

Journal of Image  
and Graphics

# 中国图象图形学报



ISSN1006-8961  
CN11-3758/TB

2012 **10**  
Vol.17 No.

中国科学院遥感应用研究所  
中国图象图形学学会主办  
北京应用物理与计算数学研究所

# 中国图象图形学报

Zhongguo Tuxiang Tuxing Xuebao

2012年10月 第17卷 第10期(总第198期)

## 目次

### 综述

张量值图像插值方法综述 ..... 邵宇, 刘莹, 孙富春(1197)

### 图像处理和编码

利用模运算及其周期性特点的安全隐写算法 ..... 廖琪男(1206)

结合快速融合与颜色传递的双波段夜视图像染色 ..... 李郁峰, 冯晓云, 徐铭蔚, 黄文丽(1213)

Weber 定律下尺度空间的自适应构建 ..... 刘立, 张瑞军, 万亚平, 黄欣阳, 彭复员(1222)

改进权值函数的非局部均值去噪算法 ..... 单建华(1227)

### 图像分析和识别

非相似度保持投影 ..... 陈才扣, 侯钰(1232)

非正交二值子空间模板表示的并行生成 ..... 杨培, 武港山, 杨扬, 任桐炜(1237)

Adaboost 和随机图划分的无监督图像分类 ..... 李巍, 杨素锦, 段晓华(1245)

aiNet 背景抑制的单帧红外弱小目标检测 ..... 陈炳文, 王文伟, 秦前清(1252)

韦伯-中心环绕结构的图像显著性检测模型 ..... 林丽莉, 周文晖(1261)

气象传真图信息提取 ..... 李存东, 肖传毅, 潘海朗, 陈日清, 杨劲松(1268)

### 图像理解和计算机视觉

多要素空间场景相似性匹配模型及应用 ..... 宋腾义, 汪闽(1274)

### 计算机图形学

Delaunay 三角网通用合并算子及分治算法的简化 ..... 刘永和, 冯锦明, 郭维栋, 田根, 金毅(1283)

基于 Laplace 谱嵌入和 Mean Shift 的三角网格一致性分割 ..... 马亚奇, 李忠科, 赵静(1292)  
断裂面匹配的破碎刚体复原 ..... 李群辉, 周明全, 耿国华(1298)

### 虚拟现实与增强现实

核爆炸外观景象实时模拟 ..... 郑涛, 徐晓刚, 邵承永(1305)

### 医学图像处理

全局脑白质纤维群智能跟踪算法 ..... 冯远静, 王哲进, 张贵军, 俞立(1312)

### 遥感图像处理

对偶四元数线阵遥感影像几何定位 ..... 盛庆红, 姬亭, 刘微微, 王惠南(1319)

修正安装矩阵提高 FY-3B/MERSI 的地理定位精度 ..... 吴荣华, 杨忠东, 关敏, 李翔翔(1327)

## 中国图象图形学报

刊名题字: 宋 健

月刊(1996 年创刊)

第 17 卷 第 10 期

2012 年 10 月 16 日出版

主管单位 中国科学院

主 办 中国科学院遥感应用研究所  
中国图象图形学学会  
北京应用物理与计算数学研究所

主 编 李小文

编辑出版 《中国图象图形学报》编辑出版委员会

北京 9718 信箱 邮编 100101  
电子信箱:jig@irsa.ac.cn  
电话:010-64807995 010-82614429  
网 址:www.cjig.cn

印刷装订 北京北林印刷厂

广告经营许可证 京朝工商广字第 0346 号

总 发 行 北京报刊发行局

订 购 全国各地邮局

国外发行 中国国际图书贸易总公司  
(中国国际书店)  
(北京 399 信箱 邮编 100044)

Superintended by Chinese Academy of Sciences

Sponsored by Institute of Remote Sensing Application,  
CAS China Society of Image and Graphics  
Institute of Applied Physics and Computational  
Mathematics

Chief editor LI Xiaowen

Editor, Publisher Editorial and Publishing Board  
of Journal of Image and Graphics  
(P. O. Box 9718, Beijing 100101, China)  
E-mail:jig@irsa.ac.cn

Distributed by Beijing Bureau for Distribution of Newspapers  
and Journals

Domestic All Local Post Offices in China

Foreign China International Book Trading Corporation  
(P. O. Box 399, Beijing 100044, China)

Printed by Beijing Beilin Printing House

ISSN 1006-8961 CN11-3758/TB CODE ZTTFXZ 国内邮发代号: 82-831 国外发行代号: M1406 国内定价: 45.00 元

# Journal of Image and Graphics

(Monthly, Started in 1996)

Vol. 17 No. 10 October 2012

## Contents

### Review

Overview of tensor valued images interpolation technology ..... Shao Yu, Liu Ying, Sun Fuchun (1197)

### Image Processing and Coding

Secure steganography based on modulo and its cyclical characteristic ..... Liao Qinan (1206)

Night vision dual-band images coloration using fast fusion and color transfer  
..... Li Yufeng, Feng Xiaoyun, Xu Mingwei, Huang Wenli (1213)

Adaptive algorithm of scale-space construction method based on Weber's law  
..... Liu Li, Zhang Ruijun, Wan Yaping, Huang Xinyang, Peng Fuyuan (1222)

Non-local means denoising algorithm with enhanced weight function ..... Shan Jianhua (1227)

### Image Analysis and Recognition

Dissimilarity preserving projection ..... Chen Caikou, Hou Yu (1232)

Parallel algorithm for generating template representation based on non-orthogonal binary subspace  
..... Yang Pei, Wu Gangshan, Yang Yang, Ren Tongwei (1237)

