

# 一种改进的 LSB 数字图像隐藏算法<sup>\*</sup>

袁占亭, 张秋余, 刘洪国, 彭 铎

(兰州理工大学 计算机与通信学院, 兰州 730050)

**摘 要:** 目前针对常用的 LSB 信息隐藏, SPA 分析 (sample pair analysis) 和 RS 方法 (regular and singular groups method) 能以很高的精度估计出图像中隐藏信息的比率。基于几何变换的性质, 提出了一种可用于图像置乱技术的亚仿射变换, 并利用矩阵编码思想改进 LSB 的嵌入方式, 从而使嵌入数据获得了较好的抗隐写分析性能。实验结果表明, 该算法能有效抵抗 RS 和 SPA 隐写分析, 并保持图像的直方图统计特征, 且适用于灰度图像和彩色图像, 易于实现。

**关键词:** 信息隐藏; 抗隐写分析; 改进的最低有效位嵌入; 亚仿射变换; 图像置乱

**中图分类号:** TP391      **文献标志码:** A      **文章编号:** 1001-3695(2009)01-0372-03

## Improved LSB steganography method

YUAN Zhan-ting ZHANG Qiu-yu LIU Hong-guo PENG Duo

(School of Computer & Communication Lanzhou University of Technology Lanzhou 730050, China)

**Abstract** As for the common LSB steganography, SPA (sample pair analysis) and (regular and singular groups method) could estimate the embedding rate in image with high precision. This paper presented a subset of affine transformation with integer coefficients and invariance of image area to realize the scrambling of digital image. A perfect steganographic encoding scheme based on linear block code theory LSB steganography which made the embedded messages have more steganalysis counteraction ability. Experimental results show that the proposed approach is undetectable by RS (regular singular) steganalysis and SPA (sample pair analysis) steganalysis and the histogram's statistical property is preserved well. Otherwise it is applicable for both gray images and color images and can be implemented conveniently.

**Key words** information hiding; steganalysis counteraction; improved LSB (least significant bit) embedding; sub-affine transformation; image scrambling

### 0 引言

信息隐藏是一个崭新的研究领域, 它横跨数字信号处理、图像处理、语音处理、模式识别、数字通信、多媒体技术、密码学等多个学科, 它是把一个有意义的秘密信息隐藏在另一个称为载体的信息 (如普通图片) 中, 得到隐密载体。非法者不知道这个普通信息中是否隐藏了其他信息, 而且即使知道, 也难以提取或去除隐藏的信息。信息隐藏中所用的载体可以是文字、图像、声音及视频等。到目前为止, 研究最成熟的信息隐藏载体就是数字图像。

信息隐藏技术基本上可以分为两大类, 即空域法和频域法。LSB 是空域法中常见的算法, 就是用秘密信息位来替换最不重要位, 传统的 LSB 嵌入方式主要分为序贯式嵌入和随机间隔式嵌入<sup>[1]</sup>。图像像素的最低 1、2 位所组成的位平面反映的基本是噪声, 没有太多的图像有用信息。因此, 传统的 LSB 算法是在载体元素的一个最低位嵌入 1 bit 秘密信息 (或在载体元素的两个最低位嵌入 2 bit 秘密信息)。LSB 算法以其隐蔽性好、信息隐藏量大且易于实现等优点, 而被广泛采用。

近年来, 很多专家学者对 LSB 隐藏和分析技术进行了深

入研究。很多方法对传统的 LSB 隐藏算法分析已经趋于成熟, 如 Fridrich 等人<sup>[2]</sup>提出了一种 24 bit 彩色图像中空域 LSB 隐藏信息的 RPQ (the raw quick pairs) 检测方法。该方法简单且计算复杂度小, 当颜色数小于像素数目的 30% 时可以得到较好的判别效果。该方法只适用于彩色图像。如果图像中的色彩数超过图像总像素数目的 50%, 该方法的结论就不太可靠。Fridrich 等人<sup>[3,4]</sup>还提出了 RS 方法。该方法通过统计图像中正则组和奇异组数量的变化来估计嵌入长度, 适合于彩色或灰度图像。当信息非顺序嵌入时可以比较精确地估计隐藏长度。Dumit 等人<sup>[5]</sup>通过样本分析对 LSB 隐藏信息进行检测 (记为 SPA) 方法。当嵌入在 LSB 上的信息的比例大于 3% 时, 该方法能以相当高的精度估计出隐藏信息的长度。

