基于交叉熵的数字图像置乱程度评价方法

陈燕梅 张胜元
(福建师范大学数学与计算机科学学院，福州 350007)

摘 要 将交叉熵与图像的最优分块处理相结合，提出了一种基于分块交叉熵的数字图像置乱程度的评价方法。为了能用图像交叉熵反映出图像置乱效果，采用具有周期性的置乱变换进行实验，结果表明，该方法能够较好地刻画图像的置乱程度，反映了加密次数与置乱程度的关系，与人的视觉基本相符。而且对于不同的图像，该评价方法能在一定程度上反映了所用的置乱变换在各个加密阶段的效果。

关键词 数字图像 置乱变换 交叉熵 置乱程度
中图法分类号：TP391 **文献标识码**：A **文章编号**：1006-8961(2007)06-0997-05

Digital Image Scrambling Degree Evaluation Method Based on Cross-entropy

CHEN Yan-mei, ZHANG Sheng-yuan
(*School of Mathematics and Computer Science, Fujian Normal University, Fuzhou* 350007)

Abstract By unifying the cross-entropy and the image optimal block processing, a digital image scrambling degree evaluation method based on block cross-entropy is proposed. To reflect the image scrambling effect by image cross-entropy, the scramble transformations with periods are simulated. The results show that: the proposed method is effective to describe the relationship between the enciphering effect and the number of iterations in the enciphering techniques, which largely consists with human vision. For different images, when some transformation is used, this appraisal method can reflect to some extent the scrambling effects in each encryption stage.

Keywords digital image, scramble transformation, cross-entropy, image scrambling degree

1 引 言

随着计算机网络和多媒体技术的迅速发展，数字图像信息安全成为国际上热门的研究课题。数字图像置乱技术，可以看作数字图像加密的一种途径，也可以用做数字图像隐藏、数字水印图像植入、数值计算恢复方法和数字图像分存的预处理和后处理过程[1]。

现有几种数字图像置乱方法，主要是基于 Arnold 变换的系列置乱方法；用分形图形学中的方法来对空间曲线进行填充，以及利用其他数学知识和奇特现象进行数字图像置乱[2]。用这些置乱变换对图像进行置乱，直观效果各不相同。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着重要的理论和实际意义。

基于此，诸多文献对图像的置乱效果进行了探讨。文献[3]、[4]主要从像素移动的距离考虑图像的置乱度，文献[5]提出用不动点、自然率、k 阶位置因子、k 阶矩、置乱矩阵的相关性等方法来进行置乱程度的度量，但效果都不是很理想；文献[6]、[7]从

基金项目：福建省自然科学基金计划资助项目(2006J0189)
收稿日期：2005-11-18；**改回日期**：2006-02-24

第一作者简介：陈燕梅(1981～)，女。福建师范大学数学与计算机科学学院硕士研究生。主要研究方向为密码学与信息安全、图像处理。E-mail：happygirlcym@126.com

图像像素点与周围像素点灰度值偏差的角度考虑，得到了一些较满意的数据；文献[8]将熵的方法引入到图像置乱度的衡量中，提出了基于分块熵距离的分析方法。即先计算原始图像与置乱图像各分块的熵，再求两个熵值矩阵对应值差的平方和，以此作为图像的置乱度。此方法仅是用熵衡量两幅图像各自的信息，而没有从本质上体现原始图像与置乱图像之间的交互信息，也没有说明不同大小的图像应该如何分块；文献[9]在文献[8]关于差分熵的方法的基础上提出一种基于纹理特征的置乱度计算式，但缺乏置乱图像在位置上的考虑。

一般来说，置乱后图像相对于原始图像越“乱”，也就是置乱图像与原始图像的信息偏离越大，表明该置乱效果越好。这里的“乱”是相对于原始图像的视觉效果。在此基础上，本文将交叉熵与图像的最优分块处理相结合，提出了一种基于交叉熵的数字图像置乱程度的评价方法。

