

基于 Walsh 变换的图像置乱程度评价方法^{*}

柏 森^{1,2}, 廖晓峰²

(1. 重庆大学计算机学院, 重庆 400044)

(2. 重庆通信学院, 重庆 400035)

摘 要: 图像的置乱变换在信息隐藏和数字水印中有广泛的应用, 对图像置乱程度的评价是非常重要的, 它能帮助判定用怎样的置乱变换和对图像进行多少次置乱, 才能获得好的信息隐藏隐蔽性和鲁棒性。利用 Walsh 变换的能力集中特性, 并考虑置乱程度应满足的性质, 提出了基于 Walsh 变换的图像置乱程度评价方法, 实验表明所给出的评价方法能较好地刻划图像的置乱程度, 与人的主观评价更接近。

关键词: 信息隐藏; 数字水印; 置乱变换; 图像置乱程度; Walsh 变换

中图分类号: TP391 **文献标识码:** A **文章编号:** 0529-6579 (2004) S2-0058-04

信息隐藏是信息安全领域的一个新方向, 它在网络通信中保护信息不受破坏、不被篡改, 将起到重要作用。信息隐藏是网络环境下把机密信息隐藏在大量其他信息中不让对手发觉的一种方法, 数字水印技术是数字作品版权保护的重要措施。

图像是含有大量信息的信息载体, 此所谓: “千言万语不及一幅图”。因此图像的隐藏与伪装技术是一个非常重要的研究领域, 而图像的置乱变换既可作为一种常见的图像加密方法, 又可作为进一步隐藏的预处理, 是一种值得深入研究的方法。已有很多文献提出了图像置乱的方法^[1-4], 如文献 [1] 提到的 Arnold 变换、Hilbert 曲线变换、E-曲线变换, 文献 [2] 提出的几何变换, 文献 [4] 提出的 Fibonacci 变换等, 这些置乱变换置乱图像后的直观效果各不相同。在数字水印中, 也常以图像信息(如公司徽标, 企业产品商标等)作为水印信息。为了增强水印的鲁棒性, 也需要先将作为水印的图像进行置乱。一般地, 图像置乱的效果越好, 将其作为秘密信息隐藏在载体信息后, 其隐蔽性越好, 抗检测能力越高; 将其作为水印嵌入到被保护媒体后则鲁棒性越强。因此, 对置乱程度的研究在信息隐藏领域有重要的理论和实际意义。文献 [5] 提出了用不动点、自然率、k 阶位移因子、k 阶矩、置乱矩阵的相关性等方法来进行图像置乱程度的评价。文献 [6] 提出了用均值和方差之比来定义置乱程度, 但都没有找到一种十分理想的置乱程度评价方法。

本文首先提出了理想置乱变换和置乱程度的定义, 然后提出了基于 Walsh 变换的图像置乱程度评价方法。实验表明, 所提出的方法能较好地刻划图像的置乱效果。

1 理想的图像置乱变换及置乱程度

为了较准确地评价图像置乱方法的好坏, 这里简单分析一下理想的置乱变换及置乱程度的定义。

设 256 级灰度图像 A 经置乱变换 T 变为 B , $f_A(v)$ 表示图像 A 中灰度值为 v 的像素个数, $v = 0, 1, 2, \dots, 255$ 。

定义 1 取图像 B 的任意区域 D , 用 $f_{BD}(v)$ 表示在图像 B 的区域 D 中灰度值为 v 的像素数。若对每个 v 有

$$\frac{f_{BD}(v)}{\|D\|} = \frac{f_A(v)}{n \times m}$$

其中, $\|D\|$ 表示区域 D 中的像素数。则称 T 为最佳置乱变换, 或理想置乱变换。

定义 2 图像 $A = [a(x, y)]_{n \times m}$ 被置乱变换 T 变到了图像 B , 其置乱程度定义为

$$s = \min_D \left(1 - \sum_{v=0}^{255} \left| \frac{f_{BD}(v)}{\|D\|} - \frac{f_A(v)}{n \times m} \right| \right) \quad (1)$$

由上述定义 1 和定义 2, 不难得到如下的性质。

性质 1 $0 \leq s \leq 1$ 。

性质 2 当达到理想置乱时, $s=1$ 。

性质 1 和性质 2 可以认为是任何好的置乱程度定义应该具有的性质。性质的证明比较容易, 从

* 收稿日期: 2004-09-11

基金项目: 重庆市应用基础资助项目 (8028)

