文章编号:　1000-5013(2008)02-0203-05

基于循环矩阵思想的数字图像置乱算法

叶国栋[1], 黄小玲[2], 岳中亮[1], 朱长青[3]

(1. 广东海洋大学 理学院, 广东 湛江 524088; 2. 汕头大学 理学院, 广东 汕头 515063;
3. 南京师范大学 虚拟地理环境教育部重点实验室, 江苏 南京 2100462)

摘要:　以循环矩阵为基础, 提出一种新的图像置乱算法. 该算法借助数学知识, 从空间位置上均匀地打乱图像像素的位置, 置乱度高且偏差小. 通过对循环矩阵方法、约瑟夫遍历方法和混沌方法的数值比较实验, 表明该算法具有实现简单、操作容易、稳定性高、效果更佳等优势. 在不公开密钥 s 和 t 的情况下, 既使是公开算法, 对加密后的图像也是难以破解的. 算法可用于任意大小的方阵图像, 也可以直接推广到彩色图像, 但不适合于非方阵图像.

关键词:　图像置乱; 循环矩阵; 约瑟夫遍历; 混沌算法
中图分类号:　TP 391; O 151.21　　文献标识码:　A

数字图像置乱技术是借鉴密码学的基本思想, 将需要保护的图像直接进行置乱或分存等处理, 使其在视觉效果上不包含任何有意义的内容. 即将图像中的像素打乱成一幅杂乱无章的、难以辨别出其原始信息的图像. 它不仅可以看作是数字图像加密的一种途径, 而且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. 目前已经有较多的置乱技术, 如 Arnold 变换、Hilbert 曲线、Tangram 算法、IFS 模型、Gray 码变换等[1-4]. 这些方法能很好地隐藏图像, 也在一定程度上达到了保密的目的. 但是, 它们对图像变化少, 容易被破解[5]. 基于混沌映射思想的数字图像置乱算法[6-9]是目前的研究热点, 它是一种可逆置换, 易受量化精度的影响且很难完全保持混沌固有的特性[6]. 本文提出了一种较为简单的, 基于循环矩阵思想图像置乱算法. 它具有稳定性好、保密性强等特点, 特别对于任意大小的方阵图像, 置乱效果显著.

1　图像置乱算法思想

1.1　约瑟夫遍历方法的图像置乱

设有 n 个人围坐在一个圆桌周围, 依次编号为 1 到 n, 现从编号为 s 的人开始报数, 数到第 k 的人出列, 然后从出列的下一个人重新开始报数, 数到第 k 的人又出列. 如此重复, 直到所有的人全部出列为止. 如设 $n=8$, $s=1$, $k=4$, 则出列顺序为 4, 8, 5, 2, 1, 3, 7, 6. 若把出列顺序看成是遍历序列, 则称为约瑟夫遍历. 对一幅 $M\times N$ 的图像的约瑟夫遍历, 首先对行(或列)按照约瑟夫遍历的顺序调整各行(或列)像素的位置. 其次, 再对各列(或行)按照约瑟夫遍历的顺序, 调整各列(或行)像素的位置.

1.2　基于循环矩阵方法图像置乱

设 $\boldsymbol{C}_n=\begin{pmatrix} c_0 & c_{-1} & \cdots & c_{2-n} & c_{1-n} \\ c_1 & c_0 & c_{-1} & \cdots & c_{2-n} \\ M & c_1 & c_0 & O & M \\ c_{2-n} & \cdots & O & O & c_{-1} \\ c_{n-1} & c_{n-2} & \cdots & c_1 & c_0 \end{pmatrix}$, 如果有 $c_{-k}=c_{n-k}$, $1\leqslant k\leqslant n-1$, 则称 $n\times n$ 矩阵 $\boldsymbol{C}_n$ 为循环

收稿日期:　2007-07-17
作者简介:　叶国栋(1981-), 男, 助教, 主要从事数值代数与计算、信息安全的研究. E-mail: yegd@163.com.
基金项目:　国家高技术研究发展计划(863)项目(2006AA12Z223)

矩阵[10].

