基于骑士巡游变换的数字图象细节隐藏技术

柏 森[1,2] 曹长修[2] 曹龙汉[1,2] 王 田[2] 汪纪锋[3]

[1](重庆通信学院,重庆 400035) [2](重庆大学自动化学院,重庆 400044) [3](重庆邮电学院,重庆 400065)

摘 要 为了研究一种不致引起他人破解欲望只置乱图象细节,而不破坏图象总体形象的数字图象隐藏技术,首先给出了骑士巡游问题及骑士巡游矩阵的概念,并提出了一种新的图象置乱变换——骑士巡游变换,同时分析了该变换方法隐藏图象细节的原理;然后,给出了图象细节隐藏的实验结果,实验结果表明,该方法不仅达到了隐藏图象细节而又不破坏图象总体形象的目的,而且使隐藏图象看上去像受到某种噪声干扰一样,从而不易引起别人破解的欲望,同时该变换还可以很好地将文字信息隐藏在图象之中;最后,对骑士巡游变换在图象伪装与隐藏方面的特性进行了分析,表明该变换具有较高的保密度和较强的免疫性.

关键词 图象变换 置乱变换 骑士巡游变换 图象隐藏 图象复原

中图法分类号: TP391 TP309.7 **文献标识码**: A **文章编号**: 1006-8961(2001)11-1096-05

Digital Image Details Hiding Technology Based on Knight-tour Transformation

BAI Sen[1,2], CAO Chang-xiu[2], CAO Long-han[1,2], WANG Tian[2], WANG Ji-feng[3]

[1](*Chongqing Communication Institute, Chongqing* 400035)

[2](*Automatization Institute, Chongqing University, Chongqing* 400044)

[3](*Chongqing University of Post and Telecommunications, Chongqing* 400065)

Abstract This paper is devoted to seek a new image hiding technology, which only scrambles the detail of images and keeps invariable in the mass, instead of arousing the desire to decrypt the image. Firstly, the concept of knight-tour problem and knight-tour matrix are introduced. A new scramble transformation is presented, which is called a knight-tour transformation(KTT). The principle that KTT can hide the details of images is analyzed. Secondly, several experimental results involving details hiding of images are given. Several edges detection experiments are also given to illustrate the usefulness of our method in hiding images' details. The experiments show that the image is approximately invariable in collectivity and it seems to be polluted by some noises. Therefore, the scrambled image does not easily stimulate other people's desire of trying to decrypt it. In addition, the transformation also can hide text information into image. By means of this the security of image and the information hiding into it are increased. This is propitious to transmit security of image details and confidential texts. Finally, it shows that the security is high and the immunity is strong by analyzing KTT 's characteristics on image hiding and disguising.

Keywords Image transformation, Scrambling transformation, Knight-tour transformation, Image hiding, Image restoration

0 引 言

随着国际互联网技术的日益普及,信息安全与保密越来越引起人们的重视,大家知道,在一切信息中,图象是一种非常直观,而又含有大量信息的载体,此所谓"千言万语不及一幅图".随着 ATM 技术的日趋完善,图象的传输将越来越广泛,图象的破坏

基金项目:重庆市科技计划应用基础研究项目(99-5918)

收稿日期:2000-04-18;**改回日期**:2000-12-19

及失密问题也越来越引起人们的重视，因为图象的安全与保密不仅与国家的政治、军事和外交有关，而且与团体、单位和个人密切相关，因此图象信息的安全传输，将是迫切需要解决的问题.

