CN 43-1258/TP
ISSN 1007-130X

计算机工程与科学
Computer Engineering & Science

第 35 卷第 5 期 2013 年 5 月
Vol. 35, No. 5, May. 2013

文章编号:1007-130X(2013)05-0136-06

基于广义骑士巡游的 RGB 图像加密压缩算法*

刘博文,柏　森,阳　溢,刘程浩

(1. 重庆通信学院,重庆 400035;2. 应急通信重庆市重点实验室,重庆 400035)

摘　要:从考虑涉密图像的安全性和传输效率的角度出发,引入广义骑士巡游置乱加密技术,提出了一种 RGB 图像加密压缩算法。算法将原始 RGB 图像颜色模式转换为 YCbCr,对 YCbCr 三层分别进行 8×8分块,对每个块进行 DCT 变换,构建以块为单位的三维棋盘,然后采用广义骑士巡游置乱规则对该三维棋盘加密,最后进行 JPEG 压缩得到加密压缩图像。仿真验证和实验分析表明,该算法对图像压缩性能影响小,在满足一定安全性的前提下,压缩效率得到提高。

关键词:RGB 图像加密;广义骑士巡游置乱;广义骑士巡游;分块

中图分类号:TP309.7　　**文献标志码**:A

doi:10.3969/j.issn.1007-130X.2013.05.022

An algorithm of RGB image encryption and compression based on generalized Knight's tour

LIU Bo-wen, BAI Sen, YANG Yi, LIU Cheng-hao

(1. Chongqing Communication Institute, Chongqing 400035;
2. Chongqing Key Laboratory of Emergency Communication, Chongqing 400035, China)

Abstract: An algorithm of RGB image encryption and compression based on the technique of generalized knight's tour scrambling encryption is proposed by considering from the view of ensuring the confidential image security and transmission efficiency. In this algorithm the YCbCr layers of original image are divided into 8×8 blocks respectively after image pattern turned from RGB to YCbCr, then every block is transformed by DCT to build 3-dimensional chessboard, And the 3-dimensional chessboard is encrypted by the principle of generalized knight's tour, Finally the encrypted and compressed image could be gained by JPEG compression. Experimental results and analysis show that the algorithm is low impact on image compression capability, it gets higher compression efficiency in content of some degree of safety.

Key words: RGB image encryption; generalized knight's tour scrambling; generalized knight's tour; blocking

1　引言

随着计算机网络技术和多媒体技术的飞速发展,数字图像、视频等多媒体在人们日常生活中的应用越来越多,并成为人们传递信息的主要工具。由于这些传输信息的媒体需要在开放的网络环境中传输和分享,人们对数据量的大小、安全性等方面提出了更高要求。目前,对数据进行加密处理是保证多媒体信息安全传输的主要方法之一。传统的数据加密经过复杂性较高的基于数论的运算操作,不能满足多媒体信息巨大的数据量及实时性的需求。在图像加密算法中,主要包括与压缩独立的加密算法[1~3]和结合压缩技术的加密算法[4~6]。

* 收稿日期:2012-03-07;修回日期:2012-08-21
基金项目:国家自然科学基金资助项目(61272043);重庆市基础与前沿研究计划资助项目(cstc2013jjB40009)
通讯地址:400035 重庆市沙坪坝区林园甲一号重庆通信学院图像实验室
Address: Chongqing Communication Institute, No A01, Linyuan, Shapingba District, Chongqing 400035, P. R. China

文献[4]较早在 DCT 变换域中实现了图像加密压缩,但加密后的系数不在原始系数的取值区间,且不能表示成 2 的幂次方的形式,无法简单地用诸如异或运算等方式实现加密。文献[5]解决了加密后的系数回到原始系数区间的问题,但效率较低,加密运算需要迭代次数过多,并且使用一维混沌序列加密后图像的安全性不高。文献[6]中提到的 CWF 算法在小波域中进行加密压缩,但其破坏了小波变换的多尺度分解树型结构,势必影响图像的可压缩性。加密和压缩两种技术的有效结合将兼顾数据的安全性及传输效率,因此成为当前国内外研究的热点。

针对多媒体信息数据量大和实时性需求的特点,提出一种基于广义骑士巡游的 RGB 图像加密压缩算法。将原始图像分块处理,以 8×8 的块作为最小单位在变换域中进行置乱,将加密和压缩有效地结合起来,使处理速度更快。在满足一定安全性的前提下,压缩效率得到提高。