随着隐写分析技术的不断发展, 对信息伪装算法的性能要求也越来越高, 在保持相当嵌入容量的同时提高算法的安全性, 成为信息伪装技术研究中的重点和难点。大量研究及实验表明, 对载密图像在嵌入秘密信息之前进行置乱变换能够有效地与处理方法对嵌入载体进行一定的预处理可为提高系统的安全性带来帮助, 对于以图像为载体的信息伪装系统来说, 置乱变换是一种有效的预处理方法。

本文提出一种基于亚仿射变幻<sup>[6]</sup>的图像置乱变换的信息

**收稿日期:** 2008-03-10; **修回日期:** 2008-05-23      **基金项目:** 国家科技支撑计划资助项目 (2006BAF01A21)

**作者简介:** 袁占亭 (1961-), 男, 陕西扶风人, 教授, 博导, 主要研究方向为信息安全、图像处理与模式识别、软件工程、计算机视觉 (lhighs@lzu.cn); 张秋余 (1966-), 男, 河北丰集人, 副研究员, 硕导, 主要研究方向为信息安全、图像处理与模式识别、软件工程、计算机视觉; 刘洪国 (1980-), 男, 山东泰安人, 硕士研究生, 主要研究方向为多媒体通信、信息隐藏; 彭铎 (1976-) 男, 甘肃兰州人, 讲师, 主要研究方向为无线电通信、多媒体通信。

伪装算法。首先对图像进行亚仿射置乱变换的预处理,记下变换次数,并以此作为密钥来控制数据嵌入和提取,再利用矩阵编码思想改进 LSB 的嵌入方式,嵌入完毕利用置乱变换的周期进行恢复,最终得到载密图像。在提取时只需对载密图像以密钥次数进行置乱,再提取图像的 LSB 即可。

1 图像置乱与亚仿射变换

针对大幅图像的信息隐藏问题,置乱技术是基础性的工作,已有很多文献提出了图像置乱的方法,如 Amold 变换<sup>[7]</sup>、Fibonacci<sup>[8,9]</sup>变换、排列变换<sup>[10]</sup>、骑士巡游变换等<sup>[11,12]</sup>。经典的 Amold 变换及基于几何运算的排列变换的参数仅有四个,用于数据加密尚嫌太少<sup>[7]</sup>。基于采样理论的排列变换和基于几何运算的排列变换,前者使得变换后的图像在视觉上通常具有基本上相同的形态,达不到置乱加密的要求;后者推广了 Amold 变换。骑士巡游变换虽然有较大的密钥,但计算复杂度较高,且要经多次迭代才能达到满意的置乱效果<sup>[11]</sup>。本文采用亚仿射变换<sup>[12]</sup>。

1.1 亚仿射变换的定义

仿射变换的一般形式为 $\begin{cases} x' = ax + by + e \\ y' = cx + dy + f \end{cases}$ ,对给定的 N 阶数字图像用  $A = \{a(i, j)\}_{N \times N}$  表示,若变换

$$\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} + \begin{pmatrix} e \\ f \end{pmatrix} \tag{1}$$

其中:  $a, b, c, d, e, f$  为整数,  $x, y \in \{1, 2, \dots, N\}$  满足:

条件 1 变换是离散点域  $\{(x, y); 1 \leq x \leq N, 1 \leq y \leq N\}$  到其自身的单映射;

条件 2 变换是离散点域  $\{(x, y); 1 \leq x \leq N, 1 \leq y \leq N\}$  到其自身的满映射,则称该变换为图像的亚仿射变换。

