基于混沌分组的二维工程图信息隐藏算法

龙 敏[1], 彭 飞[2]
(1. 长沙理工大学计算机与通信工程学院, 湖南长沙 410076; 2. 湖南大学计算机与通信学院, 湖南长沙 410082)

摘 要: 基于混沌分组的思想, 提出一种二维工程图的信息隐藏算法. 该算法先获得工程图中的实体集, 对实体的句柄进行处理后得到混沌系统的初值和迭代次数, 根据迭代后得到的值进行分组, 对同一分组的实体重复嵌入相同隐秘信息, 从而实现信息的冗余隐藏. 试验结果表明, 该信息隐藏算法对图形修改攻击、旋转、平移以及均匀缩放等攻击具有较好的鲁棒性.

关键词: 信息隐藏; 二维工程图; 混沌
中图分类号: TP391.72 文献标识码: A 文章编号: 0372-2112 (2009) 01-0079-05

An Information Hiding Algorithm for Two-Dimensional Engineering Graphics Based on Chaotic Grouping

LONG Min[1], PENG Fei[2]
(1. *School of Computer and Communication Engineering, Changsha University of Science and Technology, Changsha, Hunan 410076, China;*
2. *School of Computer and Communication, Hunan University, Changsha, Hunan 410082, China*)

Abstract: An information hiding algorithm based on chaotic grouping is proposed. The entity set is firstly acquired from the engineering graphic, then some operations are executed to the handle of the entities, and the initial values and iteration times are gotten for iteration of the chaotic system. Group operation is processed according to the iteration results, and information hidden is achieved by embedding the same message in the entities in the same group. Simulation results show that the proposed algorithm is robust against the attacks such as modification, rotation, moving and equal scaling.

Key words: information hiding; two-dimension engineering graphic; chaos

1 引言

随着社会信息化速度的加快, 信息隐藏技术得到了广泛的发展与应用[1-4]. 工程图广泛应用于机电行业、建筑行业以及服装等行业, 它是设计师们的工作成果, 也是企业的重要资产, 其版权与图像、视频、音频以及文本一样需要得到有效的保护. 目前, 已经出现一些针对二维工程图信息隐藏的研究, 但还处于起步阶段[5]. 文献[6]提出了一种通过修改二维工程图中各实体顶点间的距离比例来嵌入信息的信息隐藏方法; 文献[7]提出了一种在文献[6]基础上改进了的信息隐藏方法. 虽然这些方法能够有效的抵抗旋转、平移、均匀缩放以及删除等攻击, 但是由于修改了顶点间的距离, 则改变了二维工程图的尺寸, 会在实际应用中影响产品的加工与制造. 文献[8]提出一种结合 HVS 修改实体线宽的工程图信息隐藏算法, 该算法无需改变二维工程图的尺寸, 但对图形修改攻击非常敏感. 本文基于混沌分组的思想提出了一种二维工程图的信息隐藏算法. 该信息隐藏算法除了拥有文献[8]算法的优点以外, 同时对图形修改等攻击具有较好的鲁棒性.

2 混沌分组与二维工程图信息隐藏

AutoCAD 是美国 Autodesk 公司的产品, 已经广泛应用于机电、建筑以及服装等行业的工程图纸设计中, 是一种典型的工程图设计软件. 这里将以 AutoCAD2006 为应用背景, 讨论基于混沌分组的二维工程图的信息隐藏.

2.1 混沌分组原理

Logistic 映射:

$$x(n+1) = a \cdot x(n) \cdot (1 - x(n)), \quad (1)$$

其中 $0 \leqslant x(n) \leqslant 1$, $n \in Z$, 当 $3.57 \leqslant a \leqslant 4$ 时, 式(1)产生的序列是混沌序列, 该混沌序列具有类似随机噪声和连续宽频谱等的特性. 也就是说, 由初始条件 x_0 在 Logistic 映射的作用下所产生的序列 $\{x(k), k = 0, 1, 2, 3, \cdots\}$ 是

收稿日期: 2007-08-20; 修回日期: 2008-08-26
基金项目: 湖南省自然科学基金(No. 08JJ4020)

非周期、不收敛的, 且对初始值非常敏感.