2 广义骑士巡游及加密原理

18 世纪 50 年代末,著名数学家 Euler 首次提出了骑士巡游问题 KTP(Knight's Tour Problem)。骑士巡游问题,起源于国际象棋,就是骑士(马)从棋盘上的某个初始棋格开始,以跳"斜日"的方式跳遍棋盘上的每个棋格一次且仅一次的一种方案[7],如图 1 所示。

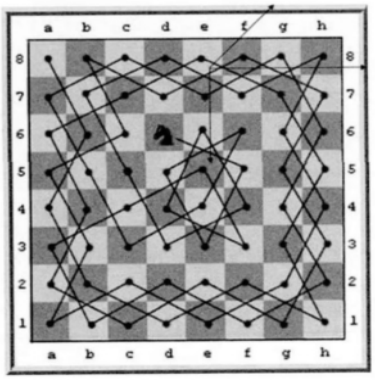

Figure 1 Schematic diagram of knight's tour

图 1 骑士巡游示意图

所谓广义骑士巡游,有两层含义:(1)棋盘是广义的,即棋盘是 m 维空间上任意形状的棋盘;(2)骑士是广义的,即骑士不再局限于"马跳斜日",而是满足一定条件[8]下的任意跳法。三维棋盘示意图如图 2 所示。

骑士的巡游只由少数几个参数(骑士巡游起始位置、巡游规则等)控制。在三维棋盘上建立坐标系,将第一层棋盘左上角视为原点,棋盘上的每一格视为对应坐标系上一个点,则骑士巡游起始位置 $k_1(x,y,z)$ 表示骑士从第 z 层棋盘上第 x 行、第 y 列的棋格上开始移动。巡游规则 $k_2[i,j,k]$ 表示骑士每次移动的方法,即从起始位置的棋格在空间三个方向上分别跳 i、j、k 个棋格,简称为[i, j, k]马。骑士巡游的巡游路径用骑士巡游矩阵 $\boldsymbol{T}$ 来表示,例如一个 8×8×3 棋盘上[1,2,2]马的广义骑士巡游矩阵如图 3 所示。其中,1 表示骑士巡游的起点,192 表示巡游的终点。基于骑士巡游的置乱加密基本原理就是将棋盘中位置 1 的元素移动到位置 2,位置 2 的元素移动到位置 3,以此类推,最后将位置 192 的元素移到位置 1 上。

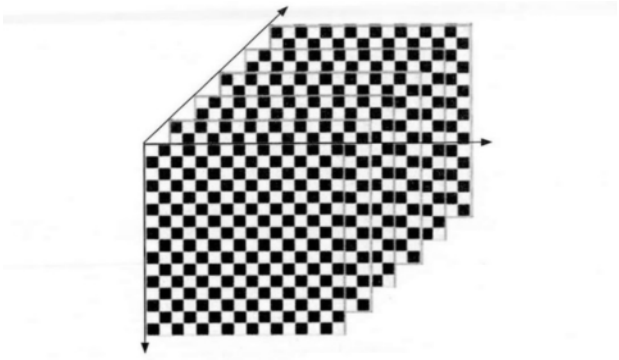

Figure 2 Schematic diagram of 3D-chessboard

图 2 三维棋盘示意图

$$\boldsymbol{T}(:,:,1)=\begin{bmatrix}186&97&44&149&50&89&20&143\\39&152&183&92&137&146&53&86\\94&189&174&47&180&17&140&23\\155&42&125&134&77&64&83&56\\128&99&74&177&2&119&28&169\\71&158&131&122&37&80&61&116\\102&5&164&69&110&11&172&31\\161&66&105&8&167&34&113&14\end{bmatrix}$$

$$\boldsymbol{T}(:,:,2)=\begin{bmatrix}175&48&95&188&139&22&181&18\\126&133&154&41&84&55&78&63\\45&148&191&98&25&142&51&90\\184&123&38&151&58&87&136&145\\163&68&107&10&173&30&109&16\\104&7&160&65&112&13&166&33\\75&178&3&100&27&170&1&118\\130&121&72&157&60&115&36&81\end{bmatrix}$$

$$\boldsymbol{T}(:,:,3)=\begin{bmatrix}190&93&46&147&52&91&24&141\\43&150&185&124&135&144&57&88\\96&187&176&49&182&19&138&21\\153&40&127&132&79&62&85&54\\4&101&76&179&192&117&26&171\\73&156&129&120&35&82&59&114\\106&9&162&67&108&15&168&29\\159&70&103&6&165&32&111&12\end{bmatrix}$$

