一种新的衡量图像置乱程度的方法*

卢振泰, 黎罗罗
(中山大学数学与计算科学学院, 广东 广州 510275)

摘 要: 随着图像加密技术的发展, 出现了各种各样的加密方法, 其中有基于 Arnold 变换, 仿射变换, Hilbert 曲线, 幻方, 骑士巡游, Gray 码, 混沌序列和基于频域的置乱加密技术。但是却缺少一种能有效衡量这些方法的置乱程度及反映加密次数与置乱程度关系的标准。由于图像中相邻像素之间存在的相关性随着两者间距离的增加而减小, 与原始图像相比置乱图像相邻元素的灰度值差值越大说明它的相关性越小, 从而置乱程度也就越好。基于这一点提出了一种新的判断置乱程度的方法。实验结果表明该方法能有效衡量置乱程度及反映加密次数与置乱程度的关系。

关键词: 数字图像; 图像变换; 几何变换; 置乱变换
中图分类号: TP391 文献标识码: A 文章编号: 0529-6579 (2005) S1-0126-04

计算机网络的飞速发展使数字信息的存取和共享更加快捷和方便, 同时信息安全成为人们关心的热点问题[1—4], 而信息安全中图像安全更是大家所关心的。对于具有更大信息量的数字图像, 传统的密码学尚缺少足够的研究。随着计算机技术和数字图像处理技术的发展, 已经有了不少加密方法。其中基于位置变换的有 Arnold 变换[5—7], 正交拉丁方[8], 仿射变换[9], 幻方[10], 骑士巡游[10, 13, 15], 基于像素值变化的有广义 Gray 码变换[10, 11], 混沌序列[12] 等加密技术。一般地, 图象置乱的效果越好, 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。但是, 目前仍缺少一种十分有效衡量这些方法的置乱加密效果 (置乱程度) 及反映加密次数与置乱加密效果关系的方法。

1 已有方法

文献 [14] 提出的置乱程度的表达方法: 假定图像中像素点 (i, j) 经置乱变换 T 变到了 (i', j'), 则定义变换 T 对图像的置乱程度为:

$$S_T(A) = \frac{1}{(m\times n)^{3/2}}\sum_{i=1}^{n}\sum_{j=1}^{m}\sqrt{(i-i')^2+(j-j')^2} \quad (1)$$

图 1 是由式(1) 利用 Arnold 变换对 256× 256Lena°bmp 图像加密 50 次得到的加密次数与置乱程度的关系。

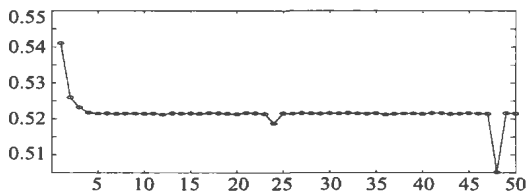

图 1 加密次数与置乱程度的关系
Fig. 1 Relationship between the enciphering effect and the number of iterations

很显然这与实际情况相矛盾, 如图 2 所示, 从直观上看, 最初的 5 次置乱后, 置乱程度是逐渐加强的, 而图 1 所示置乱程度在第一次加密时达到是大值, 而后减小。

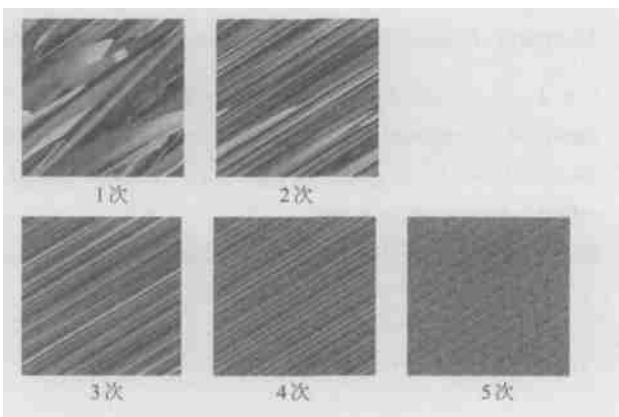

图 2 Arnold 变换加密情况
Fig. 2 The enciphering effect of Arnold transformation

* 收稿日期: 2005— 02— 02
基金项目: 国家自然科学基金资助项目 (60373082)
作者简介: 卢振泰 (1981 年生), 男, 研究生; 通讯联系人: 黎罗罗; E-mail: Luzhentai@163.com