2 数字图像的置乱变换

一幅数字图像 P 可以看作是一个矩阵 P，矩阵元素所在的行与列，就是图像显示在计算机屏幕上的诸像素点的坐标，元素的数值就是像素的灰度（通常有 256 个等级，用整数 0 至 255 表示）。彩色图像可以取成混合矩阵，每个像素灰度值与红色（R）、绿色（G）、蓝色（B）有关，可以用 3 个数值矩阵（P^R，P^G，P^B）表示。

图像置乱变换是数字图像加密中研究比较广泛的一种方法，利用数字图像具有数字阵列的特点，搅乱图像中像素的位置或颜色使之变成一幅杂乱无章的图像，达到无法辨认出原始图像的目的。现有的数字图像置乱方法主要是在空域或频域上对图像进行置乱变换。本文以空域上像素位置变换为例介绍两种具有周期性的置乱变换算法。

2.1 基于 Arnold 变换的置乱算法

对数字图像的像素位置置乱，实际上是对对应点的灰度值或 RGB 颜色值的移动。换句话说，即将原来点(x,y)处像素的灰度值或 RGB 颜色值移动到变换后的点(x',y')处。

对于正方形图像，离散化的 Arnold 变换为[10]

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

其中，N 为图像的宽度和高度。

迭代地对一幅数字图像使用 Arnold 变换，即将左端输出的(x',y')作为下一次 Arnold 变换的输入，可得到一系列置乱图像。

2.2 基于亚仿射变换的置乱算法

亚仿射变换是基于仿射变换的思想。文献[11]给出了用于图像置乱变换的亚仿射变换。

对给定的 N 阶数字图像用 $\boldsymbol{A}=\{a(i,j)\}_{N\times N}$ 表示，若变换

$$\begin{pmatrix}x'\\y'\end{pmatrix}=\begin{pmatrix}a&b\\c&d\end{pmatrix}\begin{pmatrix}x\\y\end{pmatrix}+\begin{pmatrix}e\\f\end{pmatrix}\quad(2)$$

其中，a,b,c,d,e,f 为整数，$x,y\in\{1,2,\cdots,N\}$ 满足

条件 1　变换是离散点域$\{(x,y):1\leqslant x\leqslant N,1\leqslant y\leqslant N\}$到其自身的单映射；

条件 2　变换是离散点域$\{(x,y):1\leqslant x\leqslant N,1\leqslant y\leqslant N\}$到其自身的满映射，则称该变换为图像的亚仿射变换。

对于平面仿射几何变换，将 3 对变换点代入式(2)后就可完全确定 a,b,c,d,e,f，即可求得仿射变换的解。但并不是任意指定的 3 个变换点对都能得到亚仿射变换，文献[11]中给出了一个典型的亚仿射变换：

$$\begin{pmatrix}x'\\y'\end{pmatrix}=\begin{cases}\begin{pmatrix}1&-1\\-1&0\end{pmatrix}\begin{pmatrix}x\\y\end{pmatrix}+\begin{pmatrix}N+1\\N+1\end{pmatrix} & x<y\\ \begin{pmatrix}1&-1\\-1&0\end{pmatrix}\begin{pmatrix}x\\y\end{pmatrix}+\begin{pmatrix}1\\N+1\end{pmatrix} & x\geqslant y\end{cases}\quad(3)$$

与上述 Arnold 变换相同，可以迭代地使用亚仿射变换对数字图像进行置乱。

3 基于交叉熵的数字图像置乱程度评价方法

3.1 交叉熵[12,13]

Kullback 建议使用交叉熵（又称“相对熵”）来测定两个概率分布 $\boldsymbol{X}=\{x_1,x_2,\cdots,x_i,\cdots,x_n\}$，$\boldsymbol{Y}=\{y_1,y_2,\cdots,y_i,\cdots,y_n\}$ 之间的信息差异，交叉熵定义为

$$D(\boldsymbol{X},\boldsymbol{Y})=\sum_{i=1}^{n}x_i\log(x_i/y_i)\quad(4)$$

显然，当 $\boldsymbol{X}=\boldsymbol{Y}$ 时，交叉熵取得最小值 0，即有 $H(\boldsymbol{X},\boldsymbol{Y})\geqslant 0$。