Figure 3 Matrix representation of generalized knight's tour path

图 3 [1,2,2]马广义骑士巡游矩阵

3 基于广义骑士巡游的RGB图像加密压缩算法

3.1 算法思想

在采用JPEG算法压缩图像的过程中,DCT变换以8×8的块作为最小单元。为减少加密对压缩的影响,考虑以块为单位进行置乱加密。本文提出的算法将原始图像的Y、Cb、Cr三层分别进行8×8分块操作,对块化后的每一块进行DCT变换得到一个系数块化矩阵。将这个系数块化矩阵中的每一块视为棋盘上的棋格,按照骑士巡游规则对每块进行移动,以实现图像的加密。对加密后的数据进行JPEG压缩编码后,就得到加密压缩图像。这样,采用本文算法不仅使得每一小块内依然具有原有的相关性,还可以保持较高的可压缩性。

本文提出的加密压缩流程如图4所示。

3.2 算法步骤

设原始图像为 $\boldsymbol{I}_{m\times n\times 3}$,加密后图像为 $\boldsymbol{I}'_{m\times n\times 3}$,加密压缩后图像为 $\boldsymbol{I}''_{m\times n\times 3}$。本文加密压缩算法过程如下:

(1) 读取原始彩色图像 $\boldsymbol{I}_{m\times n\times 3}$,在YCbCr模式下,分别对其Y、Cb、Cr三层进行8×8分块,将图像每层分成 $k\times l$ 个小块,然后对每一块进行DCT变换得到系数块化矩阵 $\boldsymbol{C}_{k\times l\times 3}$,其中,$\lfloor m/8 \rfloor$,$l=\lfloor n/8 \rfloor$($\lfloor\rfloor$表示下取整)。

(2)根据第2节的介绍,选择起始位置 $k_1(x,y,z)$、巡游规则 $k_2[i,j,k]$作为初始密钥,使用文献[9]中的算法得到骑士巡游矩阵 $\boldsymbol{T}_{k\times l\times 3}$。

(3)将 $\boldsymbol{C}_{k\times l\times 3}$ 中每个块看成 $\boldsymbol{T}_{k\times l\times 3}$ 上的一格,使 $\boldsymbol{C}_{k\times l\times 3}$ 与 $\boldsymbol{T}_{k\times l\times 3}$ 中元素一一对应。根据骑士巡游置乱原理进行骑士巡游块置乱加密,得到加密后的系数块化矩阵 $\boldsymbol{C}'_{k\times l\times 3}$。

(4)对 $\boldsymbol{C}'_{k\times l\times 3}$ 进行DCT逆变换,将逆变换后的数据块化还原,得到加密后图像 $\boldsymbol{I}'_{m\times n\times 3}$。

(5)令 $\boldsymbol{I}_{m\times n\times 3}=\boldsymbol{I}'_{m\times n\times 3}$,重复步骤(1)~步骤(5),直至得到满意的加密效果为止。最后将 $\boldsymbol{I}'_{m\times n\times 3}$ 进行JPEG压缩,得到最终加密压缩图像 $\boldsymbol{I}''_{m\times n\times 3}$。

解密是上述过程的逆过程。

4 实验与分析

为验证本文算法的有效性,本节以大小为256×256的Lena和Baboon两幅测试图像为例,采用MATLAB进行仿真实验。实验中起始位置都选取 $k_1(1,1,1)$,初始密钥由巡游规则 k_2 决定。

4.1 直观效果

采用[1,6,2]马作为初始密钥分别对测试图像进行1次、2次、5次加密实验,其加密压缩效果分别如图5和图6所示。

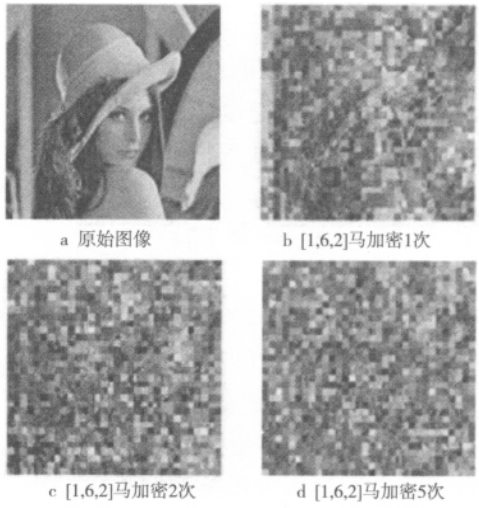

Figure 5 Encryption and compression results of Lena

图5 Lena图像加密压缩效果图

通过效果图可以看出,以[1,6,2]马作为密钥,1次加密后的图像效果并不十分理想,可以看出一些原始图像轮廓,进行2次加密后就能得到较好的加密效果,且不同加密次数下加密效果接近。从直观效果来看,基于广义骑士巡游的图像加密压缩方案在加密效果上较理想。