文献 [15] 中定义的置乱度为：

$$S_r(X, X') = \frac{\sum_{i=1}^{m}\sum_{j=1}^{n}(x_{ij} - x'_{ij})^2}{\sum_{i=1}^{m}\sum_{j=1}^{n}(x_{ij} - r_{ij})^2} \quad (2)$$

其中，$X = \{x_{ij}\}_{m\times n}$ 表示原始图像，$X = \{x'_{ij}\}_{m\times n}$ 表示置乱图像，$R = \{r_{ij}\}_{m\times n}$ 表示与原始图像相同大小的均匀分布噪声图像。使用与原始图像相同大小的均匀分布噪声图像 R 作为参数。本文中计算 S_r 时，采用的是同一幅均匀分布噪声图像，因此可以只考虑分子项。分别利用仿射变换和 Arnold 变换对 256×256 图像加密 50 次，而得到的加密次数与置乱程度的关系如图 3 所示。

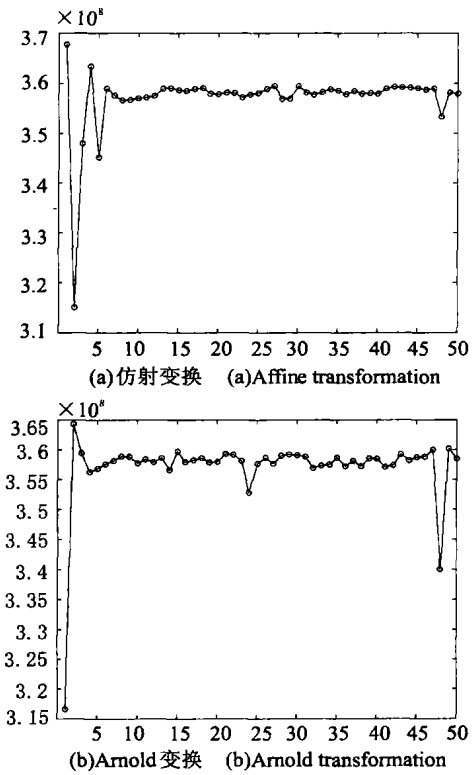

图 3　加密次数与置乱程度的关系

Fig. 3　Relationship between the enciphering effect and the number of iterations

显然，利用式 (2) 得到的仿射变换加密次数与置乱程度的关系与实际情况仍存在矛盾。Arnold 变换置乱加密 2 次时置乱程度达到最大值，这也与实际情况相矛盾 (如图 4 所示)。文 [15] 提出的方法也存在置乱程度与客观评价不一致的地方。这些表明现有的置乱程度衡量方法都不能很好地刻画图像加密次数与置乱程度的关系。

2　新的衡量方法

为了更好地反映图像加密次数与置乱程度的关系，本文提出了一种新的判断置乱程度的方法。

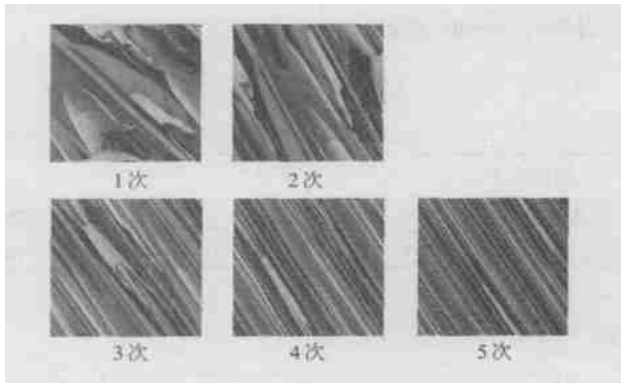

图 4　仿射变换加密情况

Fig. 4　The enciphering effect of Arndld transformation

数字图像可看作是一个矩阵，这个矩阵的元素有其特殊性，这就是相关性，即距离相近的元素，其代表的图像信息如灰度值，RGB 分量值等相差不大。根据这一性质，可以知道图像置乱程度的大小与加密后图像的相关性有关，相关性越小说明置乱程度越高，反之越低。图像的相关系数，可以直接反映任意两个像素之间的相关性，也就是在统计平均的意义上来计算它们之间的相似程度。

自相关系数平均值的曲线基本上呈指数规律衰减，即表明了相邻像素之间存在的相关性随着两者之间的距离增加而迅速减小。显然与原始图像相比置乱图像相邻元素的灰度值差值越大说明它的相关性越小，从而置乱程度也就越好。基于这一点我们得到了一种新的判断置乱程度的方法：

$$S_r = \frac{w(I') - w(I)}{w(I')},\ w = \sqrt{N_1 + N_2 + N_3 + N_4} \quad (3)$$