从数据加密角度比较,亚仿射变换中有六个参数可供选择,比几何变换增加了两个;从密钥量角度出发,增加了大量的密钥。

1.2 亚仿射变换的解

对于平面仿射几何变换,将三对变换点代入矩阵式后就可完全确定  $a, b, c, d, e, f$  即可求得仿射变换的解。

例如,指定三个变换点对为  $(1, 1) \rightarrow (N, N)$ ,  $(1, N) \rightarrow (N, 1)$ ,  $(N, 1) \rightarrow (1, N)$ , 分别代入式 (1) 求得的解为  $a = -1, b = 0, c = 0, d = -1, e = N + 1, f = N + 1$ , 即所求的亚仿射变换为

$$\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} + \begin{pmatrix} N+1 \\ N+1 \end{pmatrix} \quad (x, y \in \{1, 2, \dots, N\})$$

但并不是任意指定的三个变换点对均能得到亚仿射变换。例如,指定三个变换点对为  $(1, 1) \rightarrow (N, 1)$ ,  $(N, N) \rightarrow (1, 1)$ ,  $(2, 1) \rightarrow (N, 2)$ , 分别代入式 (1) 求得的解为  $a = 0, b = -1, c = 1, d = -1, e = N + 1, f = 1$ 。容易验证,这样得到的仿射变换并不是定义 2 给出的亚仿射变换,因为它不满足定义中的条件 1 和 2。这说明亚仿射变换并不容易求出,需要很强的技巧。给出另外两个亚仿射变换如下<sup>[13]</sup>:

$$\begin{pmatrix} x \\ y \end{pmatrix} = \begin{cases} \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} + \begin{pmatrix} N+1 \\ 0 \end{pmatrix} & \text{当 } x < y \text{ 时} \\ \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} + \begin{pmatrix} 1 \\ N+1 \end{pmatrix} & \text{当 } x \geq y \text{ 时} \end{cases} \tag{2}$$

$x, y \in \{1, 2, \dots, N\}$

$$\begin{pmatrix} x \\ y \end{pmatrix} = \begin{cases} \begin{pmatrix} 1 & -1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} + \begin{pmatrix} N+1 \\ N+1 \end{pmatrix} & \text{当 } x < y \text{ 时} \\ \begin{pmatrix} 1 & -1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} + \begin{pmatrix} 1 \\ N+1 \end{pmatrix} & \text{当 } x \geq y \text{ 时} \end{cases} \tag{3}$$

$x, y \in \{1, 2, \dots, N\}$

1.3 亚仿射变换在图像置乱中的应用

一幅数字图像可用矩阵  $A = \{a(i, j)\}_{N \times N}$  表示。其中  $a(i, j)$  表示图像在第  $i$  行  $j$  列像素处的灰度值 (或 RGB 分量值)。数字图像的置乱原理是:将原来点  $(x, y)$  处像素对应的灰度值或 RGB 颜色值移动到变换后的点  $(x', y')$  处。如果对一幅数字图像迭代地使用亚仿射变换,即将左端的  $(x', y')^T$  作为下一次相应变换的输入,则可重复这个过程一直做下去。用式 (3) 给出仿射几何变换,对 Lena 图像 (512×512 像素) 进行置乱的效果如图 1 所示。

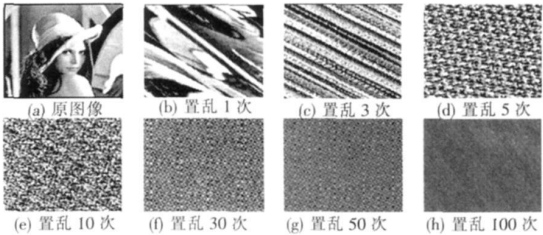


图 1 灰度图像 Lena 的置乱

从图 1 可以看出,亚仿射变换用于图像置乱有较好的置乱效果。在经过一定的迭代置乱变换后,可将原图像的各种灰度值均匀地分布到图像区域中,从而能较好地隐蔽原图像的信息,为进一步进行图像隐藏打下良好的基础。