4.2 置乱度

置乱度用来评估图像被置乱或加密程度,即图像加密的直观效果好坏的重要指标,它能较为客观地反映图像的加密效果。目前,许多相关研究都给

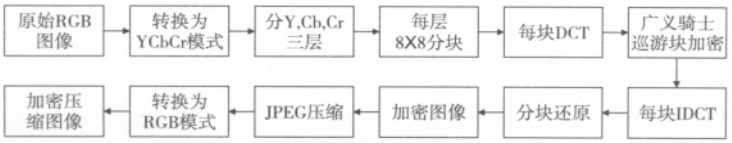

Figure 4 Flowchart of encryption and compression

图4 加密压缩流程图

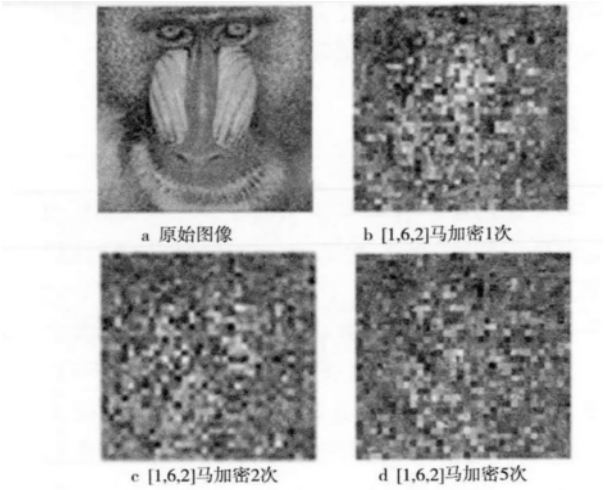

Figure 6 Encryption and compression results of Baboon

图 6 Baboon 图像加密压缩效果图

出了置乱度的定义,但又各不相同。本文引用文献[10]定义的置乱度作为评价标准,其计算式为:

$$S_r(I,\tilde{I}) = \frac{\sum_{i=1}^{M}\sum_{j=1}^{M}(I_{ij}-\tilde{I}_{ij})^2}{\sum_{i=1}^{M}\sum_{j=1}^{M}(I_{ij}-R_{ij})^2} \quad (1)$$

其中,I_{ij} 表示原始图像(i,j)位置的值,$\tilde{I}_{ij}$ 表示置乱或加密图像(i,j)位置的值,R_{ij} 表示与原始图像大小相同的均匀分布噪声图像(i,j)位置的值。为了使加密图像的置乱度具有可比性,通常采用同一幅均匀分布的噪声图像进行比较。采用 Lena 图像作为测试图像,分别用[1,2,2]马、[1,4,2]马、[1,6,2]马作为密钥,对加密一次后的加密图像的 RGB 三层进行置乱度计算,得到的实验结果如表 1 所示。

Table 1 Scrambling measure of image encryption

图 1 加密图像的置乱度

本文算法加密方式	Lena 图像		
	R	G	B
[1,2,2]马加密	0.9302	0.7606	0.8103
[1,4,2]马加密	0.9893	0.7850	0.8919
[1,6,2]马加密	1.0243	0.8637	0.9257

从表 1 可以清楚地看出,采用[1,6,2]马加密后图像在 RGB 三层上的置乱度都高于[1,2,2]马和[1,4,2]马的置乱度,其主要原因在于[1,6,2]马的移动距离大于后两者,使得相关性破坏更严重,加密效果更好。

随着加密次数的增加,加密算法的置乱度也将随之变化,采用[1,6,2]马进行多次加密测试,其置乱次数与置乱度关系如图 7 所示。

图 7 中,随着加密次数的增加,前 3 次的置乱度出现较大振荡,但经过 5 次加密后,其置乱度维持在 0.67～0.91,可视为稳定。采用基于广义骑士巡游的图像加密压缩算法,只需较少置乱次数就能达到置乱的效果,算法的效率高、处理速度快。