对于两幅图像 A 和 B，分别取它们像素灰度级的概率分布 X 和 Y，则 $D(\boldsymbol{X},\boldsymbol{Y})$ 为图像 $\boldsymbol{B}$ 与图像 $\boldsymbol{A}$ 的交叉熵。两幅图像的交叉熵是评价两副图像差别

的关键指标,它直接反映了两幅图像对应像素的差异,交叉熵越小,就表示两幅图像间的差异越小。

3.2　置乱程度的评价方法

数字图像置乱的目的在于打乱图像,使得攻击者不能识别图像的内容。一般来说,若置乱后的图像相对于原始图像越"乱",表明该置乱变换就越有效。本文认为这里的"乱"是相对的视觉效果,"乱"和"整齐"的区别在于,一幅较"乱"的图像应满足与原始图像对应像素的差异较大,而"整齐"的图像正好相反。同时,位置不同灰度相同的两个像素点在观察者的眼中是没有区别的。由上述交叉熵的分析可知,若置乱图像包含的原始图像的信息越少,也就是置乱的程度越大,则交叉熵越大,表明该置乱算法越有效。如果仅是对两幅图像直接进行交叉熵的计算,则忽略了图像的空间信息,这就意味着不同的图像,尽管它们有不同的灰度值空间分布,只要有相同的灰度直方图,就会有相同的熵值,而分块处理可引入图像的位置因素。当然,如果图像被划分的块数越多,引入的空间信息也就越多,但同时也会付出计算上的代价。在图像处理中,有图像最优分块算法,如 Matlab 软件中的 bestblk 函数。本文采用了该函数对图像进行最优分块处理,恰当地引入图像的空间信息,再计算置乱度。算法如下:

(1) 读入原始图像与置乱图像的信息,将 RGB 值分别存至矩阵 $\boldsymbol{P}$ 和 $\tilde{\boldsymbol{P}}$,$\boldsymbol{P}=(p_{ij})_{m\times n}$,$\tilde{\boldsymbol{P}}=(\tilde{p}_{ij})_{m\times n}$,$p_{ij},\tilde{p}_{ij}\in\{0,1,\cdots,255\}$;

(2) 对矩阵 $\boldsymbol{P}$ 和 $\tilde{\boldsymbol{P}}$ 进行最优分块,确定分块的大小 $mb\times nb$ 和块数 t;

(3) 采用式(4),对 $\boldsymbol{P}$ 和 $\tilde{\boldsymbol{P}}$ 相对应的每一分块计算交叉熵值,$D_1,D_2,\cdots,D_t$;

(4) 用平均的交叉熵值 D 表示图像的置乱度,$D=\sum_{i=1}^{t}D_i/t$;

算法说明:(1) 以上算法可在 Matlab6.5 上仿真实现。(2) 若图像矩阵不能实现完整分块,则在底部与右侧补零,使之成为完整分块。(3) Matlab 中矩阵最优分块函数 bestblk([m,n],k)将对 $m\times n$ 的矩阵返回行列数最大值不超过 k 的最优块大小 $mb\times nb$。该函数对指定的某个 k,执行以下算法:

如果 $m\leqslant k$,则取 mb 为 m;