基于这一循环矩阵的思想,对任意具有上述形式的矩阵 $\boldsymbol{C}_n$,把它的对角线和平行于对角线的所有 $\boldsymbol{C}_{n-k}$, $\boldsymbol{C}_{-k}$ $(1 \leqslant k \leqslant n-1)$ 组成 n 维列向量进行提取,例如当 $k=1, 2$ 时,提取出的列向量分别为 $(c_{n-1}, c_{-1}, \cdots, c_{-1})^{\mathrm{T}}$ 和 $(c_{n-2}, c_{n-2}, c_{-2}, \cdots, c_{-2})^{\mathrm{T}}$. 对整个矩阵进行提取后得到 n 个 $n \times 1$ 列向量,然后再用一个可逆的排序算法把这 n 个列向量重新组合成一个新的矩阵,即得到想要的置乱矩阵. 但排序算法必须是可逆的,比如约瑟夫遍历等. 基于这一思想把它推广到一般的矩阵.

例 **1** 设 $\boldsymbol{A}=\begin{pmatrix} a & b & c & d \\ e & f & g & h \\ i & j & k & l \\ m & n & p & q \end{pmatrix}$,则可以提取到 4 组 4×1 维列向量: $(a \quad f \quad k \quad q)^{\mathrm{T}}$, $(e \quad j \quad p \quad d)^{\mathrm{T}}$, $(i \quad n \quad c \quad h)^{\mathrm{T}}$, $(m \quad b \quad g \quad l)^{\mathrm{T}}$. 再把它们分别放入 4 个列向量如 $\boldsymbol{b}_1, \boldsymbol{b}_2, \boldsymbol{b}_3, \boldsymbol{b}_4$ 中. 然后,对这 4 个列向量进行重新排列,排列后得到一个新的矩阵 $\boldsymbol{B}$. 如果可以得到 $\boldsymbol{B}=(\boldsymbol{b}_2 \quad \boldsymbol{b}_1 \quad \boldsymbol{b}_4 \quad \boldsymbol{b}_3)$,即得到置乱后的新矩阵 $\boldsymbol{B}=\begin{pmatrix} e & a & m & i \\ j & f & b & n \\ p & k & g & c \\ d & q & l & h \end{pmatrix}$.

循环矩阵的这一思想,可以运用于数字图像置乱技术,因为图像实质上就是由一个矩阵组成的. 可逆排序算法有很多,本文采用著名的约瑟夫遍历算法(JM)作为可逆的排序算法.

1.3 相邻灰度差与灰度置乱度

本文采用文[5]中相邻灰度差与灰度置乱度的概念. 图像中某像素与其相邻像素的灰度差为

$$GD(x, y) = [\Sigma[G(x, y) - D(x', y')]^2]/4.$$

上式中, (x', y') 取值为 $(x-1, y), (x+1, y), (x, y-1), (x, y+1)$; $G(x, y)$ 为坐标 (x, y) 处的灰度值. 除去图像边缘上的像素外,计算图像中其余各个像素与其相邻像素的灰度差,然后相加平均得到整个图像的平均相邻灰度差为

$$E(GD(x, y)) = [\sum_{x=2}^{M-1}\sum_{y=2}^{N-1} GD(x, y)]/[(M-2) \times (N-2)].$$

灰度值置乱度定义为

$$GDD(I, I') = [E'(GD(x, y)) - E(GD(x, y))]/[E'(GD(x, y)) + E(GD(x, y))].$$

这里, E 和 E' 分别表示置乱前、后的平均相邻灰度差

1.4 图像置乱算法

图像置乱算法有如下 3 个步骤. (1) 按照上述循环矩阵方法(CM),先对原始图($N \times N$)的矩阵提取 N 组 $N \times 1$ 维向量. 这是一个可逆过程. (2) 用一个可逆的排序算法,对第 1 步已经得到的 N 组向量施予可逆的全排列. 这里,采用约瑟夫扁历对向量组重新排序. 为了提高保密性,可在每次迭代时变化 s 和 k 这两个参数值,也就是所谓的密钥. 要想破解置乱后的保密图,就要先得得到这两个密钥. (3) 破解过程. 因为 CM 和 JM 都是可逆的,只按上面的步骤先得到密钥,再按逆进行图像恢复即可.