Unsupervised image categorization based on Adaboost and stochastic graph partition ..... Li Wei, Yang Sujin, Duan Xiaohua (1245)

Infrared dim target detection in single image based on background suppression by aiNet  
..... Chen Bingwen, Wang Wenwei, Qin Qianqing (1252)

Image saliency detection model with Weber's law based on center-surround structure ..... Lin Lili, Zhou Wenhui (1261)

Information extraction from meteorological facsimile maps  
..... Li Cundong, Xiao Chuanyi, Pan Hailang, Chen Riqing, Yang Jinsong (1268)

### Image Understanding and Computer Vision

Multi-feature based spatial scene matching model and its application ..... Song Tengyi, Wang Min (1274)

### Computer Graphics

Merging planar Delaunay triangulations based on universal operators and the implementation of a divide-conquer algorithm  
..... Liu Yonghe, Feng Jinming, Guo Weidong, Tian Gen, Jin Yi (1283)

Consistence segmentation of triangle mesh using Laplace spectral embedding and Mean Shift  
..... Ma Yaqi, Li Zhongke, Zhao Jing (1292)

Reassembly of broken 3D solids based on fractured surfaces matching ..... Li Qunhui, Zhou Mingquan, Geng Guohua (1298)

### Virtual Reality and Augmented Reality

Real-time simulation of nuclear explosion scene ..... Zheng Tao, Xu Xiaogang, Shao Chengyong (1305)

### Medical Image Processing

Global white matter tractography using swarm optimization ..... Feng Yuanjing, Wang Zhejin, Zhang Guijun, Yu Li (1312)

### Remote Sensing Image Processing

Geo-positioning line-array CCD images with dual quaternion ..... Sheng Qinghong, Ji Ting, Liu Weiwei, Wang Huinan (1319)

Improved FY-3B/MERSI geolocation accuracy using installation matrix  
..... Wu Ronghua, Yang Zhongdong, Guan Min, Li Xiangxiang (1327)

中图法分类号: TP391 文献标识码: A 文章编号: 1006-8961(2012)10-1206-07

论文引用格式: 廖琪男. 利用模运算及其周期性特点的安全隐写算法[J]. 中国图象图形学报, 2012, 17(10): 1206-1212.

# 利用模运算及其周期性特点的安全隐写算法

廖琪男

广西财经学院计算机与信息管理学系, 南宁 530003

**摘要:** 为了提供较大的可调信息嵌入量和保持载密图像良好的视觉质量, 提出一种基于模运算及其周期性特点的安全隐写算法。首先将秘密信息流转为  $n$  进制信息流表示, 然后根据余数循环的特点, 应用具有安全特性的模函数将一位  $n$  进制信息嵌入载体图像的一个像素中, 直至信息嵌入完毕。选择不同的参数  $n$  可以得到不同的嵌入率和载密图像视觉质量。理论分析和实验结果表明, 本文算法在保持高嵌入率的同时仍保持较好的载密图像视觉质量, 且安全性好; 其信息嵌入率选择具有高度弹性, 可以根据实际要求选择在嵌入率和载密图像质量都很理想的隐写方案。与同类算法相比具有更强的实用性。

**关键词:** 数字图像; 模函数; 余数循环; 隐写

## Secure steganography based on modulo and its cyclical characteristic

Liao Qinan

Department of Computer & Information Management, Guangxi University of Finance & Economics, Nanning 530003, China

**Abstract:** In order to provide a large, scalable embedding capacity and maintain a good visual quality of the stego-image, in this paper, a secure steganography based on modulo and its cyclical characteristic is presented. First, the secret data stream is converted into an  $n$ -ary notational system data stream. Then, according to the characteristic of the remainder cycle, one  $n$ -ary notational information will be embedded into one pixel of the cover image by a modulus function with security features, until the secret data is embedded completely. Different parameter  $n$  gets different rates of embedding and visual quality of the stego-image. Theoretical analysis and experimental results show that the algorithm can maintain a high embedding rate while maintaining good visual quality of stego-image, and good security. The information-embedding rate is highly flexible, and the method can choose the steganographic scheme according to the actual requirements, for which the embedding rate and stego-image quality are ideal. It is more practical than other similar algorithms.

**Key words:** digital image; modulus function; remainder cycle; steganography

## 0 引言

随着 Internet 和多媒体技术的迅速发展和广泛应用, 信息隐藏技术成为信息安全领域的一门新兴学科。其中基于数字图像的隐秘技术是信息隐藏技术研究的热点课题。

在空间域中, 最简单而又著名的方法就是最低

有效位(LSB)取代算法和基于 LSB 的密写算法<sup>[1-2]</sup>, LSB 算法会使直方图呈现值对或类似值对的异常现象, 容易被直方图检测分析和 RS 监测分析等隐写分析<sup>[3]</sup>。2006 年 Zhang 与 Wang 两人提出 EMD (exploiting modification direction) 信息隐藏方法<sup>[4]</sup>, 该方法是利用模数运算的余数循环的周期性特点进行信息隐藏, 由于其具有良好的图像视觉质量与信息嵌入量, 故有许多研究者都根据模数运算的这种

收稿日期: 2011-12-01; 修回日期: 2012-03-28

基金项目: 广西教育厅科研项目(201106LX474)

第一作者简介: 廖琪男(1964—), 男, 教授, 主要研究方向为数字图像处理、数字图像加密、信息隐藏。E-mail: lqner@163.com

特性提出改进式模数运算信息隐藏算法<sup>[5-8]</sup>,这些算法在嵌入率和效率等方面的性能都有了不同程度的提高。但仍存在着嵌入率低、安全性差等欠缺或不足。