如果 $m>k$,考虑所有介于 min(m/10,k/2)和 k 之间的数,取 mb 为使 padding 最小化的值。

对列做同样处理得到 nb。因此,若输入的图像矩阵 $m=n$,则 $mb=nb$。

4　实验结果与分析

对于一幅 100×100 的 Lena 图像(图 1),采用上述算法进行仿真实验,结果见图 2、图 3、图 4 和表 1。

图 1　原图

Fig. 1　Primary image

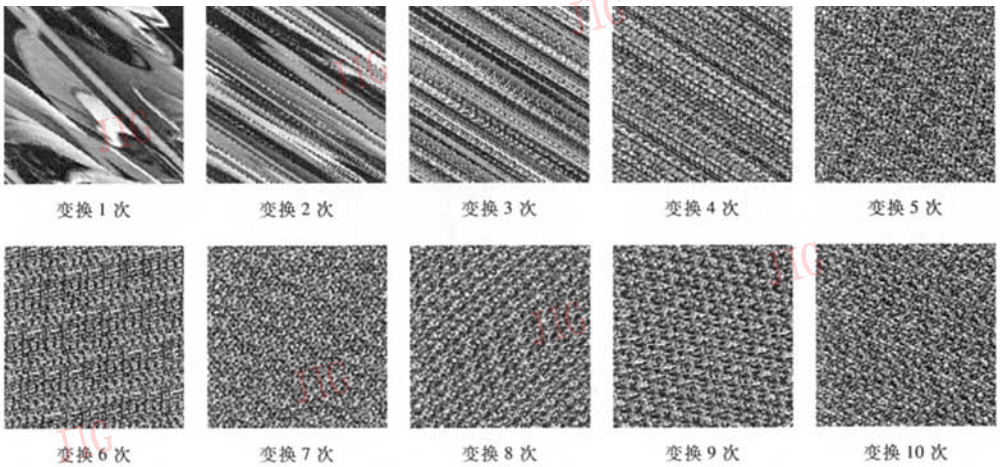

图 2　Arnold 变换加密效果

Fig. 2　The enciphering effect of Arnold transformation

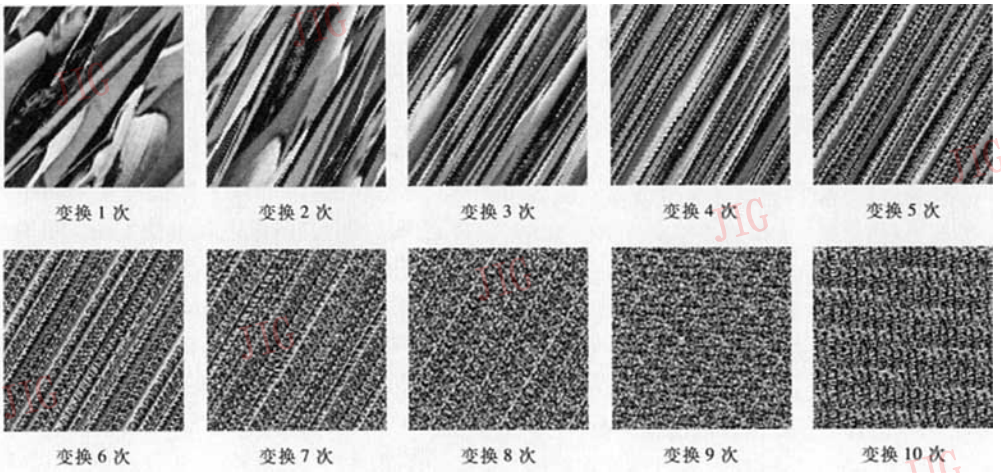

图 3 亚仿射变换加密效果

Fig. 3 The enciphering effect of Sub-affine transformation

对于上述图像,用 bestblk([100,100],8)返回行列数不超过 8 的最优块大小 5×5,计算置乱度如表 1 和图 4 所示。

表 1 Arnold 变换和亚仿射变换对图像进行加密求得的置乱度

Tab. 1 The scrambling degrees of encryption images using Arnold transformation and Sub-affine transformation

加密次数	1	2	3	4	5	6	7	8	9	10
Arnold 变换	0.034 7	0.065 2	0.073 5	0.103 6	0.117 3	0.131 3	0.126 1	0.116 7	0.101 2	0.112 3
亚仿射变换	0.022 5	0.027 7	0.036 5	0.042 9	0.060 2	0.060 4	0.066 9	0.051 7	0.072 6	0.062 4

