n \geq 3$, 则数列 $\{F_n\}$ 称为 Fibonacci 数列。

定义 2^[9] 设 F_n, F_{n+1} 是 Fibonacci 数列中的两个相邻数, 称以下变换:

$$S_k = (kF_n + r) \bmod F_{n+1} \quad (1)$$

为 Fibonacci 变换。这里 r 可作算法中密钥的一部分:

* 收稿日期: 2004-07-01

基金项目: 国家 973 资助项目 (2002CB312104); 北京市自然科学基金资助项目 (4002011); 北京市科技新星计划资助项目 (2000107); 北京市科技发展计划资助项目 (KM2003100069027)

作者简介: 商艳红 (1979 年生), 女, 硕士研究生; E-mail: yh_shang@126.com

$r = 0, 1, 2, \dots, F_{n+1} - 1, k = 0, 1, 2, \dots, F_{n+1} - 1$
由定义可以看出, 该变换可将数列 $\{Q\} = (0, 1, 2, \dots, F_{n+1} - 1)$ 变换成另一新数列 $\{S\} = (S_0, S_1, S_2, \dots, S_{F_{n+1}-1})$, 且可以证明数列 $\{S\}$ 是数列 $\{Q\}$ 的一个新的伪随机置换^[9]。下面介绍 Fibonacci 变换具有的 2 个独特性质。

1.1 Fibonacci 变换的周期性

数列经过相同的变换 N 次后, 能够变换回原始数列, 则认为该变换具有周期性, 最小的 N 即为该变换的周期。测试了 Fibonacci 变换的周期性, 部分周期如表 1 所示。

表 1 Fibonacci 变换的部分周期表

Tab 1 The part periodic table of the Fib. transformation						
N	F_n	$r=0$	$r=1$	$r=2$	$r=3$	$r=4$
8	21	2	6	6	2	6
9	34	4	4	4	4	4
10	55	2	22	22	22	22
11	89	4	4	4	4	4
12	144	2	16	8	16	4
13	233	4	4	4	4	4
14	377	2	58	58	58	58
15	610	4	4	4	4	4
16	987	2	42	42	14	42

表 1 显示: 当 $r=0$ 时, Fibonacci 变换的周期为 2 或 4。文献 [9] 对此从理论上给出了数学证明。而当, Fibonacci 变换的周期则要复杂些, 这恰恰为增加密钥空间提供了方便。

1.2 Fibonacci 变换的均匀性

如果把数列首尾相接构成一循环数列形式, 则循环数列中相邻的数或等循环距离^[9]的数通过 Fibonacci 变换, 被均匀地分散到变换后的循环数列中。在新的循环数列中仍等循环距离, 且尽可能的远。如定义 2 中当密钥 $r=0$ 时, 数列

$\{Q\} = (0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12)$

Fibonacci
↓
变换

$\{S\} = (0, 8, 3, 11, 6, 1, 9, 4, 12, 7, 2, 10, 5)$

在循环数列 $\{S\}$ 中, 将原来相邻的数 (1, 2) 和 (3, 4) 变换成 (8, 3) 和 (11, 6), 循环距离仍然相等且为最大值 5。文献 [9] 给出了这一性质的详细数学证明。

2 Fibonacci 变换在图像置乱中的应用

文献 [9] 研究了 Fibonacci 变换在数字图像置乱中的应用, 这里我们试图定量地讨论 Fibonacci 变换的置乱效果。首先我们给出数字图像置乱度的

定义, 然后比较了 Fibonacci 变换和 Arnold 变换的置乱效果。实验结果表明, Fibonacci 变换的置乱效果比 Arnold 变换的置乱效果要好。

2.1 置乱度定义

文献 [10] 给出了一种置乱度的定义——灰度差分熵, 该定义是对灰度差分直方图的分析得出的。其建立步骤如下:

- (1) 统计位移量为 d 的像素之间的灰度差;
- (2) 统计同一灰度差的像素对数;
- (3) 建立灰度差分直方图, 横坐标为各级灰度差, 纵坐标为对应灰度差的像素对数。

依据该直方图, 定义置乱度 SH 计算公式为:

$$SH = - \sum_{i=0}^{255} p_i \log_2 p_i$$

这里 p_i 为各级灰度差的分布概率。

上述灰度差分熵所测数据虽然较好地刻画了图像的置乱效果, 然而, 我们认为置乱度应是一种对置乱效果的定量描述。也就是说, 置乱度不应受原图的影响, 其标准化或归一化问题是非常重要的。为此, 我们给出如下改进的定义。

定义 3 在数字图像矩阵中, 某一矩阵元素和距其 $k-1$ 个元素的距离称之为 k 阶距, 相邻元素之间的距离称之为 一阶距。

定义 4 位移量 d 以 k 阶距建立的灰度差分直方图称之为 k 阶距灰度差分直方图, 由此直方图计算的灰度差分熵称之为 k 阶距灰度差分熵。

为了提高计算精确度, 我们以八邻域像素对统计灰度差, 对上面的计算公式作如下修改:

定义 5 数字图像的置乱度定义为:

$$SH' = \frac{SH_{old}}{SH_{new}} \tag{2}$$

其中, SH_{old} 为置乱前灰度差分熵, SH_{new} 为置乱后灰度差分熵。计算公式分别如式 (3), (4):

$$SH_{old} = (SH_{old,1} + SH_{old,2}) \tag{3}$$

$$SH_{new} = (SH_{new,1} + SH_{new,2}) \tag{4}$$

这里, $SH_{old,1}$ 、 $SH_{old,2}$ 、 $SH_{new,1}$ 、 $SH_{new,2}$ 分别是置乱前一阶距、二阶距灰度差分熵, 以及置乱后一阶距、二阶距灰度差分熵。

灰度差分直方图反映了图像灰度的空间组织信息。需置乱的图像都表达了一定的信息, 因此一阶距、二阶距灰度差分直方图都集中在差值为 0 的附近, 使得 0 附近分布概率较大; 而置乱后的图像“杂乱无章”, 所得两灰度差分直方图分布较均匀。由熵的意义可知, 熵反映了各级灰度差分布概率 p_i 的一致性。当各级分布概率 p_i 接近相等时, 置乱后灰度差分熵 SH_{new} 值较大, 对于同一幅图像而

言, SH_{old} 值是固定的, 因此在该公式中, 置乱度 SH' 越小置乱效果越好; 反之, 置乱度 SH' 越大置乱效果越差, 当 SH' 为 1 时, 图像没有被置乱或恢复到原图像。

我们之所以选取一阶距和二阶距灰度差分熵的平均值来计算置乱度, 是因为从人的视觉上考虑, 只有细小的图像结构得到置乱了, 整幅图像的置乱效果才能令人满意。因此, 我们只需比较位移量较小的灰度差分直方图就能逼真地刻画; 此外平均值的计算使得计算结果较准确的反映实际图像信息。

2.2 改进置乱度的几点优势

(1) 置乱度 SH' 满足图像旋转不变性。

证明 图像作旋转即将原像素 (x, y) 变换到 (X, Y) 可用

$$\begin{bmatrix} X \\ Y \end{bmatrix} = \begin{bmatrix} \cos \theta & -\sin \theta \\ \sin \theta & \cos \theta \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \quad (5)$$

表示。这里 θ 为 90° 、 180° 、 270° 分别表示图像逆时针旋转的度数。在 (i, j) 八邻域中以逆时针旋转 90° 为例, 经简单计算可知: 相邻像素仍然相邻。故灰度差分直方图不变, 即旋转后一阶距灰度差分熵, 二阶距灰度差分熵不变, 因此置乱度 SH' 不变。当 θ 为 180° 、 270° 时, 同理可证。综上, 图像经旋转变换后, 置乱度 SH' 不变。