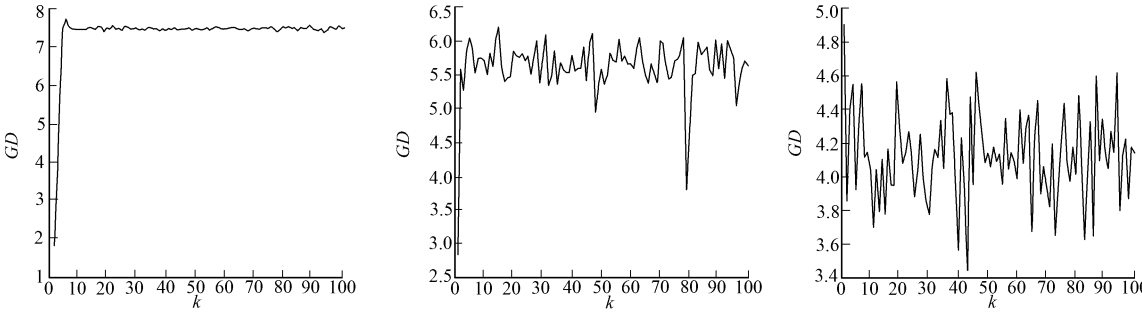
2 数值例子与评价

现在用循环矩阵方法(CM)、约瑟夫遍历方法(JM)和混沌方法(LM)3 种方法进行数值实验. 这里,LM 法采用一维 Logistic 映射, $x_{j+1}=1-2 \cdot x_j^2, x \in [-1, 1]$ 产生序列[6].

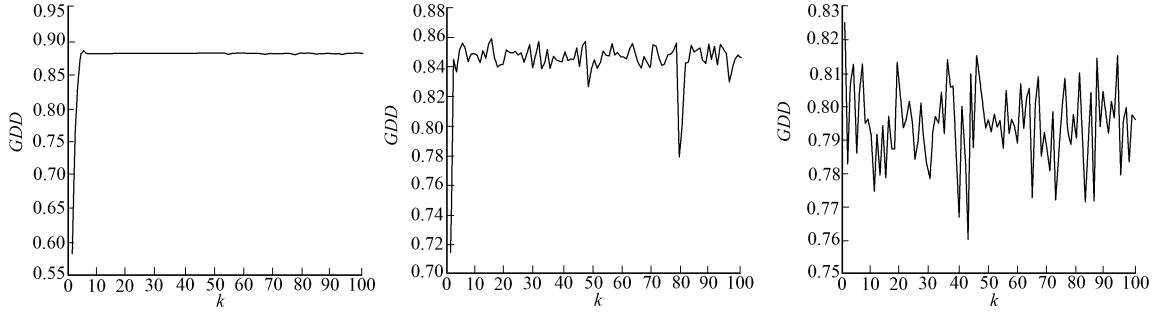
图 1 例 2 的原始图像

Fig. 1 Original image in example 2

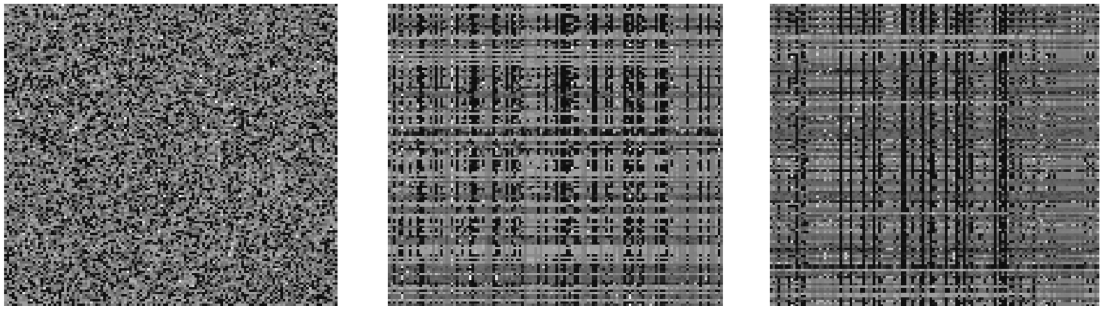
例 **2** 图 1 是以照相人的图像作为原始图,其大小为 128 px × 128 px. 图 2(a), (b), (c) 分别表示用 CM, JM(每次迭代用两次不同参数 s_1, k_1 和 s_2, k_2)和 LM 法进行置乱(迭代次数 $k=100$)后得到的灰度值变化图. 图 2(d), (e), (f) 分别表示 3 种方法的灰度置乱度变化; 图 2(g), (h), (i) 分别是用 3 种算法迭代 10 次所得到的置乱图. 从