Schuster H. G[9]证明了式(1)当 $a=4$ 时产生的混沌序列的概率分布密度函数 $\rho(x)$ 如下式所示:

$$\rho(x)=\begin{cases}\dfrac{1}{\pi\sqrt{x(1-x)}}, & 0<x<1\\ 0, & \text{其它}\end{cases} \tag{2}$$

从式(2)可以看出, Logistic 映射生成的混沌序列具有遍历性, 同时还具有 δ-like 型自相关函数和零相关函数[10].

同时, 由式(2), 可以计算出式(1)当 $a=4$ 时产生的混沌序列在区间$(c, d]$的概率分布函数 $F(x)$ 为:

$$F(x)=\frac{2}{\pi}(\arcsin\sqrt{d}-\arcsin\sqrt{c}),\ 0\leqslant c\leqslant d\leqslant 1 \tag{3}$$

命题 **1** Logistic 映射的状态空间$[0, 1]$可以分成分布概率相等的任意 n 等分.

证明 设需要将 Logistic 映射的状态空间$[0, 1]$分成分布概率相等的 n 等分($n\geqslant 2$), 分别表示为$[0, e_1]$, $(e_1, e_2]$, …, $(e_{i-1}, e_i]$, …, $(e_{n-1}, e_n]$, 则由(3)式可得:

$$\begin{cases}\dfrac{2}{\pi}\left(\arcsin\sqrt{e_1}-\arcsin\sqrt{0}\right)=\dfrac{1}{n}\\ \dfrac{2}{\pi}\left(\arcsin\sqrt{e_2}-\arcsin\sqrt{e_1}\right)=\dfrac{1}{n}\\ \cdots\\ \dfrac{2}{\pi}\left(\arcsin\sqrt{e_i}-\arcsin\sqrt{e_{i-1}}\right)=\dfrac{1}{n}\\ \cdots\\ \dfrac{2}{\pi}\left(\arcsin\sqrt{e_n}-\arcsin\sqrt{e_{n-1}}\right)=\dfrac{1}{n}\end{cases} \tag{4}$$

则由(4)得方程有解, 并可计算得到,

$e_1=\sin^2\dfrac{\pi}{2n}$, $e_2=\sin^2\dfrac{\pi}{n}$, $e_3=\sin^2\dfrac{3\pi}{2n}$, …, $e_i=\sin^2\dfrac{i\pi}{2n}$, …, $e_n=\sin^2\dfrac{\pi}{2}=1$

证毕.

由命题 1 可知, 我们可以通过类似方法将 Logistic 映射的状态空间分成具有相同概率分布的任意 n 个子空间$[0, e_1]$, $(e_1, e_2]$, …, $(e_{i-1}, e_i]$, …, $(e_{n-1}, 1]$.

2.2 基于混沌的二维工程图实体分组

对于一个二维工程图来说, 图形由大量的实体组成, 其中每个实体都有一个在该图中唯一的被称为“句柄”(Handle)的参数, 这些值在进行图形插入、外部参照和写块操作中始终保持不变[11]. 因此, 我们从“句柄”出发将二维工程图实体分成 n 组, 分组的步骤为:

(1)获得二维工程图的第 i 个实体的句柄H_i($1\leqslant i\leqslant m$);

(2)对该实体的句柄 H_i 在密钥 K 的作用下进行处理, 使其转化成为一个$(0, 1)$之间数 x_i^0 以及一个正整数 t_i($t_i\geqslant 20$), 分别作为 Logistic 映射的初始值和迭代次数(注意: 要求 $t_i\geqslant 20$ 是为了保证 Logisitc 映射迭代到混沌区域);

(3)以 x_i^0 为 Logistic 映射的初值, 经过 t_i 迭代后得到值$x_i^{t_i}$;

(4)判断 $x_i^{t_i}$ 所处的子空间. 通过比较 $x_i^{t_i}$ 和 e_j 的大小, 如果 $e_{j-1}<g_i\leqslant e_j$, 则将实体归为第 j 组, 否则继续比较, 直到将实体归组.

(5) i 从 1 到 m, 将所有实体归为 n 组的成员.

通过上述五步, 我们就可以将二维工程图的所有实体分成 n 组, 并且, 每组的实体的个数从概率上是相等的.