无论图像是否旋转, 图像信息都明显的表达出来, 这一旋转不变性非常符合人类的视觉感官效果, 是评价置乱度的一条基本要求。

(2) 当且仅当置乱度 SH' 为 1, 置乱变换恢复到原始图像或其旋转图像。由于我们对灰度差分熵作了归一化处理, 当置乱图像恢复到原图时, 灰度差分熵等于原图的灰度差分熵, 故此时置乱度 SH' 为 1。由置乱度的旋转不变性, 当置乱度 SH' 为 1 时, 恰好是原图或原图的旋转图像。这一良好的性质可以指导我们对置乱变换周期性的检测。

(3) 置乱度 SH' 在 0.7 附近可看作一幅效果满意的置乱图像。经大量实验数据验证, 我们认为置乱度基本不受图像尺寸和原始图像的影响。一般情况下, 置乱度 SH' 在 0.7 附近即可看作一幅效果满意的置乱图, 当然 SH' 越小效果越好。

2.3 改进置乱度与置乱效果比较

从表 2 可以看出: ①该置乱度计算量小, 能从图像的细小空间结构上反映置乱效果, 测试数据和人的视觉一致, 可满足一定的加密度量指标; ②对原灰度差分熵的归一化处理规范了图像置乱的度量, 是置乱效果的一种定量分析; ③Arnold 变换需要进行多次置乱才能达到较好的置乱效果, 周期较长; 而 Fibonacci 变换只需做一次变换就可达到满

意的置乱效果, 速度很快, 从而满足网络的实时性要求, Fibonacci 置乱算法具有一定的优势。

表 2 144×144 和 233×233 Lena 图置乱度 SH'
Tab 2 144×144 and 233×233 Lena image scrambling degree

置乱次数	144×144 Lena		233×233 Lena	
	Arnold 变换	Fibonacci	Arnold 变换	Fibonacci
1 次	0.948558	0.739332	0.944511	0.681453
2 次	0.832313	1	0.815214	0.993367
3 次	0.769123		0.732049	0.681308
4 次	0.744451		0.694699	1
5 次	0.737061		0.681528	

3 Fibonacci 变换在图像水印中的应用

由于当密钥取 0 时, Fibonacci 变换的周期只有 2 或 4, 该算法只要变换一次就可以达到令人满意的置乱效果, 大幅度地提高了算法的速度; 除此之外, Fibonacci 变换的均匀性可使错误像素均匀地分散到整幅水印中。这两点是水印图像预处理中的关键要求, 而基于 Fibonacci 变换的置乱算法都能够得到很好的解决, 因此, 我们认为该置乱算法非常适用于水印图像的预处理。

3.1 水印的嵌入及提取算法

下面以一种简单的空域算法——融合技术^[10, 11]为例说明 Fibonacci 变换的置乱算法在数字图像水印中的应用效果。基本的融合技术可表述为:

$$S = t \times W + (1 - t) \times G \quad (0 \leq t \leq 1) \quad (6)$$

其中, S 为融合后的图像, W 为水印图像, G 为载体图像, t 为嵌入水印的比例因子。显然, t 接近 0 时, 融合后的图像 S 接近载体图像 G 。融合的两幅图像需要尺寸相同。其水印的提取算法可用

$$W' = \frac{S - tG}{1 - t} \quad (7)$$

表示, 为了使水印像素得到均匀分散, 利用 Fibonacci 变换我们给出了一种改进的融合水印及其提取算法。

设灰度级水印图像及公开载体图像分别为

$$W = \{W_{ij}, i = 0, 1, \dots, M_w - 1, j = 0, 1, \dots, N_w - 1\}$$

$$G = \{G_{ij}, i = 0, 1, \dots, M_g - 1, j = 0, 1, \dots, N_g - 1\}$$

为了简化算法, 我们取载体图像的大小为 Fibonacci 数列中的数。改进的嵌入及提取算法的步骤可以描述如下:

(1) 用 Fibonacci 变换将水印图像的像素位置打乱; 利用式(1)将水印图像的行列分别作变换, 选取 F_{n+1} 为载体图像的宽 M_g 和 N_g 高, 置乱算法可表述如下:

$$X_i = (i \times g(M_G) + r) \bmod M_G$$
$$i, r \in (0, 1, 2, \dots, M_W - 1)$$
$$X_j = (j \times g(M_G) + r) \bmod N_G$$
$$j, r \in (0, 1, 2, \dots, N_W - 1)$$

这里, $g(x)$ 为 x 的前一个 Fibonacci 数, r 是置乱密钥, 这样做的目的是将水印图像的像素扩散到载体图像大小的空间域上, 使得水印图像像素有更广泛的分散空间, 且置乱后的水印图像与载体图像尺寸相同。例如数列 $\{0, 1, 2, 3\}$ 可用计算式 $X_i = (i \times 89) \bmod 144$ 分散到 144 的空间上为 $\{0, 89, 34, 123\}$ 。

(2) 利用融合式 (2) 将置乱后的水印与公开载体图像融合嵌入。比例因子 t 选用 0.1, 嵌入时出现的小数灰度值以四舍五入法量化为 0 到 255 上。

(3) 用提取式 (3) 结合载体图像提取嵌入的水印图像。对于计算中出现灰度值超过 255 或小于 0 的情况, 分别将其量化为 255 或 0 来保证图像数据的正确性。小数灰度值仍然以四舍五入法处理。

(4) 借助 Fibonacci 变换的周期性将提取的水印图像恢复成水印。

3.2 实验结果与攻击实验

实验图像显示: 提取的水印从视觉上看基本没有变化。此外, 我们对嵌入水印的图像也做了一些处理, 测试了 Fibonacci 变换在水印预处理中所起到的积极作用 (图 1, 2)。

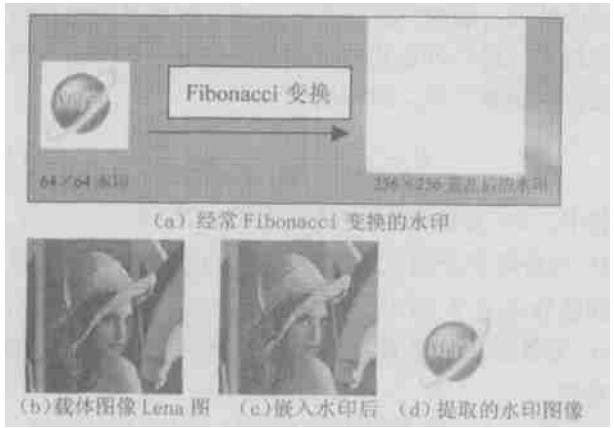


图 1 改进水印嵌入实例

Fig. 1 An improved watermark embedding example

4 结 论

本文讨论了 Fibonacci 变换的置乱效果和在数字图像水印中的应用, 定性和定量地说明了 Fibonacci 变换在数字图像置乱和数字水印嵌入中的优越性。今后我们将考虑 Fibonacci 变换在多媒体信息隐藏中的应用。

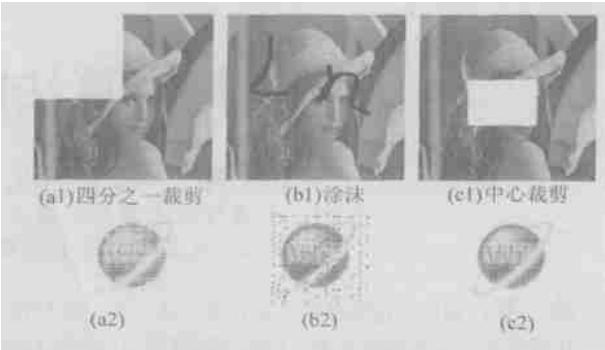


图 2 抗攻击实验

Fig. 2 Anti-attack experiment

(a1) 1/4 裁剪; (b1) 涂沫; (c1) 中心裁剪;
(a2), (b2), (c2) 对应提取的水印图像

参考文献:

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

[2] 丁玮, 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] 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.