(a) CM 的灰度差　　(b) JM 的灰度差　　(c) LM 的灰度差



(d) CM 的置乱度　　(e) JM 的置乱度　　(f) LM 的置乱度



(g) CM 的置乱结果(均匀)　　(h) JM 的置乱结果　　(i) LM 的置乱结果

图 2　例 2 的 3 种算法的数值实验比较

Fig. 1　Numerical experiment comparison of 3 algorithm in example 2

图 2(a)~(f) 的数值实验结果, 特别是图中曲线的走向可以看出, 运用 CM 的数字图像置乱算法效果比 JM 算法更好, 置乱度也更高, 更能隐藏图像信息, 稳定性也较高(除了迭代中第 1~3 次). 从图 2(g)~(i) 可以看出, CM 的置乱效果更加稳定、更加均匀. 对 3 种算法迭代前 10 次的数据进行比较, 结果如表 1 所示. 表 1 中, 灰度差的各数据均需再乘以 1 000.

例 **3**　图 3 是一幅 256 px × 256 px 作为预处理图像的军事图, 图 4(a)~(f) 是分别用 CM, JM(每次迭代使用两次不同参数) 和 LM 对图 3 所做出来的效果图(迭代 100 次). 从图 4(a) 与图 4(c), 图 4(d) 与图 4(f), 图 4(g) 与图 4(i) 的相互比较, 可得出如下结果: 相对而言, CM 法比 LM 法稳定、保密性强、置乱程度好, 更

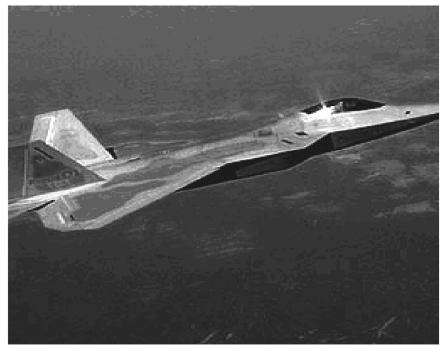


图 3　例 3 的原始图像

Fig. 2　Original image in example 3

表 1　例 2 的 3 种算法的灰度差和灰度置乱度

Tab. 1　The gray deference and gray scrambling degree of 3 algorithms in example 2

	k	1	2	3	4	5	6	7	8	9	10
	CM	1.786 3	3.462 2	5.608 8	7.488 3	7.729 1	7.469 8	7.438 6	7.421 6	7.427 9	7.425 4
GD	JM	6.507 1	5.560 5	5.594 3	6.153 8	5.081 0	5.894 8	5.956 9	5.819 1	8.390 0	6.031 9
	LM	4.902 9	3.854 5	4.396 7	4.548 1	3.923 7	4.297 6	4.551 3	4.111 9	4.144 9	4.037 3

续表

Continue table

	k	1	2	3	4	5	6	7	8	9	10
	CM	0.583 6	0.761 1	0.845 5	0.882 0	0.885 4	0.881 7	0.881 2	0.881 0	0.881 1	0.881 0
GDD	JM	0.865 4	0.844 2	0.845 1	0.858 2	0.830 8	0.852 4	0.553 8	0.850 6	0.839 7	0.855 5
	LM	0.825 2	0.782 8	0.807 0	0.812 8	0.786 2	0.803 0	0.812 9	0.795 0	0.796 4	0.791 6

适用于图像的加密. 同样, 对 3 种算法迭代前 10 次的数据进行比较, 结果如表 2 所示. 表 2 中, 灰度差的各数据均需再乘以 1 000.