图象的隐藏与伪装技术是图象安全传输的手段之一，虽然此外还有很多的数据加密方法，但笔者认为，不会引起他人破解欲望的秘密才是最安全的秘密. 文献[1]中就提出了用分存与置乱变换两种方式来隐藏与伪装图象. 其中，分存虽然能够很好地隐藏图象，而又不易引起别人的注意，但是，它使得数据量发生了膨胀[2]. 文献[1]中提出的 Hilbert 曲线方式、E-曲线方式、Arnold 变换、幻方变换等几种置乱变换，虽能很好地隐藏图象和达到保密的目的，但是，它们容易引起别人破解的欲望，其中，幻方变换不仅只适用于方阵图象，而且还依赖幻方的构造，幻方构造得不好，将达不到图象隐藏的目的. 另外，文献[3]中提到的混沌(chaos)变换，也会使图象变得太无序，使人觉察出它是被隐藏过的；文献[4]提出的按签名函数进行置乱的算法，也存在一个签名函数的选取问题，若选得好，则置乱效果才好. 就笔者所知，目前还没有一种算法，能满足仅隐藏图象的细节，而不破坏图象总体的要求.

本文讨论的是能否提出一种新的置乱变换，它只置乱图象的细节秘密，而不破坏图象总的形象，从而不易引起他人的破解欲望，以达到隐藏图象真实细节的目的.

1　基于骑士巡游变换的图象细节隐藏技术

一幅图象可用一个矩阵 $\boldsymbol{A}=\{a(i,j)\}_{n\times m}$ 表示，其中，$a(i,j)$ 表示图象第 i 行 j 列象素的灰度值(或 R、G、B 分量值).

1.1　骑士巡游问题

所谓骑士巡游，就如同象棋一样，给出一块具有 n^2 个格子的 $n\times n$ 棋盘，一位骑士(knight，马)按国际象棋规则移动，放在初始坐标为 (x_0,y_0) 的格子里，骑士巡游问题(Knight-tour Problem)就是要求寻找一种方案使之过每个格子一次，且仅一次. 该问题可以较自然地推广到 $n\times m$ 棋盘.

一个 9×9 棋盘和 9×5 棋盘的骑士巡游路线如下面的矩阵 $\boldsymbol{T}_1$ 和 $\boldsymbol{T}_2$ 所示，称其为巡游矩阵，其中，1 表示骑士巡游的起点，$t(i,j)$ 的值表示骑士第 $t(i,j)$ 步巡游到 i 行 j 列.

$$\boldsymbol{T}_1=\begin{bmatrix}1&34&3&16&31&42&37&14&29\\4&17&32&43&36&15&30&41&38\\33&2&35&64&69&54&39&28&13\\18&5&68&73&44&65&46&53&40\\81&74&63&70&67&72&55&12&27\\6&19&80&75&62&45&66&47&52\\79&76&61&22&71&56&51&26&11\\20&7&78&59&50&9&21&57&48\\77&60&21&8&23&58&49&10&25\end{bmatrix}$$

$$\boldsymbol{T}_2=\begin{bmatrix}1&18&11&6&3\\10&5&2&19&12\\17&14&21&4&7\\22&9&16&13&20\\15&28&33&8&41\\32&23&42&27&34\\29&36&31&40&45\\24&43&38&35&26\\37&30&25&44&39\end{bmatrix}$$

1.2　骑士巡游变换

对于图象 $\boldsymbol{A}=\{a(i,j)\}_{n\times m}$，用巡游矩阵 $\boldsymbol{T}=\{t(i,j)\}_{n\times m}$ 作置乱变换，得到图象 $\boldsymbol{B}$. 其变换方法如下：

将 $\boldsymbol{A}$ 与 $\boldsymbol{T}$ 按行列作一一对应，将 $\boldsymbol{A}$ 中与 $\boldsymbol{T}$ 中位置 1 对应(下简称对应位置)的象素灰度值(或 R、G、B分量值)移到对应位置 2，将对应位置 2 的象素灰度值移到对应位置 3，……以此类推，最后将对应 $n\times m$ 位置的象素灰度值移到对应位置 1，就得到了按 $\boldsymbol{T}$ 置乱后的图象 $\boldsymbol{B}$. 如图 1 所示，一个“木”字通过骑士巡游置乱变换后，被隐藏了起来. 这种按骑士巡游路径进行置乱的变换，简称为骑士巡游变换.