作者简介: 柏 森 (1963 年生), 男, 教授; E-mail: baixenchina@tom.com

略。定义 2 给出的置乱程度 (1) 式, 是理论上的定义, 与主观的判断相一致。因为, 它实质上表示, 图像的各灰度值在图像 B 的各区域内分布得越均匀, 其置乱程度越好。但定义 2 不便于计算。因此必须寻求新的易于计算的图像置乱程度的评价方法。

2 Walsh 变换及其性能分析

Walsh 函数是在 1923 年由美国数学家 Walsh 提出来的, 后来发展为 Walsh 变换。与傅立叶变换相比, Walsh 变换的主要优点在于存储空间少和运算速度快, 这一点对图像以及对其他大数据量进行实时处理时是非常重要的, 因此, Walsh 变换用于图像置乱程度的评价更具有计算快速的优越性。图像 Walsh 变换的定义如下。

定义 3 设图像 $A = [a(x, y)]_{N \times N}$, 则其 Walsh 变换定义为:

$$W(u, v) = \frac{1}{N} \sum_{x=0}^{N-1} \sum_{y=0}^{N-1} a(x, y) \prod_{i=1}^{n-1} (-1)^{p_i}$$

其中, $p = [b_i(x)b_{n-1-i}(u) + b_i(y)b_{n-1-i}(v)]$, $n = \log_2 N$, $b_k(x)$ 是 x 的二进制表示的第 k 位值。若定义 Walsh 变换的核矩阵为 $G = [g(x, u)]_{N \times N}$, 其中 $g(x, u) = \frac{1}{N} \prod_{i=1}^{n-1} (-1)^{b_i(x)b_{n-1-i}(u)}$, 则 Walsh 变换的矩阵形式为

$$W = \frac{1}{N^2} G \circ A \circ G \tag{2}$$

一个 8×8 矩阵的 Walsh 变换的核矩阵为:

$$\begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\ 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 \\ 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 \\ 1 & -1 & 1 & -1 & 1 & -1 & -1 & -1 \\ 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 \\ 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 \\ 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 \end{bmatrix}$$

从 Walsh 变换的核矩阵及 Walsh 变换的定义可知, 图像的 Walsh 变换实质是先对图像各列不同部分求和、求差构成新的矩阵, 然后再按行进行同样操作, 最后再乘常数因子 $1/N^2$ 。其中 $W(1, 1)$ 是图像 A 的灰度值之和的平均值。当图像的灰度值一样, 即 $a(x, y) = \text{常数}$ 时, $W(u, v) = 0$ (当 $u \neq 1, v \neq 1$ 时), 即能量集中于左上角的一点 $W(1, 1)$ 处。进一步的分析和实验表明, 当图像灰度值分布越均匀时

(根据前面的分析, 也就是当图像的置乱程度越好时), 其 Walsh 变换后的能量越集中于左上角, 因此, 可用其能量的集中性能来定义图像的置乱程度。

3 基于 Walsh 变换的置乱程度

由第 2 节的分析可知, 可用 Walsh 变换后能量的集中性能来定义图像的置乱程度, 同时考虑到置乱程度的定义应满足第 1 节给出的性质 1 和性质 2, 因此, 给出基于 Walsh 变换的置乱程度定义如下。

定义 4 假定被某种置乱变换 T 置乱后的图像 $A = [a(x, y)]_{N \times N}$ 经式 (2) 定义的 Walsh 变换后得到的矩阵 $W = [w(i, j)]_{N \times N}$, 则定义该变换置乱后的图像 A 的置乱程度为

$$S_T(A) = \frac{2w(1, 1)}{w(1, 1) + \sum_{i=1}^N \sum_{j=1}^N |w(i, j)|} \tag{3}$$

容易证明如下的定理。

定理 $0 < S_T(A) < 1$

该定理表明 (3) 式定义的置乱程度能较好满足置乱程度的性质。定理的证明比较简单, 从略。用文献 [3] 中提出的基于行列式计算思想的图像置乱算法, 对 Lena 图像进行置乱后的效果如图 1 所示, 其前 15 次置乱的置乱程度如表 1 所示。其中 0 次表示原始图像, 相应的置乱程度应理解为图像本身具有的乱度。比较图 1 和表 1, 不难发现, 按定义 4 中 (3) 式计算的置乱程度与主观评价基本一致。原始图像的乱度为 0.2463 比置乱一次的置乱程度 0.2308 大, 也是不难理解的。这是因为置乱一次时, 将原始图像灰度值变化较小的区域 (如肩部等) 拉大了的缘故。用 (3) 式对 Arnold 置乱变换 (文献 [1]) 进行计算, 可以得到类似的结论, 其前 15 次置乱的置乱程度如表 2 所示。两种置乱变换的置乱次数和置乱程度的关系如图 2 所示, 注意到基于行列式计算思想的图像置乱变换的周期为 384, Arnold 置乱变换的周期为 192。前者当置乱次数为 144 时, 达到最大置乱程度 0.7929, 后者置乱次数为 120 时, 达到最大置乱程度 0.7938。从图 2 中可以得出: ①两种置乱变换很快 (15 次置乱) 可达到较理想的置乱程度 (0.73 以上); ②置乱次数并不是越多越好, 并且置乱程度关于周期的一半有某种程度的对称性, 将其称为置乱程度或置乱变换的“半周期性”。