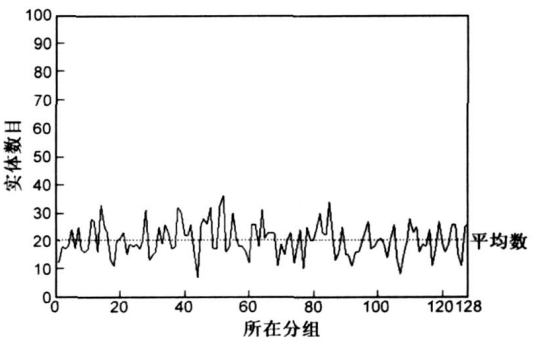

图1 工程图实体分组实际分布1

图 1 和图 2 分别是实际工程图的分组情况, 其中图 1 中 $m=2614$, $n=128$, 图 2 中 $m=8774$, $n=128$. 可以看出当 n 的取值越大, 每组所包含的实体数更加趋向均匀.

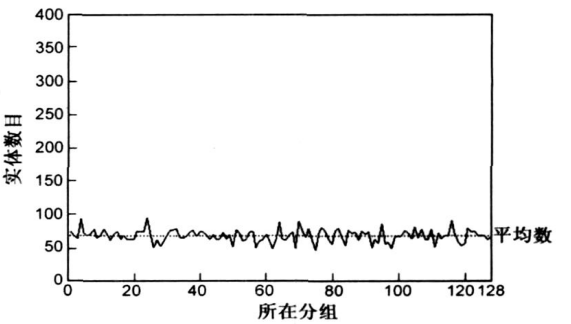

图2 实体分组实际分布2

3 基于混沌分组的二维工程图信息隐藏算法

3.1 信息隐藏算法

信息隐藏算法描述如下:

(1)将要隐藏的信息转化成为二进制序列 $M=\{m_1, m_2, \cdots, m_i, \cdots, m_n\}$, 可在密钥 K' 的作用下由 AES 算法进行加密, 得到加密后的信息 $C=\{c_1, c_2, \cdots, c_i, \cdots, c_n\}$, M 和 C 的长度均为n;

(2)在密钥 K 的作用下, 按照 2.2 所介绍的方法将

工程图 G 中的实体分为 n 组;

(3) 在所有属于第 i 组的实体中嵌入信息 m_i, 嵌入方法为: 根据序列 C 的值, 当 c_i 值为"1"时, 将所有第 i 组实体的线宽增大一级; 当 c_i 值为"0"时, 则保持所有第 i 组实体的线宽不变;

(4) 将所有信息嵌入后, 即获得含隐藏信息的二维工程图 G'.

3.2　隐秘信息检测算法

隐秘信息检测算法描述如下:

(1) 在密钥 K 的作用下, 按照 2.2 所介绍的方法将工程图 G' 中的实体分为 n 组, 因为二维工程图实体的句柄的不变性, 故此分组与 3.1 中的分组是相同的;

(2) 对所有属于第 i 组的实体中进行信息提取. 提取方法为: 假设第 i 组包括 j 个实体, 分别用 $e_k(1 \leqslant k \leqslant j)$ 表示; 比较 e_k 的实际线宽 l_{e_k} 与 e_k 所在层的标准线宽 l'_{e_k}, 如果 $l_{e_k} > l'_{e_k}$, 则 $c_i(k) = 1$; 当 $l_{e_k} = l'_{e_k}$ 时, $c_i(k) = 0$, 由此可以得到 k 个值. c_i 的值根据选举原则确定, 也就是说, 当 k 从 1 到 j, 如果 $c_i(k) = 1$ 的次数大于 $c_i(k) = 0$ 的次数, 则 $c_i = 1$, 否则 $c_i = 0$.

(3) 从所有 n 组实体中提取信息, 得到 $C = \{c_1, c_2, \cdots, c_i, \cdots, c_n\}$;

(4) 密钥 K' 的作用下由 AES 算法进行解密, 到隐秘信息 $M = \{m_1, m_2, \cdots, m_i, \cdots, m_n\}$.

4　性能分析

算法仿真在 P4 1.7G, RAM 256M, WinXP Professional, AutoCAD2006 以及其 VBA 开发环境中进行, 图 3 和图 4 分别为原始二维工程图和含隐藏信息"Hunan University"的二维工程图.

对比图 3 和图 4, 信息隐藏在工程图中是不可察觉的. 同时经过测试, 可以正确提取隐藏信息"Hunan University".