1.4 亚仿射变换应用于图像置乱的周期性

图像置乱的周期定义如下:对数字图像  $A = \{a(i, j)\}_{N \times N}$ , 如果亚仿射变换  $\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} + \begin{pmatrix} e \\ f \end{pmatrix}$  关于 A 的周期为  $T_N$ , 则  $T_N$  是使得图像 A 经一系列变换后回复到 A 的最小次数。由亚仿射变换的定义及图像置乱周期的定义,以式 (3) 定义的亚仿射变换为例,假定图像为  $N \times N$  像素,求得其周期  $T_N$  如表 1 所示。

表 1 亚仿射变换在不同图像尺寸 N 下的周期 $T_N$							
N	$T_N$	N	$T_N$	N	$T_N$	N	$T_N$
2	3	10	60	6	24	50	300
3	8	11	11	7	16	100	300
4	6	12	12	8	12	250	1 500
5	20	25	100	9	24	300	600

从信息隐藏的角度考虑,图像置乱变换作为进一步处理的预处理,如置乱后再进行隐藏,Amold 变换在进行迭代置乱时,很多时候有较强的纹理特征,在用 Cox 的水印方法进行隐藏时,为达到隐藏的目的就必须减小其强度控制参数,因而降低了隐蔽信道的容量。而亚仿射变换使得图像置乱后,其各种灰度值均匀分布在图像所在的区域  $\{(x, y); 1 \leq x \leq N, 1 \leq y \leq N \text{ 且为整数}\}$ , 减少了置乱图像的纹理特征,从而可以增加隐蔽信道的容量。从这个角度考虑,亚仿射变换也优于 Amold 等几何变换。

2 改进型 LSB 嵌入方式

Crandall<sup>[14]</sup>首次提出矩阵编码可以应用到基于 LSB 替换的信息伪装系统中来提高嵌入效率。如果嵌入的秘密消息长度小于载体图像的嵌入容量,采用矩阵编码可以减少对载体图

像 LSB平面带来的改变。矩阵编码方法<sup>[15]</sup>的基本思想是用  $n$  个 LSB位来表示  $k$  bit信息 ( $n>k$ )。例如要在三个 LSB位嵌入两个 bit  $x_1、x_2$ 。可以做到最多改变一个 LSB位来表示这两个 bit关系如下:

$$\begin{aligned} x_1 &= a_1 \oplus a_2, x_2 = a_2 \oplus a_3 \Rightarrow \text{不作改变} \\ x_1 &\neq a_1 \oplus a_2, x_2 = a_2 \oplus a_3 \Rightarrow \text{改变 } a_1 \\ x_1 &= a_1 \oplus a_2, x_2 \neq a_2 \oplus a_3 \Rightarrow \text{改变 } a_2 \\ x_1 &\neq a_1 \oplus a_2, x_2 \neq a_2 \oplus a_3 \Rightarrow \text{改变 } a_3 \end{aligned}$$

从上式可以看出,在这四种情况下最多只需改变一个 LSB位就能达到目的。对于最多只需改变一个 LSB位,用  $n$  个 LSB来表示  $k$  bit信息的情况,记为  $(1, n, k)$ 。每一个信息比特的码长是  $n=2K-1$ 。可以定义改变密度 (change density)为:通过改变  $n$ 和  $k$ 的值,可以进一步降低  $D(k)$ ,当然算法复杂度也随之上升。可以看出,矩阵编码技术使得嵌入的信息不再是 50%会改变图像像素的 LSB,而是随着  $n$ 和  $k$ 选取的不同而不同。如果将矩阵编码技术运用到空域掩密算法中,就可在一定程度上抵抗 RS攻击。所以应该根据要嵌入信息的大小和载体图片的大小动态地调整要使用的  $n、k$ 这样使得  $D(k)$ 对不同的嵌入信息长度有着不同的值。

改进后的算法主要运算步骤如下:

- a)对要嵌入的信息进行压缩,这样可以提高嵌入的信息长度。
- b)根据嵌入信息的长度和图像的大小确定要使用的  $n、k$ 。
- c)使用一个安全的随机数生成器,利用密钥生成信息嵌入的位置。
- d)按照上述矩阵编码方案进行信息嵌入。

3 实验结果与分析

为验证算法的性能,本文做了两个实验:

**实验 1** 选取了大小为  $512 \times 512$  的标准灰度图像 boy和彩色图像 Lena作为载体图像(图 2),在嵌入率为 30%时进行了实验,以峰值信噪比 (PSNR)作为图像质量退化度量。为区别灰度图像和彩色图像的嵌入效果,对彩色图像的三个颜色分量 (RGB)分别进行检测和计算 PSNR。

**实验 2** 以彩色图像 Lena为载体图像,比较了改进型嵌入算法对 RS和 SPA分析方法在不同的图像嵌入率下估计结果影响。



图 2 原始载体图像及加密信息

实验 1标准灰度图像 boy和彩色图像 Lena的峰值信噪比 (PSNR)实验如图 3~6所示。

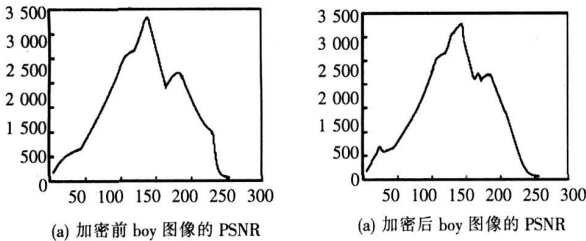


图 3 加密前后 boy 图像的 PSNR

方法的结果影响。其分析估计值的比较如表 2、3所示,结果如图 7所示。

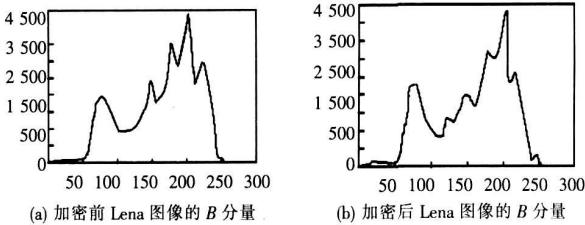


图 4 加密前后 Lena 图像 B 分量的 PSNR

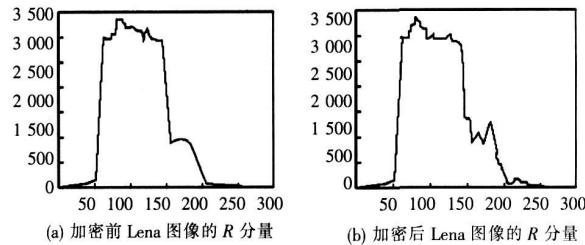


图 5 加密前后 Lena 图像 R 分量的 PSNR

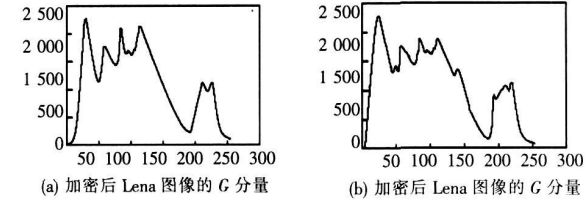


图 6 加密前后 Lena 图像 G 分量的 PSNR

表 2 不同嵌入率下 SPA 分析估计值的比较

嵌入比率/%	估计值/%	
	普通嵌入	改进后
5	5.18	0.32
10	13.22	0.49
30	35.64	0.67
60	64.37	1.06
90	88.79	1.73

表 3 不同嵌入率下 RS 分析估计值的比较

嵌入比率/%	估计值/%	
	普通嵌入	改进后
5	5.35	0.33
10	13.79	0.49
30	37.12	0.74
60	66.13	1.19
90	89.45	1.82