本文在研究现有基于 EMD 算法基础上,提出在不可感知性、嵌入量最大化和算法安全性等方面都有非凡表现的数字图像隐写算法。

## 1 相关算法

### 1.1 EMD 算法

EMD 算法<sup>[4]</sup>可以将一位  $(2n + 1)$  进制的秘密信息嵌入到  $n$  个载体像素中,最大嵌入率为 1.16 bit/pixel,嵌入过程如下:

- 1) 将秘密信息转化为二进制数据流  $D$ ;
- 2) 顺序取  $D$  中的  $L$  位数字,并将其转化为  $K$  位  $(2n + 1)$  进制的数字序列。 $L, K$  的取值计算公式为

$$L = \lfloor K \log_2(2n + 1) \rfloor \quad (1)$$

- 3) 从原始图像中取  $n$  个未嵌入秘密信息的像素的像素灰度值  $g_i$  作为一组  $(g_1, g_2, \dots, g_n)$ , 并计算嵌入与提取函数

$$f(g_1, g_2, \dots, g_n) = \left[ \sum_{i=1}^n (g_i \times i) \right] \bmod (2n + 1) \quad (2)$$

- 4) 计算一位  $(2n + 1)$  进制信息  $d$  与  $f$  之模距

$$s = (d - f) \bmod (2n + 1) \quad (3)$$

若  $s = 0$ , 则不改变任何像素值; 如果  $s \neq 0$ , 且  $s \leq n$ , 则将  $g_s$  的值加 1, 否则将  $g_{2n+1-s}$  的值减 1, 这样便实现秘密信息  $d$  的嵌入。

反复执行步骤 3)4), 直至信息嵌入完毕。

该算法嵌入率为

$$P = \log_2(2n + 1)/n \quad (4)$$

### 1.2 基于模运算的 EMD 改进算法

文献[7]提出的算法可以实现一位  $(2n + 1)$  进制秘密信息  $d$  嵌入到一个载体像素  $g_i$  中, 嵌入信息的计算函数为

$$f = (g_i + x) \bmod (2n + 1) \quad (5)$$

式中,  $|x| \leq n$ 。当  $0 \leq g_i \leq 1$  和  $254 \leq g_i \leq 255$  时,  $x$  取值分别为  $0 \leq x < 2n + 1$  和  $-(2n + 1) < x \leq 0$ 。

通过调整  $x$  使  $f = d$ , 从而载密像素为

$$g'_i = g_i + x \quad (6)$$

从载密像素提取信息的函数为

$$f = g'_i \bmod (2n + 1) \quad (7)$$

### 1.3 基于 EMD 的菱形编码密写算法

文献[8]提出的算法可以实现将一位  $(2k^2 + 2k + 1)$  进制的秘密信息嵌入到两个载体像素对中, 编码计算公式为

$$\begin{cases} S_k(p, q) = \{(a, b) \mid |p - a| + |q - b| \leq k\} \\ |S_k| = 2k^2 + 2k + 1 \end{cases} \quad (8)$$

式中,  $a, b, p$  和  $q$  为像素值,  $k$  为正整数。

当  $k = 2$  时, 菱形编码如图 1(a) 所示。

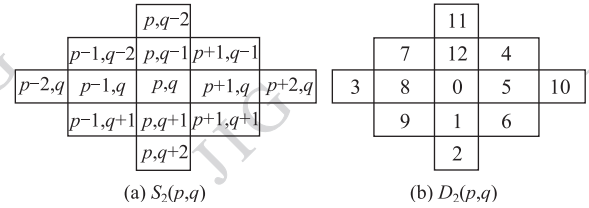


图 1 菱形编码图 ( $k = 2$ )

Fig. 1 Diamond encoding patterns with  $k = 2$

令  $l = |S_k|$ , 定义菱形函数  $f$  来计算嵌入和提取信息时的菱形特征值 (DCV), 其计算公式为

$$f(p, q) = ((2k + 1) \times p + q) \bmod l \quad (9)$$

当  $k = 2$  时, 菱形特征值如图 1(b) 所示。

嵌入信息时, 按式 (9) 计算载体像素  $(x, y)$  菱形函数  $f(x, y)$ 。当  $l$  进制信息  $d = f$  时, 不需修改载体像素  $(x, y)$ ; 当  $d \neq f$  时, 计算  $d$  与  $f$  的模距

$$s = (d - f) \bmod l \quad (10)$$

在菱形特征值表中与  $s$  对应的像素对值的变化量, 即为载体像素  $(x, y)$  应改变的值。如  $k = 2, l = 13$ ,  $(x, y) = (25, 35), d = 5, f(25, 35) = ((2 \times 2 + 1) \times 25 + 35) \bmod 13 = 4, s = (5 - 4) \bmod 13 = 1$ , 对照图 1 所示的编码表, 载密像素对  $(x', y') = (x, y + 1) = (25, 36)$ 。

当载密像素溢出时,  $(x', y')$  需调整为

$$\begin{cases} x' = x' + l & x' < 0 \\ x' = x' - l & x' > 255 \\ y' = y' + l & y' < 0 \\ y' = y' - l & y' > 255 \end{cases} \quad (11)$$