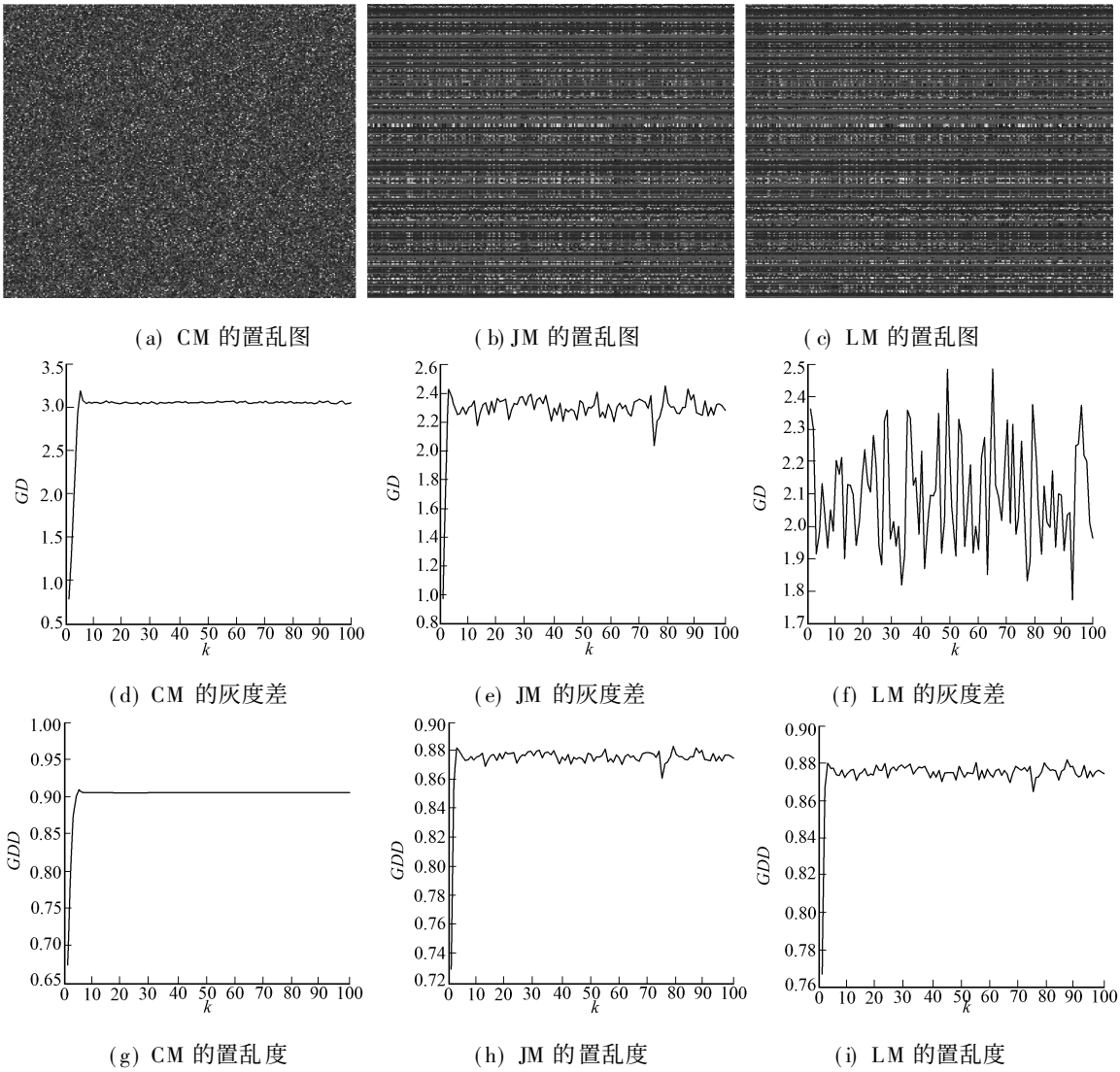


图 4 例 3 的 3 种算法置乱比较

Fig. 4 The scrambling comparison of 3 algorithm in example 3

表 2 例 3 的 3 种算法灰度差和灰度置乱度

Tab. 2 The gray deference and gray scrambling degree of 3 algorithms in example 3