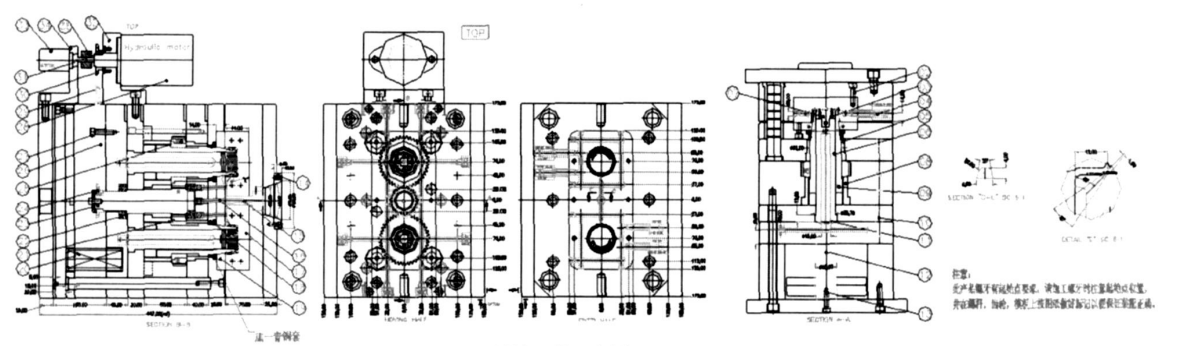

图3　原始二维工程图

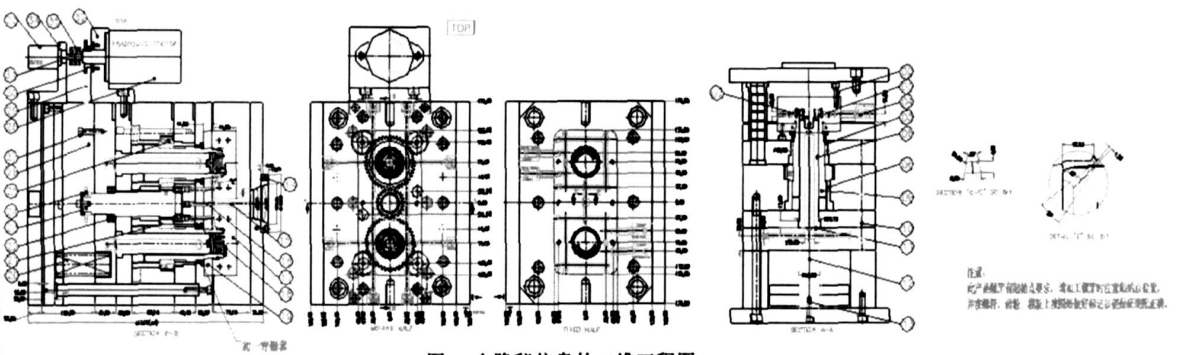

图4　含隐秘信息的二维工程图

4.1　隐藏信息容量

由于算法是通过修改线段的线宽来隐藏信息, 且每一条线段最多只能隐藏 1 比特的信息, 因此对于一个包含 n 个直线实体的二维工程图来说, 其理论可隐藏的最大信息容量为 n bit. 但是为了抵抗修改攻击, 我们采用了将实体分组的方法进行信息隐藏. 假设平均每组实体数为 w, 则实际最大可隐藏信息容量 $Capa_{max}$ 为:

$$Capa_{max} = \frac{n}{w}\text{bit} \tag{5}$$

4.2　时间复杂性分析

由于嵌入算法与检测算法是根据分组来对每条直线实体进行操作, 因此对于一个包含 n 个直线实体的二维工程图来说, 嵌入算法与检测算法的时间复杂度分别为 $O(n)$.

4.3 抗攻击能力分析

在实际应用中, 二维工程图需要进行图形修改、均匀缩放、旋转以及平移等多种操作, 因此, 需要分析该算法抵抗图形修改、均匀缩放、旋转、平移以及图形修改等攻击的能力.

4.3.1 抗均匀缩放攻击能力分析

为分析算法的抗均匀缩放攻击能力, 首先在二维工程图中嵌入隐秘信息"Hunan University", 然后将已嵌入隐秘信息的二维工程图分别进行均匀缩小和放大处理后, 再提取处理后二维工程图中的隐秘信息. 表 1 为二维工程图均匀缩放后信息提取的测试结果.