提取信息时, 按式 (9) 计算载密像素  $(x', y')$  的菱形函数  $f(x', y')$ , 即可准确提取秘密信息。

该算法嵌入率为

$$P = \log_2(2k^2 + 2k + 1)/2 \quad (12)$$

## 2 本文算法

### 2.1 相关算法的欠缺

- 1) 嵌入率低, 文献[4]的 EMD 算法的最大理论

嵌入率为 1.16 bit/pixel,文献[7]的 EMD 改进算法的最大理论嵌入率也只有 2.32 bit/pixel。文献[8]的菱形编码信息隐藏算法,表面上可以达到比较高的嵌入率,但其像素最大修改量大,在嵌入率大时载密图像在低亮或高亮区域会出现“群岛像素点现象”,隐蔽性差,不宜取大的嵌入率。

2) 模运算的模只为奇数,文献[4,7]算法的模为  $(2n+1)$ ,文献[8]算法的模为  $(2k^2+2k+1)$ 。这些算法提供可选择的嵌入率种类少;不能将  $L$  位二进制信息完全用  $K$  位  $(2n+1)$  进制或  $(2k^2+2k+1)$  进制表示,更不能 1 位  $(2n+1)$  进制或  $(2k^2+2k+1)$  进制表示,这不仅达不到最大理论嵌入率,而且应用起来不方便,特别是在需要动态改变嵌入率时更不方便。例如,根据式(1),如用 2 位五进制数表示 4 位二进制数,此时 2 位五进制数可表示的数的范围为  $[00,44]_5$ ,4 位二进制数转化为 2 位五进制数的范围为  $[00,30]_5$ ,其中的  $[31,44]_5$  范围内的数没有用来表示二进制的秘密信息。因此,这些算法降低了其应用的效率、灵活性和方便性。

3) 嵌入和提取函数是固定的,都没有考虑算法自身的安全性。载密图像一旦被怀疑或被检测分析有信息隐藏,就会被轻而易举地提取信息。

### 2.2 本文算法

本文算法可实现将一位  $n$  进制秘密信息嵌入到一个载体像素中。为此,对于二进制信息,先将二进制信息流用  $n$  进制表示,然后嵌入载体图像的像素中。

#### 2.2.1 二进制信息流转 $n$ 进制信息流

依次取二进制数据流  $D$  的  $L$  位数字,将其转化为  $K$  位  $n$  进制的数字序列。 $L, K$  的取值计算公式为

$$L = \lfloor K \log_2 n \rfloor \quad (13)$$

当  $n=2^m$  时,可以用一位  $n$  进制信息完全表示  $m$  位二进制信息,即  $K=1, L=m$ 。

#### 2.2.2 嵌入算法

在现有基于模函数的隐写算法基础上,深入研究模运算的正负间周期的特点、考虑算法的安全性而提出新的安全隐写算法,其嵌入函数为

$$f = (\alpha_i + p_i + x) \bmod n \quad (14)$$

式中,  $n=2,3,\dots$ ;  $\alpha_i$  为随像素  $p_i$  变化的安全系数,相当于模距平移量,  $\alpha_i=0,1,2,\dots,n-1$ ;  $x$  为使  $p_i$  变化最小的  $n$  个整数,  $x$  取值范围为

$$-\lfloor n/2 \rfloor \leq x \leq \lfloor n/2 \rfloor, n = 2k + 1 \quad (15)$$

$$-n/2 + 1 \leq x \leq n/2, n = 2k \quad (16)$$

$$-n/2 \leq x \leq n/2 - 1, n = 2k \quad (17)$$

由模数运算规则,满足式(15)(16)或式(17)的  $x$ ,一定使式(14)满足

$$\{f | f = (\alpha_i + p_i + x) \bmod n\} = \{0, 1, 2, \dots, n-1\} \quad (18)$$

也就是说,一位  $n$  进制信息为  $d$ ,在式(15)(16)或(17)所表示的  $x$  范围内完全可以确定一个唯一的  $x$  值,使  $f=d$ 。这时,  $d$  的载密像素  $p'_i$  为

$$p'_i = p_i + x \quad (19)$$

当计算载密像素  $p'_i$  溢出,即  $p'_i < 0$ ,或  $p'_i > 255$  时,根据模数运算周期性特点,对  $p'_i$  调整为

$$\begin{cases} p'_i = p'_i + n & p'_i < 0 \\ p'_i = p'_i - n & p'_i > 255 \end{cases} \quad (20)$$

例如,当  $n=4, \alpha_1=2, p_1=55, n$  进制信息  $d_1=2$  时,嵌入过程为

- 1)  $f = (2 + 55 - 1) \bmod 4 = 0$ ;
- 2)  $f = (2 + 55 - 0) \bmod 4 = 1$ ;
- 3)  $f = (2 + 55 + 1) \bmod 4 = 2 = d_1$ ;
- 4)  $x = 1, p'_1 = p_1 + x = 56$ 。

又例如,当  $n=5, \alpha_2=4, p_2=0, n$  进制信息  $d_2=3$  时,嵌入过程为

- 1)  $f = (4 + 0 - 2) \bmod 5 = 2$ ;
- 2)  $f = (4 + 0 - 1) \bmod 5 = 3 = d_2$ ;
- 3)  $x = -1, p'_2 = 0 - 1 = -1 < 0$ ;
- 4)  $p'_2 = p'_2 + 5 = -1 + 5 = 4$ 。

为提高算法安全性,  $\alpha_i$  的取值按全排列组合成不同的取值方案,并由随机序号  $N_i$  选择取值,其中之一取值方案如表 1 所示。

表 1  $\alpha_i$  的取值与随机序号的对应关系  
Table 1 Corresponding relation of  $\alpha_i$  and  $N_i$

|            | $N_i$ |   |   |     |       |
|------------|-------|---|---|-----|-------|
|            | 0     | 1 | 2 | ... | $n-1$ |
| $\alpha_i$ | 0     | 1 | 2 | ... | $n-1$ |