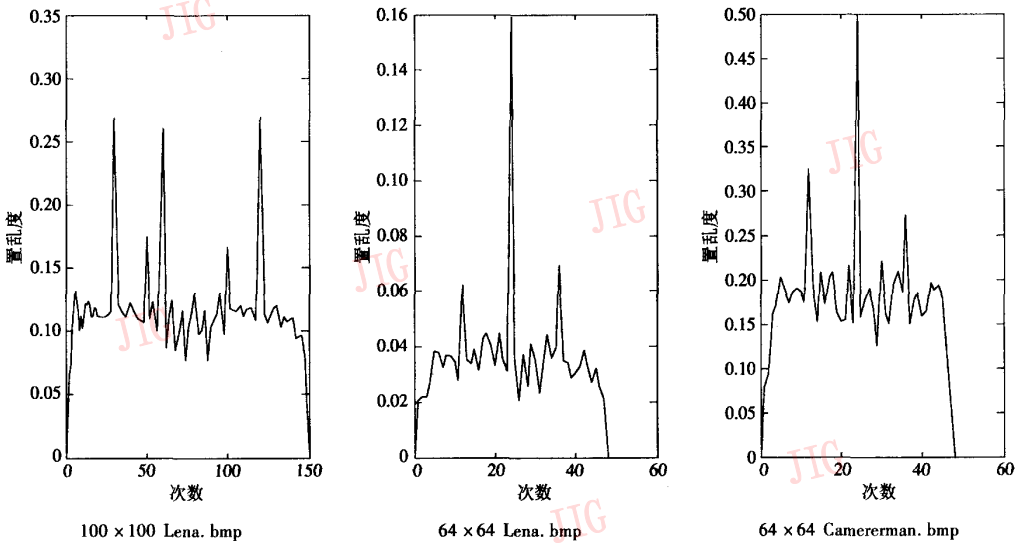

图 4 不同图像采用 Arnold 变换在一周期内的置乱度

Fig. 4 The scrambling degrees of different images in one period using Arnold transformation

从以上数据和图表可知,在开始阶段,随着加密次数的增加,置乱图像越“乱”,也就是从原始图像提取的信息越少,采用该算法计算所得的置乱度也越高。从而表明该方法能够较好地刻画图像的置乱

程度及反映加密次数与置乱程度的关系,与人的视觉基本相符。然而,不同的灰度图像采用相同的方法进行置乱变换后,得到的置乱度大小各不相同。尽管如此,该评价方法却在一定程度上反映了所用的置乱变换在各个加密阶段的效果。如图 4 中的 3 幅图在 1/4 周期、半周期、3/4 周期附近均出现了较好的置乱效果。特别是当两幅不同图像大小一致时,其置乱度的变化非常接近,如图 4 中两幅 64 × 64 的图像(置乱周期为 48)恰好都在第 12、24、36 次置乱后置乱度出现了峰值。

5　结　论

图像置乱程度的研究,对于指导我们在进行信息隐藏时,寻求更好的置乱变换有着积极的意义。本文引入了图像的空间信息,将交叉熵与图像的最优分块处理相结合,提出了一种基于分块交叉熵的数字图像置乱程度的评价方法。这种方法原理简单,易于实现。实验结果表明,该方法能够较好地刻画图像的置乱程度及反映加密次数与置乱程度的关系,与人的视觉基本相符。而且对于不同的图像,该评价方法能在一定程度上反映了所用的置乱变换在各个加密阶段的效果。当然,如果能使不同的图像利用同一变换加密后得到的置乱度相同,那将会更加直观地反映所用的置乱变换的有效性。因此,探讨一种更完善的置乱程度的衡量方法,将是今后进一步研究的主要内容。

参考文献(References)

1　Zou Jian-cheng, Li Guo-fu, Qi Dong-xu. Generalized gray code and its application in the scrambling technology of digital image[J]. Appl. Math. J. Chinese Univ. (Ser. A), 2002, **17**(3): 363 ~ 370. [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.]