表 1 二维工程图均匀缩放后的信息提取结果

缩放倍数	1/4	1/3	1/2	1	2	3	4
测试次数	10	10	10	10	10	10	10
成功提取次数	10	10	10	10	10	10	10

由表1 可知, 对已嵌入隐秘信息的二维工程图分别进行均匀缩小和放大处理并不影响隐秘信息的提取, 从而表明了算法具有较好的抗均匀缩放攻击的能力.

4.3.2 抗旋转攻击能力分析

为分析算法的抗旋转攻击能力, 首先在二维工程图中嵌入隐秘信息"Hunan University", 然后将已嵌入隐秘信息的二维工程图分别进行多次旋转处理后, 再分别提取旋转后二维工程图中的隐秘信息. 表 2 为二维工程图经过旋转后信息提取的测试结果.

表 2 二维工程图旋转后的信息提取结果

旋转角度(度)	120	90	60	30	- 30	- 60	- 90	- 120
测试次数	10	10	10	10	10	10	10	10
成功提取次数	10	10	10	10	10	10	10	10

由表2 可知, 对已嵌入隐秘信息的二维工程图进行旋转后并不影响隐秘信息的提取, 从而表明了算法具有较好的抗旋转攻击的能力.

4.3.3 抗平移攻击能力分析

为分析算法的抗平移攻击能力, 首先在二维工程图中嵌入隐秘信息"Hunan University", 然后将已嵌入隐秘信息的二维工程图分别进行多次平移处理后, 再分别提取平移后二维工程图中的隐秘信息. 测试结果表明, 在经过平移后的二维工程图中均能正确提取隐秘信息, 表明了算法具有较好的抗平移攻击能力.

4.3.4 抗图形修改攻击能力分析

此外, 为分析算法的抗图形修改攻击能力, 首先在二维工程图中嵌入隐秘信息"Hunan University", 然后对已嵌入隐秘信息的二维工程图分别进行多次删除、添加等操作后, 再分别提出经过处理后的二维工程图中的隐秘信息. 图5 为图形删除操作与隐蔽信息成功提取率的统计关系; 图6 为图形添加操作与隐蔽信息成功提取率的统计关系. 结果表明, 在对工程图形删除少于 75%, 图形添加少于 43.75% 时, 算法均能够正确提取隐蔽信息, 表明算法对图形修改攻击具有一定的鲁棒性.

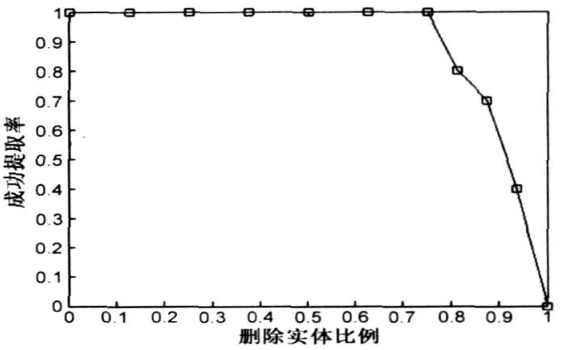

图5 抗图形删除能力分析

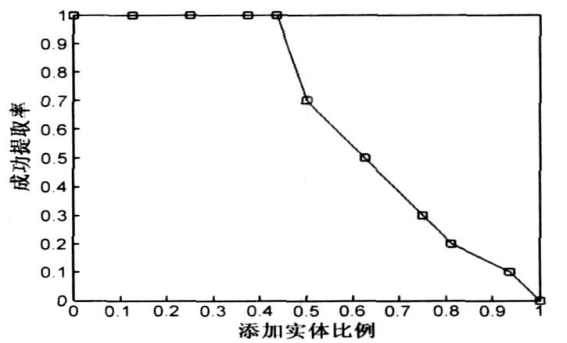

图6 抗图形添加能力分析

5 结论

文中提出一种基于混沌分组的二维工程图的信息隐藏算法, 本算法不会修改顶点间的距离, 也不会改变了二维工程图的加工尺寸, 因此不会对产品的生产和制造产生影响, 能满足实际应用的需要. 同时该算法能有效抵抗图形修改、均匀缩放、旋转和平移等攻击的能力, 该算法可望为工程图的版权保护提供了一种有效的方法.