通过对  $\alpha_i$  的全排列,可以得到  $n!$  种对应关系表,即  $n!$  个取值方案。如当嵌入率为 3 bit/pixel,即  $n=8$  时,则有 40 320 种取值方案,当嵌入率为 4 bit/pixel,即  $n=16$  时,则有  $2.0923 \times 10^{13}$  种取值方案。

序号  $N_i$  由随机数产生,即

$$N_i = \text{rand}_i \bmod n \quad (21)$$

式中,  $rand_i$  为随机整数。

### 2.2.3 提取算法

从一个载密像素中提取一位  $n$  进制信息的函数为

$$f = (\alpha_i + p'_i) \bmod n \quad (22)$$

例如, 在上面嵌入算法中的嵌入例子, 从载密像素  $p'_1$  中提取的信息为  $d_1 = (2 + 56) \bmod 4 = 2$ ; 从载密像素  $p'_2$  中提取的信息为  $d_2 = (4 + 4) \bmod 5 = 3$ 。

### 2.2.4 嵌入率

本文算法的嵌入率为

$$P = \log_2 n \quad (23)$$

由式(23)知, 本文算法的嵌入率是与  $n$  成对数函数递增的嵌入率系列值。

## 3 实验结果与分析

衡量信息隐藏算法的性能指标, 一是嵌入率, 二是载密图像的峰值信噪比 (PSNR), 其计算公式为

$$PSNR = 10 \times \lg(255^2 / MSE) \quad (24)$$

式中, MSE 是原图像与载密图像之间的均方差, 计算公式为

$$MSE = \frac{1}{m \times n} \sum_{i=1}^m \sum_{j=1}^n [I(i, j) - I'(i, j)]^2 \quad (25)$$

式中,  $m$  和  $n$  分别为图像的高和宽。

PSNR 越大, 其图像质量越高。一般要求 PSNR > 30 dB, 理想的图像视觉质量要求 PSNR > 39 dB。

理想的隐写算法是有较高的嵌入率的同时有较好的图像质量。

通过大量实验证明本文算法的有效性和可行性, 限于篇幅, 在此仅给出代表性的实验结果。实验采用 Matlab2008b 平台, 实验图像选用大小为  $512 \times 512$  的 Lena, airplane, peppers 和 baboon 的标准灰度图像, 如图 2 所示;  $n$  进制信息是由 Lorenz 混沌序列处理得到的随机  $n$  进制信息, 信息嵌入像素位置由 Lorenz 混沌序列随机确定, 式(21)中的随机整数  $rand_i$  也由 Lorenz 混沌序列处理得到。  $n$  进制随机信息嵌满载体图像的所有像素; 从载密图像提取的  $n$  进制随机信息与嵌入时的  $n$  进制随机信息完全一致。

### 3.1 嵌入率和不可感知性

#### 3.1.1 本文算法实验

对于不同  $n$  值的载密图像质量和嵌入率的实验结果如表 2 所示。由表 2 中的实验数据表明, 本文算法可以提供精细大范围的嵌入率选择, 且载密图像可以达到比较好的图像质量。

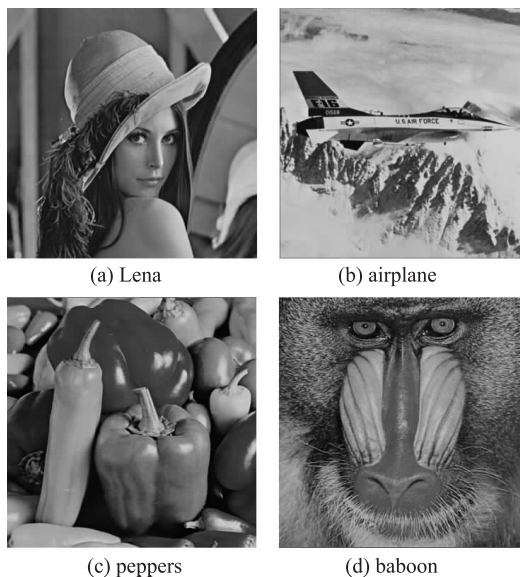


图 2 载体图像

Fig. 2 Cover images

表 2 不同  $n$  值的图像质量和嵌入率

Table 2 PSNR & embedding rate in different  $n$

| $n$ | PSNR/dB |          |         |        | $P /$<br>(bit/pixel) |
|-----|---------|----------|---------|--------|----------------------|
|     | Lena    | airplane | peppers | baboon |                      |
| 2   | 51.15   | 51.12    | 51.15   | 51.13  | 1                    |
| 3   | 49.90   | 49.89    | 49.89   | 49.89  | 1.59                 |
| 4   | 46.36   | 46.37    | 46.36   | 46.37  | 2                    |
| 5   | 45.12   | 45.12    | 45.12   | 45.12  | 2.32                 |
| 6   | 43.11   | 43.12    | 43.12   | 43.12  | 2.59                 |
| 7   | 42.11   | 42.12    | 42.10   | 42.11  | 2.81                 |
| 8   | 40.72   | 40.74    | 40.72   | 40.73  | 3                    |
| 9   | 39.91   | 39.89    | 39.89   | 39.90  | 3.17                 |
| 10  | 38.83   | 38.83    | 38.83   | 38.82  | 3.32                 |
| 11  | 38.13   | 38.13    | 38.13   | 38.12  | 3.46                 |
| 12  | 37.28   | 37.29    | 37.28   | 37.28  | 3.59                 |
| 13  | 36.67   | 36.66    | 36.66   | 36.68  | 3.7                  |
| 14  | 35.94   | 35.96    | 35.96   | 35.96  | 3.81                 |
| 15  | 35.42   | 35.42    | 35.41   | 35.42  | 3.91                 |
| 16  | 34.80   | 34.80    | 34.82   | 34.81  | 4                    |