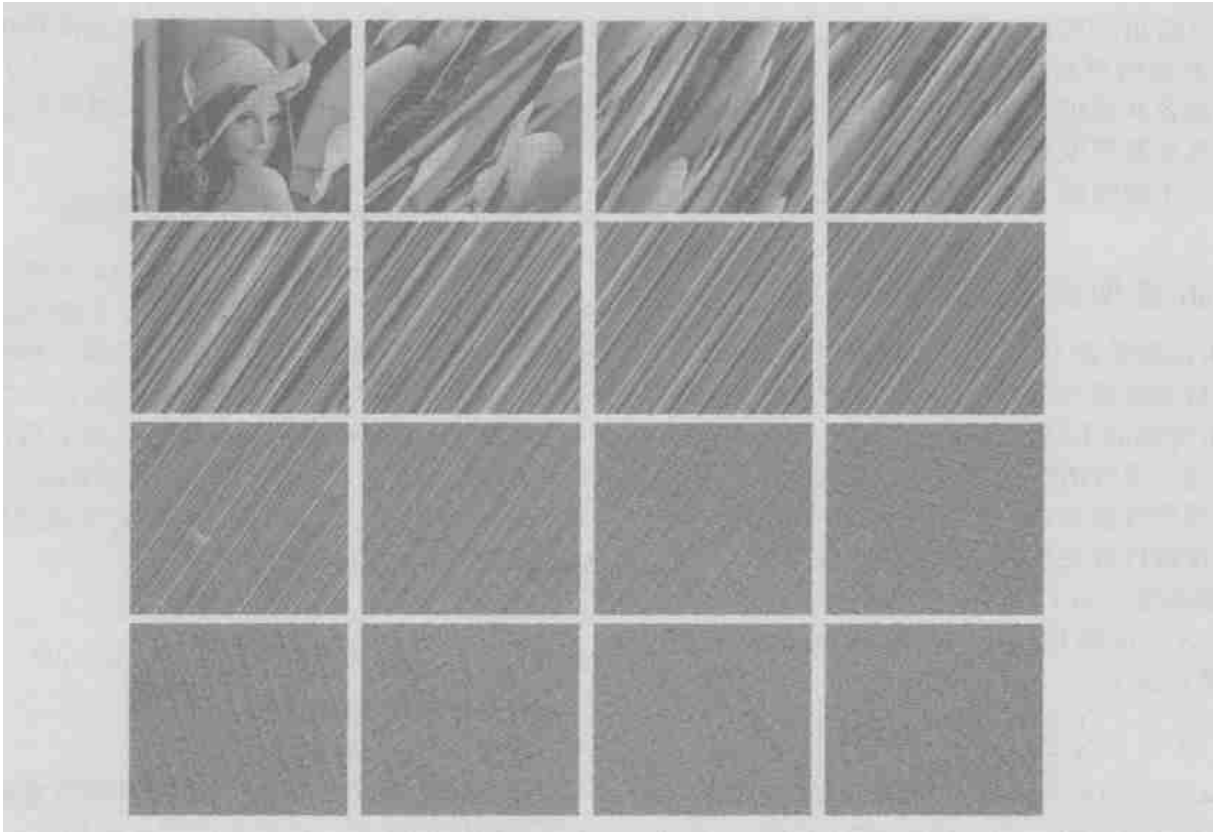


图 1 Lena 图像置乱结果

Fig 1 Results of scrambled Lena

从上到下，从左到右，依次是原始图像，置乱 1 次、2 次、…、15 次的图像

表 1 各次置乱的置乱程度

Tah 1 Images scrambling degree with the scrambling transformation

置乱次数	0	1	2	3	4	5	6	7
文献 [4] 中提出置乱程度	0.2463	0.2308	0.2543	0.2732	0.3173	0.4001	0.4812	0.5624
Arnold 变换各次置乱	0.2463	0.2421	0.2628	0.3388	0.5136	0.6900	0.7318	0.7064
置乱次数	8	9	10	11	12	13	14	15
文献 [4] 中提出置乱程度	0.6612	0.7112	0.7229	0.7292	0.7155	0.7148	0.7339	0.7358
Arnold 变换各次置乱	0.7081	0.7336	0.7352	0.7513	0.7540	0.7214	0.7342	0.7312