2　Yan Wei-qi, Zou Jian-cheng, Qi Dong-xu. A novel digital image scrambling method base on DES[J]. Journal of North China University of Technology, 2002, **14**(1): 1 ~ 7. [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, **14**(1): 1 ~ 7.]

3　Bai Sen, Cao Chang-Xiu. A Study on Image Scrambling Degree[A]. In: Proceedings of the 3th CIHW[C]. Xi'an: Xidian University Press, 2001: 75 ~ 81. [柏森, 曹长修. 图象置乱度研究[A]. 见: 信息隐藏全国学术研讨会论文集[C]. 西安: 西安电子科技大学出版社, 2001: 75 ~ 81.]

4　Zhang Hua-xong, Qiu Pei-liang. Application of shuffling techniques within watermarking[J]. Journal of Circuits and Systems, 2001, **6**(3): 33 ~ 36. [张华熊, 仇佩亮. 置乱技术在数字水印中的应用[J]. 电路与系统学报, 2001, **6**(3): 33 ~ 36.]

5　Qin Hong-lei, Hao Yan-lin, Sun Feng. Design of picture permutation network on chaos[J]. Computer Engineering and Applications, 2002, **38**(7): 104 ~ 106. [秦红磊, 郝燕玲, 孙枫. 一种基于混沌的图像置乱网络的设计[J]. 计算机工程与应用, 2002, **38**(7): 104 ~ 106.]

6　Zhang Xiao-hua, Liu Fang, Jiao Li-cheng. An image encryption arithmetic base on chaotic sequences[J]. Journal of Image and Graphics, 2003, **8**(4): 374 ~ 378. [张小华, 刘芳, 焦李成. 一种基于混沌序列的图象加密技术[J]. 中国图象图形学报, 2003, **8**(4): 374 ~ 378.]

7　Lu Zeng-tai, Li Luo-luo. A new measurement for image encryption effect[J]. Acta Scientiarum Naturalium Universitatis Sunyatseni, 2005, **44**(sup.): 126 ~ 129. [卢振泰, 黎罗罗. 一种新的衡量图像置乱程度的方法[J]. 中山大学学报(自然科学版), 2005, **44**(增刊): 126 ~ 129.]

8　Xue Xiao-tan. A Study on Watermark Arithmetic and Application in Image[D]. Fuzhou: Fuzhou University, 2002. [薛小潭. 数字水印算法研究及在图像中的应用[D]. 福州:福州大学, 2002.]

9　Shang Yan-hong, Li Nian, Xiong Chang-zheng, *et al*. Analysis of digital image scrambling effect based on texture[J]. Journal of Wuhan University(Natural Science Edition), 2004, **51**(S1): 213 ~ 216. [商艳红, 李南, 熊昌镇等. 基于纹理特征的数字图像置乱效果分析[J]. 武汉大学学报(理学版), 2004, **51**(S1): 213 ~ 216.]

10　Ding Wei, Yan Wei-qi, Qi Dong-xu. Digital image scrambling technology based on arnold transformation[J]. Journal of Computer-aided Design and Computer Graphics, 2001, **13**(4): 338 ~ 341. [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.]

11　Bai Seng, Cao Chang-xiu. Property of sub-affine transformation and its application[J]. Journal of Computer-aided Design and Computer Graphics, 2003, **15**(2): 205 ~ 208. [柏森, 曹长修. 亚仿射变换的性质及其应用[J]. 计算机辅助设计与图形学学报, 2003, **15**(2): 205 ~ 208.]

12　Yu Ying-lin. Digital Image Processing and Pattern Recognition[M]. Guangdong: South China University of Technology, 1990: 91 ~ 94. [余英林. 数字图象处理与模式识别[M]. 广东: 华南理工大学出版社, 1990: 91 ~ 94.]

13　Kullback. Information Theory and Statistics[M]. New York: John Wiley Press, 1959.