当嵌入率  $P = 3$  bit/pixel 时, PSNR 大于理想值 39 dB, 各实验载密图像的视觉质量如图 3 所示。与图 2 的原图像相比, 无任何异样感觉, 仍保持很好的图像视觉质量。

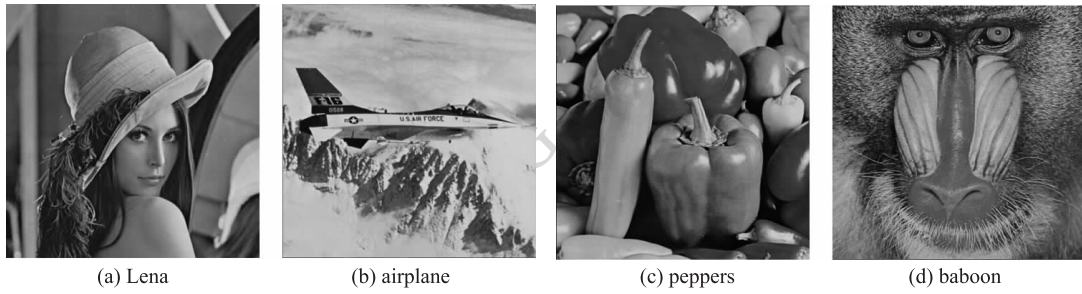


图 3 载密图像  $P=3$  bit/pixel  
Fig. 3 Stego-images,  $P=3$  bit/pixel

当嵌入率  $P=4$  bit/pixel 时,各实验载密图像的视觉质量和对应的直方图如图 4 所示。与图 2 的原图像相比,无任何失真现象,仍保持良好的图像视觉质量;其直方图也无异常现象。

### 3.1.2 与文献[4-6]算法比较

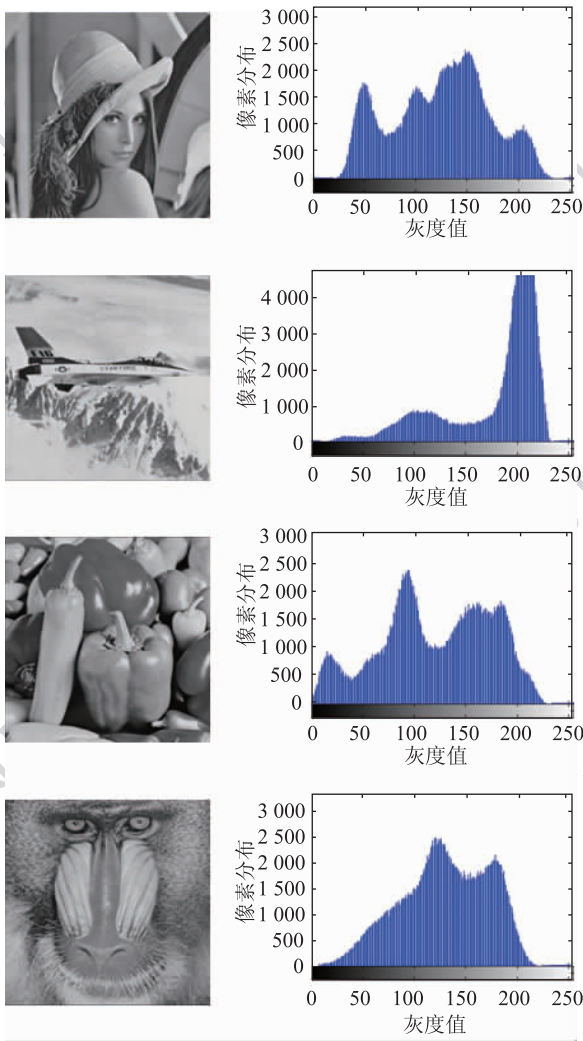
文献[4]算法,  $k=2$  时取得算法的最大理论嵌入率为 1.16 bit/pixel;文献[5]算法只有一种方案;文献[6]算法用  $K$  值决定嵌入像素数,最大理论嵌入率接近 2 bit/pixel。实验项目安排及实验结果如表 3 所示。

与本文算法的表 2 实验结果比较可知,文献[4]算法最大嵌入率下 PSNR 比本文算法最低嵌入率下 PSNR 好些,但嵌入率太小;而本文算法比文献[5-6]算法在同样嵌入率下的 PSNR 稍好些,且嵌入率大而又可调。

表 3 文献[4-6]算法实验项目及实验结果

Table 3 PSNR & embedding rate in different scheme

| 算法              | PSNR/dB |          |         |        | $P/$<br>(bit/pixel) |
|-----------------|---------|----------|---------|--------|---------------------|
|                 | Lena    | Airplane | Peppers | Baboon |                     |
| 文献[4]<br>$k=2$  | 52.11   | 52.10    | 52.11   | 52.11  | 1.16                |
| 文献[5]           | 50.18   | 50.17    | 50.18   | 50.17  | 1.50                |
| 文献[6]<br>$K=70$ | 45.13   | 45.14    | 45.15   | 45.15  | 1.99                |