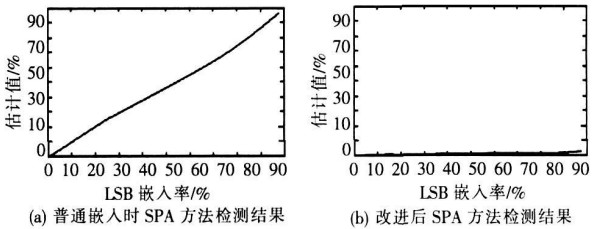


图 7 不同嵌入方法时 SPA 方法分析结果比

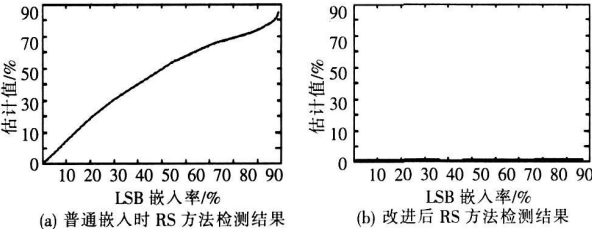


图 8 不同嵌入方法时 RS 方法分析结果比

4 结束语

通过结合亚仿射图像置乱变换与改进的 LSB嵌入方案,可使信息伪装系统在消息嵌入量和失真度与传统的 LSB嵌入算法保持一致的情况下,获得更好的安全性。以置乱次数作为控制消息嵌入和提取的密钥,同时以抗隐写分析 (下转第 377 页)

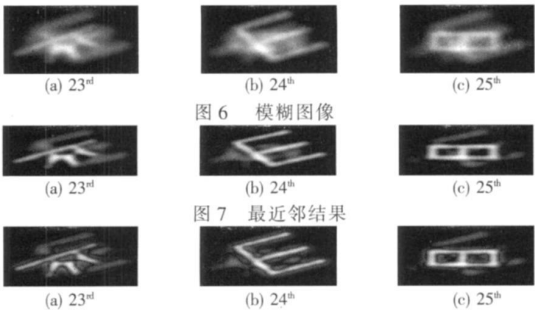


图 8 本算法迭代一次结果

2.1.2 真实样本实验

已知样本序列的成像参数为:透视镜质折射率  $n=1$ , 数值孔径  $NA=0.8$ , 系统两个通道的波长分别为  $0.52\text{ }\mu\text{m}$ ,  $0.52\text{ }\mu\text{m}$ ; 像素的尺寸为  $\Delta X=0.07\text{ }\mu\text{m}$ ,  $\Delta Y=0.07\text{ }\mu\text{m}$ ,  $\Delta Z=0.15\text{ }\mu\text{m}$ 。序列图像尺寸为  $64\times 64\times 64$ 。

图 9 为真实样本模糊图像;图 10 为最近邻算法实验结果;图 11 为采用本算法对图 10 的序列去模糊的结果。从真实样本实验中可以看出使用本方法的图像与最近邻复原的结果相比更加清晰。

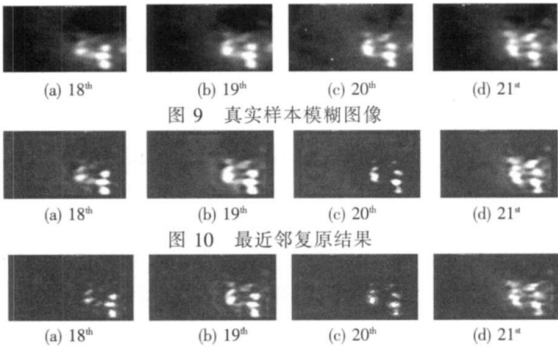


图 11 本算法迭代一次去模糊结果

3 结束语

将高维几何空间的图像复原理论应用于 COSM 中的最近邻

算法,具有以下优点:速度快,结合最近邻算法既取得了优于最近邻算法的实验效果又不会影响复原算法的速度,具有应用价值。对点扩展函数的精度要求不是很严格,用高斯点扩展函数对真实的点扩展函数进行模拟,不会对算法的处理结果产生较大的影响,可广泛应用于模糊图像的复原中。本文对如何去除三维图像的本层模糊提供了一种方法,如何利用高维空间几何理论去除图像的层间模糊,还有待于发展和研究。

参考文献:

[1] McNALLY J G. Computational optical-sectioning microscopy for 3D quantitation of cell motion: results and challenges [J]. SPE, 1994, 2302: 342-351.

[2] FANO M, POLAK M. The 3D object reconstruction from 2D slices—image preprocessing[J]. The Central European Seminar on Computer Graphics, 2000, 5: 14-15.

[3] SARDER P, NEHORIAIA. Deconvolution methods for 3-D fluorescence microscopy images[J]. IEEE Signal Processing Magazine, 2006, 23 (3): 32-45.