参考文献:

[1] 郭云彪, 尤新刚, 张春田等. 面向信息隐藏的图像复杂度研究. 电子学报[J], 2006, 34(6): 1048- 1052.
Guo Yun-biao, You Xin-gang, Zhang Chun-tian, Zhou Lin-na. Study of image bit-plane complexity in the information hiding[J]. Acta Electronica Sinica, 2006, 34(6): 1048- 1052. (in Chinese)

[2] 郑国清, 刘九芬, 黄达人等. DNA 序列作为信息隐藏载体的研究[J]. 中山大学学报(自然科学版), 2005, 44(1): 5- 8.
Zheng Guo-qing, Liu Jiu-fen, Huang Da-ren, Xu An-long. A research of DNA sequences as covers of information hiding

[J]. Acta Scientiarum Naturalium Universitatis SunYaTsenI, 2005, 44(1): 5– 8. (in Chinese)

[3] 姜楠, 王健, 钮心忻, 杨义先, 周锡增. 信息隐藏模型及容量分析[J]. 计算机应用研究, 2005, (12): 116– 117.
Jiang Nan, Wang Jian, Niu Xin-xin, Yang Yi-xian, ZHOU Xi-zeng. Model and capacity of information hiding[J]. Application Research of Computers, 2005, (12): 116– 117. (in Chinese)

[4] 程义民, 钱振兴, 王以孝, 田源. 基于数位信息的信息隐藏方法[J]. 电子与信息学报, 2005, 27(8): 1304– 1309.
Chen Yi-min, Qian Zhen-xing, Wang Yi-xiao. Tian Yuan. A method of information hiding based on the digital-position information[J]. Journal of Electronic and Information, 2005, 27(8): 1304– 1309. (in Chinese)

[5] 黄晓生, 顾景文. CAD 图形数据数字水印技术综述[J]. 工程图学报, 2005(6): 140– 145.
Huang Xiao-sheng, Gu Jing-wen. Survey of watermarking techniques for CAD graphic data[J]. Journal of Engineering Graphics, 2005(6): 140– 145. (in Chinese)

[6] 汪亚顺, 徐铭政. 基于二维工程图的数字水印比例算法[J]. 南昌大学学报(工科版), 2003, 25(4): 29– 31.
WANG Ya-shun, XU Ming-zheng. Scale digital watermarking algorithm based on two—dimensional engineering graphics[J]. Journal of Nanchang University (Engineering & Technology), 2003, 25(4): 29– 31. (in Chinese)

[7] 汪亚顺, 刘良文, 徐铭政. 基于二维工程图的数字水印扩频算法[J]. 南昌大学学报(工科版), 2005, 27(4): 91– 94.
WANG Ya-shun, LIU Liang-wen, XU Ming-zheng. Spread spectrum digital watermarking algorithm based on two-dimensional engineering graphics[J]. Journal of Nanchang University (Engineering & Technology), 2005, 27(4): 91– 94. (in Chinese)

[8] 彭飞, 孙星明. 一种基于特征的二维工程图信息隐藏算法[J]. 计算机工程与应用, 2007, 43(15): 54– 55.
Peng Fei, Sun Xing-ming. Information hiding algorithm for two-dimensional engineering graphics based on characteristics[J]. Computer engineering and applications, 2007, 43(15): 54– 55. (in Chinese)

[9] Collet P, Eckmann J P. Iterated Maps on the Interval as Dynamical System[M]. Boston: Birkhauser, 1980.

[10] 王亥, 胡建栋. Logistic-Map 混沌扩频序列[J]. 电子学报, 1997, 25(1): 19– 23.
Wang Hai and Hu Jiandong. Logistic-map chaotic spread-spectrum sequence[J]. Acta Electronica Sinica, 1997, 25(1): 19– 23. (in Chinese)

[11] Autodesk 公司, AutoCAD 2006 帮助[CP]: 开发人员文档.

作者简介:

龙　敏　女, 1977 年 3 月出生于湖南省湘乡市, 现为长沙理工大学计算机与通信工程学院副教授, 主要研究方向为: 混沌保密通信、DSP. E-mail: longm@tom.com

彭　飞　男, 1977 年 11 月出生于湖南省洞口县, 现为湖南大学计算机与通信学院副教授, 中国计算机学会会员. 主要研究方向为: 数字水印、混沌密码. E-mail: eepengf@yahoo.com.cn