(a) 载密图像 (b) 直方图

图 4 载密图像及直方图  $P=4$  bit/pixel

Fig. 4 Stego-images & histograms,  $P=4$  bit/pixel

### 3.1.3 与文献[7]算法比较

由文献[7]算法的描述可以推出,当  $2 \leq g_i \leq 253$  时,  $|x| \leq n$ 。如当  $n > 2$  时,像素值  $g_i'$  便溢出,即  $g_i' < 0$  或  $g_i' > 255$ 。由此推知,该算法并没有考虑更大的嵌入率,仅相当于本文算法的  $n=3,5$ ,这时的嵌入率和 PSNR 与本文算法相当,但其最大理论嵌入率仅为 2.32 bit/pixel。

文献[7]算法的模运算的模只为奇数  $(2n+1)$ ,本文算法的模扩展到奇数和偶数,不仅提供更多更细的嵌入率选择,而且可以实现:当  $n=2^m$  时,可以用一位  $n$  进制信息完全表示  $m$  位二进制信息,即可以完全将  $m$  位二进制信息嵌入一个像素中,达到像

素最大修改量下的最大理论嵌入率,且运算方便,可以很方便实现动态改变嵌入率,即自适应嵌入方案。

### 3.1.4 与文献[8]比较

文献[8]算法可以通过取不同的  $k$  值得到不同的嵌入率,但其像素值修改量大,溢出时调整后的像素值修改量更大。

#### 1) 像素值最大修改量比较与分析

从图 4 各载密图像的直方图可知,Lena 图像最不容易溢出,在此仅以 Lena 图像为例测试文献[8]算法的性能。实验项目及实验结果如表 4 所示。

表 4 文献[8]算法实验项目及实验结果 (Lena 图像)

Table 4 Items & results in reference [8] (Lena image)

| $k$ | $ S_k $ | 是否溢出 | 最大修改量 | PSNR/dB | $P/(\text{bit/pixel})$ |
|-----|---------|------|-------|---------|------------------------|
| 1   | 5       | 否    | 1     | 52.10   | 1.16                   |
| 2   | 13      | 否    | 2     | 47.81   | 1.85                   |
| 3   | 25      | 否    | 3     | 44.95   | 2.32                   |
| 4   | 41      | 否    | 4     | 42.81   | 2.68                   |
| 5   | 61      | 否    | 5     | 41.08   | 2.97                   |
| 6   | 85      | 否    | 6     | 39.63   | 3.21                   |
| 7   | 113     | 否    | 7     | 38.39   | 3.41                   |
| 8   | 145     | 否    | 8     | 37.29   | 3.59                   |
| 9   | 181     | 否    | 9     | 36.34   | 3.75                   |
| 10  | 221     | 否    | 10    | 35.48   | 3.89                   |

文献[8]算法的像素值最大修改量等于  $k$ ,本文算法的像素值最大修改量由式(15)–(17)决定。为了比较本文算法与文献[8]算法在不溢出时的像素值最大修改量,本实验绘制各嵌入算法随嵌入率变化的最大像素值修改量曲线图,如图 5 所示。

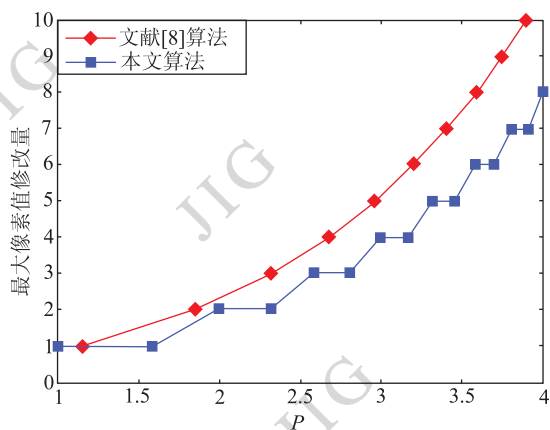


图 5 最大像素值修改量比较

Fig. 5 Maximum pixel value changes of different methods

图 5 实验结果表明,文献[8]算法在  $k > 1$  时,其最大修改量大于本文算法。从表 2 和表 4 的实验数据可知,PSNR 在一定程度上也反映出这种变化。表 5 为两算法在嵌入率相同或相近时的最大修改量比较。

表 5 最大像素值修改量比较

Table 5 Maximum pixel value changes of different methods

| 序号 | 文献[8]算法 |                        | 本文算法 |                        |       |   |
|----|---------|------------------------|------|------------------------|-------|---|
|    | $k$     | $P/(\text{bit/pixel})$ | $n$  | $P/(\text{bit/pixel})$ |       |   |
| 1  | 3       | 2.322                  | 3    | 5                      | 2.322 | 2 |
| 2  | 5       | 2.965                  | 5    | 8                      | 3.000 | 4 |
| 3  | 8       | 3.590                  | 8    | 12                     | 3.585 | 6 |
| 4  | 10      | 3.894                  | 10   | 15                     | 3.907 | 7 |

#### 2) 溢出像素最大修改量比较与分析

从图 4 的各载密图像的直方图可知,Peppers 图像最容易溢出,在此仅以 Peppers 图像为例测试文献[8]算法的性能。实验项目及实验结果如表 6 所示。

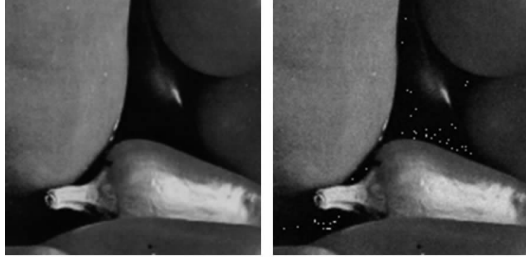
表 6 文献[8]算法实验项目及实验结果(peppers 图像)