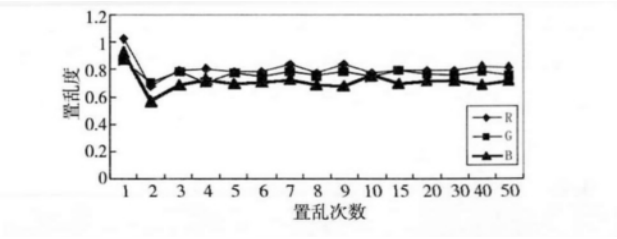

Figure 7 Relationship between times of scrambling and scrambling measure

图 7 [1,6,2]马置乱次数与置乱度关系图

4.3 压缩率

压缩率作为图像压缩的一个评价指标,其计算式如式(2)所示:

$$\text{压缩率} = \frac{\text{原始图象大小}-\text{压缩后图象大小}}{\text{原始图象大小}} \times 100\% \quad (2)$$

在压缩率测试中,对 Lena 图像算法分别选择[1,2,2]马、[1,4,2]马 、[1,6,2]马作为密钥,经过 1 次加密后得到压缩率如表 2 所示。

Table 2 Efficiency of compression

图 2 压缩效率

加密方式	原始图像大小/kbyte	加密压缩后图像大小/kbyte	压缩率/%
直接压缩	192	12.4	93.541
本文算法采用[1,2,2]马	192	15.7	91.822
本文算法采用[1,4,2]马	192	16.1	91.614
本文算法采用[1,6,2]马	192	16	91.666

随着加密次数的增加,其压缩率也将随之降低。采用[1,6,2]马作为密钥,进行多次加密后图像的压缩率如表 3 所示。

Table 3 Relationship of encryption times and compression

图 3 加密次数与压缩率

加密次数 t	加密压缩后图像大小/kbyte	压缩率/%
1	16	91.666
2	16.7	91.302
3	16.7	91.302
5	16.9	91.197
10	17.0	91.145
20	17.1	91.093

由表 2 和表 3 可以看出,采用基于广义骑士巡游的 RGB 图像加密压缩算法得到的压缩率较高,

接近对原始图像直接压缩的压缩率,并且随着加密次数的增加,压缩率缓慢下降。由于高压缩率可以满足现实生活中多媒体技术的需求,本文的算法具有很好的实用性。

4.4 密钥敏感性测试

图像加密要求具有较高的密钥敏感性,即密钥之间发生微小变化时,加密算法得到的效果是敏感的,这样就能保证密码系统针对穷举攻击、统计攻击的安全性。本文采用[1,6,2]马和[1,4,2]马进行1次加密测试,其加密效果如图8所示。

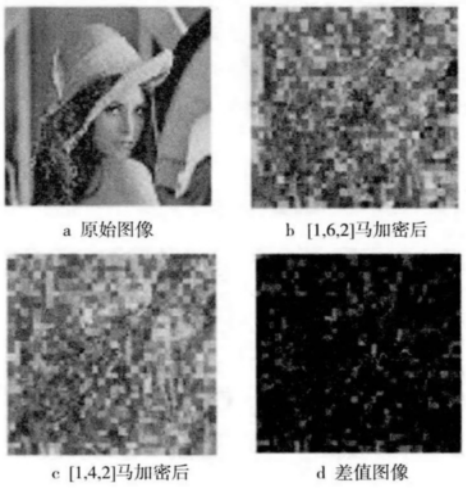

Figure 8 Experiment results of secret key's sensitivity

图8 密钥敏感性测试

通过图8可以看出,密钥中坐标上移动2个单位的变换时,将导致加密图像大部分发生改变,即产生了雪崩效应。因此,本文的加密压缩算法对骑士巡游棋盘密钥具有很高的敏感性,可以抵抗常见密码攻击和差分攻击。

4.5 实时性分析

为检测算法的时效性,本文采用50幅256×256图像样本分别作测试,密钥选取[1,6,2]马,取运算时间的平均值作为本算法的有效运算时间,压缩采用MATLAB中imwrite函数实现,然后计算出平均压缩率。实验结果如表4所示。