(a) 原图象　　(b) 按骑士巡游路径 T_1 置乱后的图象

图 1　按骑士巡游变换的图象置乱

对于图象 $\boldsymbol{A}=\{a(i,j)\}_{n\times m}$ 和骑士巡游矩阵 $\boldsymbol{T}=\{t(i,j)\}_{n\times m}$，假设用 $\boldsymbol{T}$ 置乱 $\boldsymbol{A}$ 得到 $\boldsymbol{B}=\{b(i,j)\}_{n\times m}$，则其置乱算法可描述为：

```
for i=1 to n
    for j=1 to m
        Do
          if t(i,j)==1 then
```

(1) 从 T 中找到第 u 行第 v 列元素,使

$t(u,v)=n\times m$

(2) $b(i,j)=a(u,v)$

else

(1) 从 T 中找到第 u 行第 v 列元素,使

$t(u,v)=t(i,j)-1$

(2) $b(i,j)=a(u,v)$

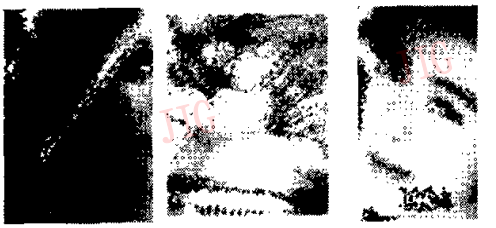
End;

1.3 骑士巡游变换隐藏图象细节的原理

一方面,由于骑士巡游的规则是:骑士(马)走斜日,即,按骑士巡游变换规则,图象的各象素的灰度值仅在相邻的 3 行 3 列间移动,且移动的方向不同,于是图象的细节将被改变,从而达到了隐藏细节的目的(如图 1);另一方面,解骑士巡游问题的算法,基本上是"试探-回溯"算法,即在确定试探的策略时,可以规定:将邻近区域的点巡游完之后,再巡游别的区域.这样不仅能使巡游的回溯次数最少[5],以加快求巡游矩阵的速度,而且还能使图象灰度值接近的区域,在变换后觉察不出其变化.由此可得如下的结论:按骑士巡游变换对图象作置乱,不仅可以隐藏图象细节,而且可以使图象总的形象保持不变,如图 2、图 3 所示.

(a) Lena 头发细节 (b) 树枝细节 (c) 小姐及文字细节

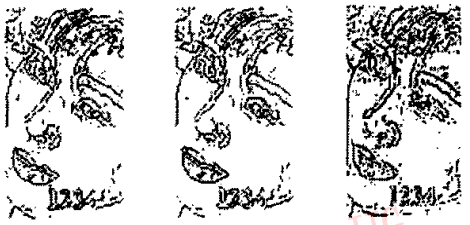
图 2 原图象



(a) 图 2(a)变换后 (b) 图 2(b)变换后 (c) 图 2(c)变换后

图 3 骑士巡游变换置乱后的结果图象

图 2(a)中的头发细节、图 2(b)中的树枝细节及图 2(c)中的"1234"文字信息及其细节,通过骑士巡游置乱变换后,在图 3 中已被隐藏.图 3 看起来不过是一些不太清晰,受到噪声干扰的图象.笔者认为,不引起别人破解欲望的加密方法,才是最安全的加密方法之一.而像幻方等置乱变换,则要么将图象变得太乱,根本看不出其原图象的任何痕迹,因而容易引起人们破解的欲望;要么基本上仅是将原图象向右上角或左下角作一平移(这依赖幻方的构成),但这样达不到隐藏的目的.从这个意义上讲,用骑士巡游变换来作图象的隐藏,其保密度是比较高的.原始图象(如图 2(c))经各种边缘检测能看出其中的信息,包括数字信息"1234"都清晰可辨(图 4),而经过骑士巡游置乱后的图象(图 3(c)),其各种边缘检测结果细节已模糊不清了,根本看不出数字信息"1234"(图 5).图 4 和图 5 中的 r 值表示边缘检测的阈值,即使将其取为更小的值,仍可得到相同的结论.