Table 6 Items & results in reference [8] (peppers image)

| $k$ | $ S_k $ | 是否溢出 | 最大修改量 | PSNR/dB | $P/(\text{bit/pixel})$ |
|-----|---------|------|-------|---------|------------------------|
| 1   | 5       | 是    | 4     | 52.12   | 1.16                   |
| 2   | 13      | 是    | 11    | 47.79   | 1.85                   |
| 3   | 25      | 是    | 23    | 44.94   | 2.32                   |
| 4   | 41      | 是    | 40    | 42.74   | 2.68                   |
| 5   | 61      | 是    | 58    | 40.90   | 2.97                   |
| 6   | 85      | 是    | 82    | 39.26   | 3.21                   |
| 7   | 113     | 是    | 111   | 37.59   | 3.41                   |
| 8   | 145     | 是    | 144   | 35.86   | 3.59                   |
| 9   | 181     | 是    | 178   | 34.37   | 3.75                   |
| 10  | 221     | 是    | 220   | 32.27   | 3.89                   |

文献[8]算法在像素值溢出时采用模数运算的周期性特点来调整(见式(11)),像素值最大修改量接近模。由于该算法的模随  $k$  的变化很大,调整后的像素值也就比原像素值变化很大,如表 6 实验数据所示。在下界溢出时,像素值由小像素值调整为

大像素值,在上界溢出时,像素值由大像素值调整为小像素值,这种现象将导致在高亮区或低亮区域出现异常的“群岛”像素点,如图6(b)所示;而本文算法在溢出时的像素值最大修改量小于 $n$ ,不会出现这种异常现象。因此,文献[8]算法对载体图像的选择有很大的局限性,对含有低亮或高亮区域的载体图像,只能选择很小的嵌入率。



(a) 原图peppers右下角 (b) 载密peppers右下角

图6 文献[8]算法溢出时的隐秘效果图像

Fig. 6 Stego-images of reference [8] when pixel value overflow

### 3.2 安全性

算法的安全性由控制安全系数 $\alpha_i$ 取值、嵌入像素位置的密钥空间和 $\alpha_i$ 全排列空间决定。对于Lorenz混沌系统,若以双精度浮点数为密钥,取其最保守精度为 $10^{-15}$ ,则密钥空间为 $10^{45}$ ,嵌入算法的密钥空间为 $10^{45}n!$ 。仅以Lorenz密钥空间计算,若完成一次解密的时间为 $10^{-3}$ s,则用密钥穷举法进行取密需要 $3.17 \times 10^{34}$ a。因此,非法者用密钥穷举法进行破密是很难在有限的时间内取密成功的。

对于一幅大小为 $m \times n$ 的载密图像,如采用穷举法对载密像素提取信息,嵌入率为 $k$ ,则计算次数为

$$NC = (mn)!(2^{mn} + 2^{2mn} + \dots + 2^{kmn}) = (mn)!2^{mn}(2^{kmn} - 1)/(2^{mn} - 1) \quad (26)$$

因此,对于大小达到一定规模的载密图像来说,穷举法对像素提取信息几乎是不可能成功的。

## 4 结论

理论分析与实验结果表明,本文算法与文献[4-8]等基于EMD的信息隐藏算法相比,具有主

要的如下3个重要特点:

- 1) 在保持良好的载密图像视觉质量的情况下达到更大的嵌入量;
- 2) 模运算的模扩充至奇数和偶数,不仅可提供的嵌入率种类翻倍,而且应用效率更高、更方便;
- 3) 引入随机安全系数,增强了算法的安全性。

因此,本文算法具有更强的实用性。用户可以根据实际应用要求选择嵌入率,使嵌入量与载密图像视觉质量之间达到很好的平衡。

### 参考文献(References)

- [1] Chan C K, Cheng L. Hiding data in images by simple LSB substitution[J]. Pattern Recognition, 2004, 37(3): 469-474.
- [2] Wu H C, Wu N I, Tsai C S, et al. Image steganographic scheme based on pixel-value differencing and LSB replacement methods [J]. IEEE Proceedings Vision, Image & Signal Processing, 2005, 152(5): 611-615.
- [3] Zhou Z P, Kang H, Lin J J, et al. A LSB steganalysis algorithm based on image wavelet detail information [J]. Journal of Image and Graphics, 2008, 13(6): 1090-1093. [周治平, 康辉, 林家骏, 等. 小波细节信息的LSB隐写分析算法[J]. 中国图象图形学报, 2008, 13(6): 1090-1093.]
- [4] Zhang X P, Wang S Z. Efficient steganographic embedding by exploiting modification direction [J]. IEEE Communications Letters, 2006, 10(11): 781-783.
- [5] Lee C F, Wang Y R, Chang C C. A steganographic method with high embedding capacity by improving exploiting modification direction [C]//Proceedings of the Third International Conference on International Information Hiding and Multimedia Signal Processing. Washington, USA: IEEE Computer Society, 2007, 1: 497-500.
- [6] Wang Z H, Kieu T D, Chang C C, et al. A novel information concealing method based on exploiting modification direction [J]. Journal of Information Hiding and Multimedia Signal Processing, 2010, 1(1): 1-9.
- [7] Jung K H, Yoo K Y. Improved exploiting modification direction method by modulus operation [J]. International Journal of Signal Processing, Image Processing and Pattern, 2009, 2(1): 79-88.
- [8] Chao R M, Wu H C, Lee C C, et al. A novel image data hiding scheme with diamond encoding [J]. EURASIP Journal on Information Security 2009(2009): 658047(1-9).