其中：I 为原始图像，I' 为加密后的图像，N_1，N_2，N_3 和 N_4 分别为图像的水平，垂直，主对角线，次对角线相邻元素差值的平方和。即：

$$N_1 = \sum_{i,j}(f(i,j) - f(i-1,j))^2;$$

$$N_2 = \sum_{i,j}(f(i,j) - f(i,j-1))^2;$$

$$N_3 = \sum_{i,j}(f(i,j) - f(i-1,j-1))^2;$$

$$N_4 = \sum_{i,j}(f(i,j) - f(i-1,j+1))^2;$$

对于一般的自然图像，由于存在较平滑的区域 (灰度值差别小)，而图像置乱加密破坏了这种平滑的区域。因此，一般地，有 $0 < w(I) < w(I')$。因此容易证明如下的性质。

性质 1　$0 \leqslant S_r < 1$。

性质 2　当图像没有置乱时，$S_r = 0$。

3　实验与分析

下面是利用 256×256 的标准图像根据式 (3)

分别进行 Arnold 变换和仿射变换得到的结果：

表 1 Arnold 变换和仿射变换对图像进行 1—10 次加密求得的置乱度

Tab. 1 Encrype image 1—10 using Arnold transformation and affine transformation

加密次数	1	2	3	4	5	6	7	8	9	10
Arnold 变换	0.2789	0.5414	0.6837	0.7408	0.7572	0.7637	0.7650	0.7584	0.7595	0.7623
仿射变换	0.1309	0.3189	0.4576	0.5640	0.6377	0.6900	0.7236	0.7433	0.7545	0.7598

在一个周期内的变换情况：

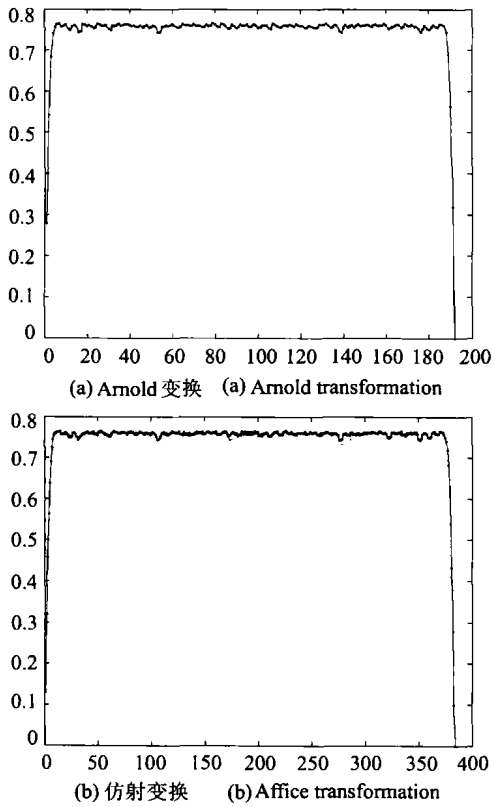

图 5 加密次数与置乱程度的关系

Fig. 5 Relationship between the enciphering effect and the number of iterations

从数据和图表中可以得出如下结论：

结论 1：Arnold 变换置乱程度优于仿射变换的置乱程度；该方法能够很好地反映加密次数与置乱程度之间的关系。

结论 2：该方法可以反映基于像素值变化的加密方法的加密次数与加密效果的关系。图 6 是利用 Gray 码变换在一个周期（周期为 8）内的变换情况。

结论 3：该方法还可以定量地反映基于频域上，混沌序列和 Gray 码变换等非置乱加密方式的置乱程度。图 7 分别是利用抽样加密 3 次，Arnold 变换对小波变换后的低频部分置乱 3 次，以及利用混沌序列[12]和广义 Gray 码变换进行加密后得到的

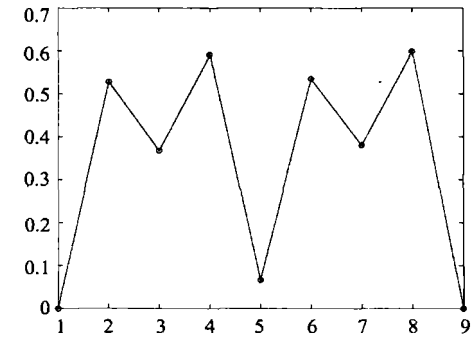

图 6 Gray 码变换加密次数与置乱程度的关系

Fig. 6 the relationship between the enciphering effect and the number of iterations using Gray transformation