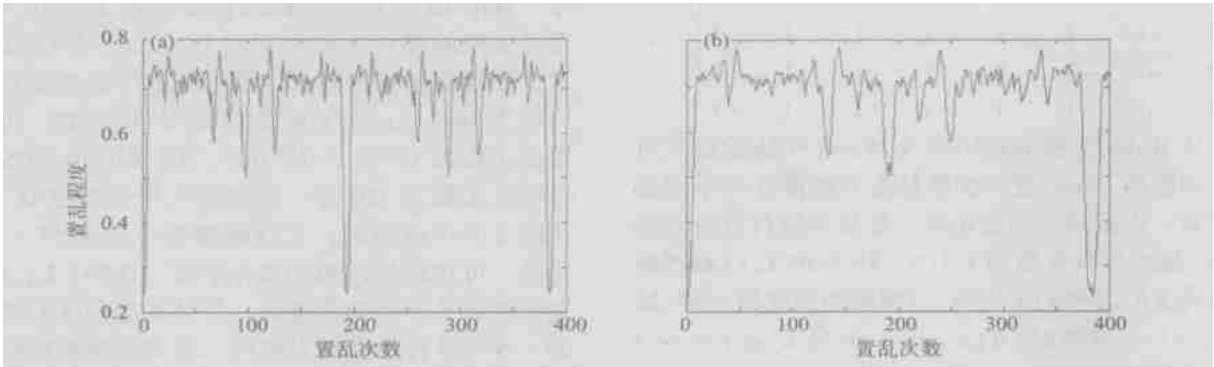


图 2 置乱次数与置乱程度的关系

Fig 2 Relation of the number of images scrambled and ISD

(a) Scrambled with transformation presented in reference [4] ; (b) Scrambled with Arnold transformation

4 结 论

本文首先从分析理想置乱变换要求出发, 得出了好的置乱程度定义应满足的性质, 然后根据 Walsh 变换的性质, 提出了基于 Walsh 变换的图像置乱程度定义。实验结果表明, 所给的定义能较好地刻画图像的置乱程度。给出图像置乱程度的更精确的定义、用理想置乱程度的思想指导我们寻求更高置乱程度的置乱变换, 以及对置乱程度和置乱变换具有“半周期性”的原理进行深入分析研究, 是我们进一步的工作。

参考文献:

[1] 丁 玮, 齐东旭. 数字图像变换及信息隐藏与伪装技术

[J]. 计算机学报, 1998, 21(9): 839— 843.
[2] 吴升, 王介生, 刘慎权. 图像的排列变换[J]. 计算机学报, 1998, 21(6): 514— 519.
[3] 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.
[4] QI D X, ZOU J C, HAN X Y. A new class of scrambling transformation and its application in the image information covering[J]. Science in China(Series E), 2000, 43(3): 304— 312.
[5] 秦红磊, 郝燕玲, 孙枫. 一种基于混沌的图像置乱网格的设计[J]. 计算机工程与应用, 2002, 38(7): 104— 106.
[6] 张华熊, 仇佩亮. 置乱技术在数字水印中的应用[J]. 电路与系统, 2001, 6(3): 32— 36.

Image Scrambling Degree Evaluation Method Based on Walsh Transformation

BAI Sen^{1,2}, LIAO Xiao feng¹

- (1. Computer College, Chongqing University, Chongqing 400044, China;
- 2. Chongqing Communication Institute, Chongqing 400035, China)

Abstract: In the context of information hiding and digital watermarking, it is of major importance to evaluate the image scrambling degree (ISD). It is helpful to decide what kind of transformation to be selected to scramble an image and how far to scramble it in order to obtain the best imperceptibility and robustness. To present a new metric for objectively assessing the ISD. The method utilizes the performance of energy concentration of Walsh transformation and takes into account the characteristics that a good ISD measurement method should be contented. Experimental results show that the proposed method is effective to assess the ISD, which correlates well with subjective assessment.

Key words: information hiding; digital watermarking; scrambling transformation; image scrambling degree (ISD); Walsh transformation