(a) Sobel ($r=0.025$) (b) Prewitt ($r=0.025$) (c) Roberts ($r=0.025$)

图 4 原图象(图 2(c))的各种边缘检测结果

(a) Sobel ($r=0.025$) (b) Prewitt ($r=0.025$) (c) Roberts ($r=0.025$)

图 5 骑士巡游变换置乱后图象(图 3(c))的各种边缘检测结果

2 骑士巡游变换的特性分析

上一节已经论述,骑士巡游变换不仅能很好地隐藏需要隐藏的信息(如图 2 (c)中的"1234"),而且能很好地隐藏图象的细节,从而将图象中的秘密伪装了起来.但作为图象隐藏的目的和技术要求,它必

须满足一定的特性，其中最重要的特性是隐藏性、隐藏场所的安全性、保密度和免疫性等. 由图 3 和图 5 可知，骑士巡游变换的细节隐藏性是显而易见的，由于它是将细节和需隐藏的信息隐藏在目标图象之中，而不是隐藏在文件头等处，因此其隐藏场所也是较安全的.

2.1　骑士巡游变换的保密度

增加密钥量是提高密码通信系统保密度的有效措施[6]，对于高为 n 象素，宽为 n 象素的图象，有如下的定理：

定理　对于骑士巡游问题，当 $n\geq 5$，且为偶数时，以任意点作为初始点都有解[7].

对于 n 不为偶数时，由于可以人为地加一或减一象素，因此，可以从 n^2 个象素点中任选一个作为巡游的起点，并且除了靠近边缘的两行、两列象素外，其余每点有 8 个方向可供选择，进行组合后即可作为骑士巡游试探方向的顺序. 此外，还可以通过对棋盘挖洞，来产生不同的骑士巡游路径[7]，比如，只要棋盘(图象)足够大，可以挖 1 个、2 个、3 个洞……，这相当于在对图象作置乱变换的时候，可以规定图象的某 1 个、2 个、3 个象素不变……. 此外，还可以通过指定骑士巡游的起点和终点来求得不同得巡游矩阵. 所以，用于骑士巡游置乱的密钥个数 k 满足下式

$$k>\left[C_{n\times n}-C_{n\times(n-2)}+C_{n(n-2)}^{1}\left(C_{n}^{1}+C_{n}^{2}+C_{n}^{3}+\cdots\right)+C_{n(n-2)}^{2}\left(C_{n}^{2}-C_{n}^{3}+C_{n}^{4}+\cdots+1\right)\right]\cdot 8!$$

这大于 Hilbert 曲线、Peano 方法、E-曲线、幻方置乱变换的密钥个数. 因为它可通过骑士巡游起点和终点的选取、巡游方向的变化以及挖洞的位置和数量的确定来构成不同的密钥，它既适合单密钥体制，也适合多密钥体制，所以，其保密度较高.

2.2　骑士巡游变换的免疫性

免疫性指的是在图象作隐藏变换的时候，其抗拒因图象文件的某种改动而导致隐藏信息丢失的能力. 所谓改动包括传输过程的信道噪声、过滤操作、重新采样、编码、有损压缩、模/数转换等.

用骑士巡游置乱变换，其抗噪声和抗过滤能力较强(如图 6 所示). 骑士巡游置乱变换后，再通过加入高斯白噪声(图 6(a))和二维自适应滤波(图 6(c))，然后用逆骑士巡游变换都能较好地复原图象(如图 6(b)和图 6(d)所示).