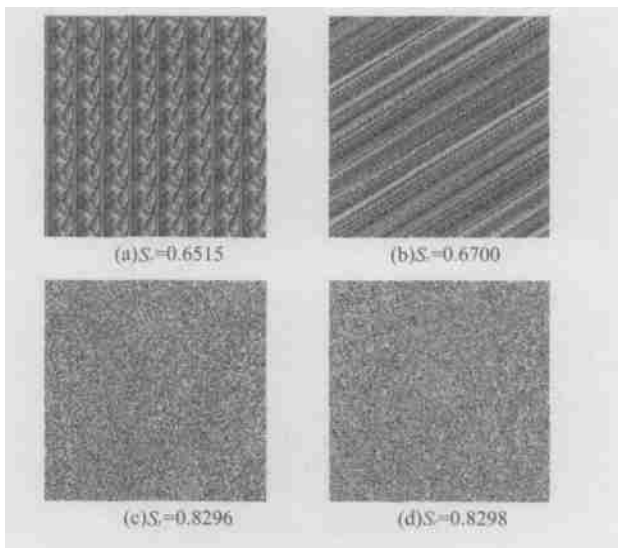

图 7 不同加密方式的加密效果

Fig. 7 The effects of different methods

结果。

结论 4：当加密次数 N 满足：$S_r(N)=\max(S_r)$时，图像的纹理性最不明显，从而达到最佳置乱程度，此时图像的安全性最高。

4 结 语

该方法能很好地反映各种方法的置乱程度及加密次数与置乱程度的关系，能够帮助我们判断为了达到最好的隐藏效果对一幅图像应该加密（置乱）到什么程度。但不同的图像利用同一变换加密得到

的结果却不同，这说明这里提出衡量方法还不够完美，因此研究一种更完美的衡量图像置乱程度的方法仍是今后要解决的一个重要问题。

参考文献：

[1] ANDERSON R J. Information Hiding：1st Int. Workshop (Lecture Notes in Computer Science)[M]. Berlin：Springer-Verlag, 1996.

[2] PFITZMANN B. Information hiding terminology, in Lecture Notes in Computer Science[M]. Berlin：Springer-Verlag, 1996.

[3] SWANSON M D, ZU B, TEWFIK A H. Robust data hiding for images[J]. Proc IEEE 7th Digital Signal Processing Workshop (DSP 96), 1996(9)：37－40.

[4] KUHN M G, ANDERSON R J. Soft tempest：Hidden data transmission using electromagnetic emanations Information Hiding 2nd Int. Workshop (Lecture Notes in Computer Science)[C]. Aucsmith D. Berlin：Springer-Verlag, 1998：124－142.

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

[6] 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)：838－843.

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

[8] 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)：14－16.

[9] 柏森, 曹长修, 柏林. 基于仿射变换的数字图象置乱技术[J]. 计算机工程与应用, 2002, 10, 74－78.

[10] 齐东旭. 分形及其计算机生成[M]. 北京：科学出版社, 1994.

[11] 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)：363－373.

[12] 易开祥, 孙鑫, 石教英. 一种基于混沌序列的图像加密算法[J]. 计算机辅助设计与图形学学报, 2000, 12(9)：672－676.

[13] 柏森, 曹长修, 曹龙汉, 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, 11(6)：1096－1099.

[14] 柏森, 曹长修. 图像置乱程度研究[C]. 全国第二界信息隐藏学术研讨会论文集. 北京, 2000.

[15] 侯启槟, 周晓旭. 基于骑士巡游的图像像素置乱算法[C]. 中国科学院自动化与信息技术学术年会, 北京, 2003.

A New Measurement for Image Encryption Effect

LU Zhen-tai, LI Luo-luo

(School of Mathematics Computational Science, Sun Yat-sen University, Guangzhou 510275)

Abstract: With the development of digital image enciphering techniques, there appeared a lot of methods including those based on Arnold transformation and affine transformation and those based on theories of Hilbert curve, Knight-tour problem and Gray code, etc. However, there are few criteria to measure the merits and demerits of these methods. In this paper some new criteria are provided to formulate the effect of existent enciphering methods. Experiments show that these criteria can also be used to measure the relationship between the enciphering effect and the number of iterations in the enciphering techniques.

Key words: digital image; image transformation; geometric transformation; scramble transformation