[4] 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, 1(13): 14-16.

[5] 邹建成, 齐东旭, 熊昌镇. 基于面包师变换的数字图像加密[J]. 北方工业大学学报, 2003, 15(1): 6-10.

[6] 闫伟齐, 邹建成, 齐东旭. 一种基于 DES 的数字图像置乱新方法[J]. 北方工业大学学报, 2002, 11(1): 1-7.

[7] 熊昌镇, 邹建成. 基于抽样术的数字图像置乱技术[J]. 信息隐藏全国学术研讨会(CIHW2002)论文集, 北京: 机械工业出版社 2002: 216-223.

[8] BERGUM G E. Applications of Fibonacci[J]. Numbers, 1991(4). 柏森, 曹长修, 等. 基于骑士巡游变换的数字图像细节隐藏技术[J]. 中国图像图形学报, 2001, 6(11): 1096-1100.

[9] ZOU J C, WARD R, QI D X. A novel digital image scrambling method based on Fibonacci sequence [C]. Proceedings of the 2004 IEEE International Symposium on Circuits and Systems, Vancouver, Vol. III: 965-968..

[10] 陈昭炯, 薛小谭. 数字水印的一个采样型算法[J]. 福州大学学报(自然科学版), 2001, 29(4): 34-42.

[11] 丁玮, 闫伟齐, 齐东旭. 基于置乱与融合的数字水印隐藏技术及其应用[J]. 中国图像图形学报, 2000, 5(8): 644-649.

(下转第 155 页)

藏系统的安全性. 信息隐藏(CIHW2002), 北京: 机械工业出版社, 2002: 28— 33.

[10] WESTFELD A, PFITZMANN A. Attacks on Steganographic Systems[J] . Lecture Notes in Computer Science, 2000, 1768: 61— 75.

[11] JESSICA F, MIROSLAV G, DAVID S. Higher order statistical steganalysis of palette images[C] . Proc EI SPIE Santa Clara, 2003: 178— 190.

Statistical Security Comparison of Steganographic Algorithm on GIF Images

DING Wei¹, KONG Xiang wei¹, YOU Xin gang^{1,2}, HU Lan²

(1. Dalian Univeraity of Technology, Dalian 116024, China;
2. Beijing Institute of Electronic Technology and Application, Beijing 100091, China)

Abstract: The principle of steganography on GIF images is introduced in this paper. Some familiar steganographic methods based on GIF images are compared by the detecting methods on one dimension statistical character and multiple dimension statistical character. The results of experiments indicate that data hiding methods on modifying indices of images have better security than methods on modifying indices and palette of images together. The steganographic method presented by Fridrich is more secure than EZ Stego because it uses the optimal parity assignment.

Key words: steganography; GIF images; palette; index; security

(上接第 151 页)

Fibonacci Transformation and Its Applications in Digital Image Watermark

SHANG Yan hong, LI Nan, ZOU Jian cheng

(CAD Research Center, North China University of Technology, Beijing 100041, China)

Abstract: A digital image scrambling method based on Fibonacci transformation is proposed. By considering its favorable property of uniformity, this paper tries to present a definition of the image scrambling effects and to compare the scrambling effects of Fibonacci transformation with those of the Arnold transformation. The experimental results show that Fibonacci transformation is better than Arnold transformation. The application of Fibonacci transformation in image watermark is also considered. The watermarking embedding algorithm is robust to some anti attack tests.

Key words: Fibonacci transformation; image scrambling; digital watermark