选用 Haar 小波 3 层分解，阈值为 7 的小波系数阈值化方法，对骑士巡游变换置乱后的图象(图 3(c))进行压缩，得到压缩率为 37.876 5 的压缩图象(图 6(e)). 压缩后用逆骑士巡游变换来得到复原图象(图 6(f)). 从图 6(f)可以看出，用骑士巡游变换作图象隐藏时，其抗压缩能力也较强.

(a) 置乱后加入高斯噪声　(c) 置乱加噪后滤波　(e) 置乱后小波压缩

(b) 图(a)的复原　(d) 滤波后复原　(f) 压缩后复原

(压缩率=37.876 5)

图 6　骑士巡游变换置乱后加噪声、滤波和压缩后恢复图象

3　结　语

骑士巡游变换具有如下优点：(1)适用于高和宽不同的图象，而幻方变换仅适用于高和宽相同的图象[1]；(2)置乱方法灵活，可通过编程来控制巡游的起点、终点以及巡游的方向，还可控制一些点不巡游(挖洞)，从而得到不同的置乱方法；(3)不仅能隐藏图象的细节，而且特别能隐藏图象中的文字信息，也可应用于其他计算机文件的加密. 该变换方法值得进一步研究的问题是：①置乱变换置乱程度的量化；②置乱程度与保密度的关系如何；③确定 n 界幻方所形成的不同类型幻方的数目，进而确定幻方变换的保密度；④对 $n\times m$ 棋盘，如何确定不同骑士巡游路径的数目，进而较精确地确定骑士巡游路径变换的保密度；⑤骑士巡游变换的神经网络复原问题；⑥如何在骑士巡游变换的同时，进行图象压缩编码等问题.

参 考 文 献

1　丁玮，齐东旭. 数字图象变换及信息隐藏与伪装技术[J]. 计算机

学报,1998,21(9):839~843.
2 苏中民,林行良. 图视秘密的任意分存[J]. 计算机学报,1996,19(3):293~299.
3 Grutchfield J P, Farmer J D, Packark N H *et al*. Chaos[J]. Scientific American, 1986,268(1):38~49.
4 卢朝阳,周幸妮. 种新的数据信息置乱算法[J]. 计算机工程与科学,1998,20(3):28~41.
5 柏森. 关于骑士巡游问题的研究[硕士论文]. 重庆:重庆大学系统工程及应用数学系,1998.
6 吴伯修,曹秀英. 密码学与语言保密通信[M]. 南京:东南大学出版社,1996,10~20.
7 柏森,杨晓帆,柏林. 骑士旅游问题一个猜想的证明[J]. 重庆大学学报(自然科学版),1998,21(5):85~89.

柏 森 1963年生,重庆通信学院一系图象处理教研室副教授,现为重庆大学自动化学院博士生.研究领域为图象处理、计算机图形学、神经网络等.已发表论文20余篇,专著2部.

曹长修 1937年生,重庆大学自动化学院自动控制研究所所长,教授,博士生导师.1959年毕业于上海交通大学自动控制系.主要研究方向为计算机网络及通信新技术、自动控制、图象处理中的新算法、智能网、数据挖掘等.已发表论文100余篇,完成科研项目30多项,著译3部.

曹龙汉 1966年生,重庆通信学院四系电力电子教研室主任,教授.现为重庆大学自动化学院博士生.研究领域为自动控制、数据挖掘、图象处理等.已发表论文20余篇,书3部,获省部级及军队科技进步奖4项.

王 田 1970年生,重庆商学院计算机系副主任,讲师。1992、1997年先后获重庆大学资环系工学学士、机械工程一系工学硕士学位,现为重庆大学自动化学院博士生.研究领域为图象处理、图象通信、智能网等.已发表论文15篇.

汪纪锋 1944年生,重庆邮电学院研究生部部长,教授,1967年毕业于重庆大学自动控制系.主要研究方向为智能控制理论在通信系统中的应用、智能网、ATM网络技术等.发表论文30余篇,专著1部.