Table 4 Relationship of times and compression

图4 运算时间与压缩率

本文算法	有效运算时间/s	压缩率/%
直接压缩	0.0089	93.61
加密1次	1.6934	91.99
加密5次	8.3565	91.43

通过表4可以看出,基于广义骑士巡游的图像加密压缩算法的运算时间较短,并且压缩率较高。快速的运算时间可以满足多媒体技术的需求,使得网络上的信息传输效率更高。

5 结束语

本文提出了一种基于广义骑士巡游的RGB图像加密压缩算法,经实验证实,在保证传输信息较高安全性的前提下,获得了较高的压缩率。该算法可作为一种图像的加密方法,将加密压缩后的涉密图像进行传输,较大程度提高了传输效率;也可作为进一步信息隐藏的预处理过程。基于广义骑士巡游的图像加密压缩方法在多媒体信息化时代具有较强的实用性,更能够满足现实生活中信息安全的各种应用场合的需要。由于块加密的局限性,本文算法只有对分辨率在256×256以上的图像加密才能得到较好效果。如何解决还原图像块效应和在JPEG2000压缩标准下的加密压缩算法是下一步研究的重点。

参考文献:

[1] Rhouma R, Meherzi S, Belghith S. OCML-based colour image encryption[J]. Chaos ,Solitons & Fractals, 2009, 40(1):309-318.

[2] Huang C K, Nien H H. Multi chaotic systems based pixel shuffle for image encryption[J]. Optics Communications, 2009,282(11):2123-2127.

[3] Tian Yan, Xie Yu-bo, Li Tao, et al. An image scrambling method based on image blocking and chaos system[J]. Journal of Image and Graphics,2007,12(1):56-60.(in Chinese)

[4] Sun Xin, Yi Kai-xiang, Sun You-xian. New image encryption algorithm based on chaos system[J]. Journal of Computer-Aided Design&Computer Graphics, 2002, 14(2):136-139.(in Chinese)

[5] Peng Cheng, Liu Lin. Encryption algorithm for compressed images based on chaotic sequences[J]. Computer Engineering,2008, 34(20):177-179.(in Chinese)

[6] Ping Liang, Sun Jun, Zhou Jun. An algorithm for image encryption based on JPEG2000[J]. Applieation&Project of Video Technologies, 2006, 7(1):87-90.(in Chinese)

[7] Parberry I. An efficient algorithm for the knight's tour problem [J]. Discrete Applied Mathematics, 1997, 73(3):251-260.

[8] Tao Ke. The problem about ND-knight move[J]. Mathematics in Practice and Theory, 1982(1):26-31.(in Chinese)

[9] Sen Bai, Liao Xiao-feng, Qu Xiao-hong, et al. Generalized knight's tour problem and its solutions algorithm[C]// Proc of the 2006 International Conference on Computational Intel-

ligence and Security, 2006:570-573. (in Chinese)

[10] Chen G, Zhao X Y, Li J L. A self-adaptive algorithm on image encryption[J]. Journal of Software, 2005, 16(11): 1975-1982. (in Chinese)

附中文参考文献:

[3] 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.

[4] 孙鑫, 易开祥, 孙优贤. 基于混沌系统的图像加密算法[J]. 计算机辅助设计与图形学学报, 2002, 14(2):136-139.

[5] 彭成, 柳林. 基于混沌序列的压缩图像加密算法[J]. 计算机工程,2008, 34(20):177-179.

[6] 平亮, 孙军, 周军. 一种基于JEPG2000标准的数字图像加密算法[J]. 视频技术应用与工程, 2006, 7(1):87-90.

[8] 陶克. 关于n维马步问题[J]. 数学的实践与认识, 1982(1): 26-31.

[9] 柏森,廖晓峰,曲晓红,等. 广义骑士巡游问题与它的解决算法[C]// 2006年国际计算智能与信息会议论文集, 2006: 570-573.

[10] 陈刚,赵晓宇,李均利. 一种自适应的图像加密算法[J]. 软件学报,2005,16(11):1975-1982.

作者简介:

刘博文(1983-),男,河北保定人,硕士,讲师,研究方向为图像加密和信息安全。**E-mail**:alven0201@163.com

LIU Bo-wen, born in 1983, MS, lecturer, his research interests include image encryption, and information security.

柏森(1965-),男,四川达县人,博士,教授,研究方向为信息隐藏和信息安全。

BAI Sen, born in 1965, PhD, professor, his research interests include steganography, and information security.

阳溢(1987-),男,重庆人,硕士生,研究方向为图像加密和信息隐藏。

YANG Yi, born in 1987, MS candidate, his research interest include image encryption, and steganography.