[4] 孟庆浩,周荣彪.复合帧运动模糊图像复原方法研究[J].计算机工程, 2006, 32(13): 187-189.

[5] 王守觉,谢美芬,曹文明.图像恢复的一种新方法[C]//2006年中国控制与决策年会论文集.天津:[出版者不详], 2006: 241-246.

[6] 沈永增,叶鸿敏,张敏捷.基于高维空间几何分析理论的图像增强实现[J].计算机仿真, 2007, 24(6): 191-193.

[7] 王守觉,王柏楠.神经网络的多维空间几何分析及其理论[J].电子学报, 2002, 30(1): 1-4.

[8] 王守觉.仿生模式识别(拓扑模式识别)——一种模式识别新模型的理论与应用[J].电子学报, 2002, 30(10): 1-4.

[9] 陶青川,邓宏彬.基于小波变换的高斯点扩展函数估计[J].光学技术, 2004, 30(3): 284-289.

[10] 李蕊,陶青川,何小海,等.基于高斯型点扩展函数的改进最近邻算法[J].光电工程, 2007, 34(6): 97-101.

(上接第 374 页)的嵌入方案将消息嵌入到置乱的图像中,这为消息的嵌入提供了抵抗隐写分析攻击和防止第三方提取这两个层次上的安全保障。从实验效果可以看出,置乱变换可作为消息载体的一种有效的预处理手段,但由于置乱变换的运算量一般都比较大,算法的运算量要高于传统的 LSB 嵌入算法。这也是在下一步研究中需要继续改进和努力的地方。

参考文献:

[1] SIEFAN K, FABIAN A, PETITCOLAS P. 信息隐藏技术——隐写术与数字水印[M]. 吴秋新,钮心忻,杨义先,等译.北京:人民邮电出版社, 2001.

[2] FRIDRICH J, GOLJAN M, DU R. Detecting LSB steganography in color and gray-scale images[J]. IEEE Multimedia, 2001, 8(4): 22-28.

[3] FRIDRICH J, GOLJAN M. Practical steganalysis of digital images—state of the art[C]//Proc of SPIE: Security and Watermarking of Multimedia Contents IV, 2002: 1-13.

[4] FRIDRICH J, GOLJAN M, DU R. Reliable detection of LSB steganography in color and grayscale images[C]//Proc of the ACM Workshop Multimedia Security Ottawa, [s n.], 2001: 27-30.

[5] DUMITR S, WU Xiao-lin, WANG Zhe. Detection of LSB steganography via sample pair analysis[J]. IEEE Trans on Signal Processing, 2003, 51(7): 1995-2007.

[6] 柏森,胡中豫,吴乐华,等.通信信息隐匿技术[M].北京:国防工业出版社, 2005.

[7] QIDong-xu, ZOU Jian-cheng, HAN Xiao-you. A new class of scrambling transformation and its application in the image information covering [J]. Science in China (Series E), 2000, 43(3): 304-312.

[8] 丁玮,齐东旭.数字图像变换及信息隐藏与伪装技术[J].计算机学报, 1998, 21(9): 839-843.

[9] 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): 339-341.

[10] 吴升,王介生,刘慎权.图像的排列变换[J].计算机学报, 1998, 21(6): 514-519.

[11] 柏森,曹长修,曹龙汉.基于骑士巡游变换的图像细节隐藏技术[J].中国图象图形学报, 2001, 6(11): 1096-1100.

[12] 柏森,曹长修.一种新的数字图像置乱隐藏算法[J].计算机工程, 2001, 27(11): 18-19.

[13] BAI Sen, CAO Chang-xiu. Property of sub-affine transformation and its application[J]. Journal of Computer Aided Design & Computer Graphics, 2003, 15(2): 205-214.

[14] CRANDALL R. Some notes on steganography[EB/OL]. (1998). <http://os.inf.wurdresden.de/~westfeld/crandall.pdf>

[15] ZHANG Tao, PENG Xi-jian. Steganalysis of spatial LSB based steganographic algorithms and countermeasures[J]. Journal of China Institute of Communications, 2003, 24(12): 156-163.