	k	1	2	3	4	5	6	7	8	9	10
	CM	0.784 2	1.361 2	2.287 8	2.919 9	3.194 9	3.073 3	3.040 3	3.053 9	3.045 0	3.056 2
GD	JM	1.155 3	2.127 2	2.394 2	2.335 2	2.336 6	2.271 2	2.259 4	2.317 2	2.239 9	2.288 6
	LM	2.361 3	2.301 6	1.913 3	1.977 3	2.133 8	2.026 3	1.932 3	2.051 0	1.982 8	2.202 1
	CM	0.674 0	0.798 3	0.874 9	0.900 6	0.908 8	0.905 3	0.904 3	0.904 8	0.904 5	0.904 8
GDD	JM	0.766 5	0.866 0	0.880 1	0.877 2	0.877 3	0.874 0	0.873 4	0.876 3	0.872 3	0.874 9
	LM	0.878 5	0.875 6	0.852 2	0.856 6	0.866 4	0.859 8	0.853 5	0.861 4	0.857 0	0.870 3

3　结束语

总之, 本文提出了基于循环矩阵思想的一种新的特别的图像置乱算法. 它充分利用了数学知识循环矩阵, 具有实现简单、操作容易、稳定性高、效果更佳等优势. 由于每交迭代时不继变化 s 和 t 的值, 破解过程只要按照以上两个步骤进行返回即可, 在不公开密钥 s 和 t 的情况下, 既使是公开算法对加密后的图像是也难以破解. 此算法可用于任意大小的方阵图像, 也可以直接推广到彩色图像. 但是, 该算法也只适用于方阵图像. 因此, 对于非方阵图像的情形是继续研究的重点内容.

参考文献:

[1] 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.
[2] 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.
[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] QI Dong-xu, ZOU Jian-cheng, HAN Xiao-you. A new class of scrambling transformation and its application in the image information covering[J]. Sciences in China (E), 2000, 43(3): 304-312.
[5] 向德生, 熊岳山. 基于约瑟夫遍历的数字图像置乱算法[J]. 计算机工程与应用, 2005(10): 44-46.
[6] 刘向东, 焉德军, 朱志良, 等. 基于排序变换的混沌图像置乱算法[J]. 中国图象图形学报, 2005, 10(5): 656-660.
[7] 刘德鹏, 蔡翔云. 水印图像的混沌置乱算法[J]. 云南大学学报: 自然科学版, 2006, 28(S1): 145-148.
[8] 范延军, 孙燮华, 阎晓东, 等. 一种基于混合混沌序列的图像置乱加密算法[J]. 中国图象图形学报, 2006, 11(3): 387-393.
[9] 田　岩, 谢玉波, 李　涛, 等. 一种基于分块和混沌网的图像置乱方法[J]. 中国图象图形学报, 2007, 12(1): 56-60.
[10] CHAN R H, NG M K. Conjugate gradient methods for toeplitz systems[J]. Siam Review, 1996, 38(2): 427-482.

Digital Image Scrambling Algorithm Based on Circulant Matrix

YE Guo-dong[1], YUE Zhong-liang[1], ZHU Chang-qing[2]

(1. Institute of Science, Guangdong Ocean University, Zhanjiang 524088, China;
2. Institute of Science, Shantou University, Shantou 515063, China;
3. Key Laboratory of Virtual Geographic Environment, Nanjing Normal Univeraity, Nanjing 210054, China)

Abstract: Presenting a new image scrambling algorithm based on circulant matrix. The algorithm throwt equably the position of image pixel into confusion from space position and has high degree of scrambling with little warp. The algorithm shows many superiority such as carrying out simply, operating easily, high stability, and better effect through the comparison of numerical experiments among the circulant matrix method, Josephus traversing and chaos method. It is hard to uncoil the encrypted image when the keys s and t are not open even if the algorithm is open. The algorithm is suitable to any size of square matrix image, and also can be extended to color image, but it do not suit for the non-square matrix image.

Keywords: image scrambling; circulant matrix; Josephus traversing; chaos algorithm

(责任编辑: 黄仲一　　英文审校: 吴逢铁)