

基于边缘匹配和模函数的安全密写算法

廖琪男

(广西财经学院计算机与信息管理学系,广西南宁 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,提出一种新的密写算法.根据人类视觉特性,利用像素的 3 个相邻像素的最大像素值与最小像素值的差值,将图像分为平滑区、过渡区和边缘区;根据模数循环的特点,应用具有安全特性的模函数以某一嵌入方案在 3 个区域中的像素自适应地嵌入不同的信息比特数.选择不同的嵌入方案可以得到不同的嵌入量和载密图像视觉质量.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.

关键词: 信息隐藏;边缘匹配;像素差值;模函数

中图分类号: TP391 **文献标识码:** A **文章编号:** 0372-2112 (2012)10-2002-07

电子学报 URL: <http://www.ejournal.org.cn> **DOI:** 10.3969/j.issn.0372-2112.2012.10.017

Secure Steganographic Algorithm Based on Side Match and Modular Function

LIAO Qi-nan

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

Abstract: To provide a large, scalable embedding capacity and maintain a good visual quality of stego-image, this paper presents a novel steganography. According to human visual characteristic, the algorithm divides an image into smooth area, transition area, and edged area by the difference between the maximum pixel value and the minimum pixel value of 3 neighboring pixels; according to the characteristics of the module cycle, it uses modulus function with security features to adaptively embed different bits information into a pixel in 3 different areas with one of the embedding schemes. Different embedding scheme gets different rates of embedding and visual quality of stego-image. Experimental results show that the algorithm can maintain a high embedding rate while maintaining good visual quality of stego-image, and good security.

Key words: steganography; side match; pixel-value difference; modular function

1 引言

Internet 的推广与普及,在为人们沟通、数字产品流通、电子商务、电子政务、电子金融等政治与经济活动带来空前便利的同时,也暴露出越来越严重的数据安全问题.为了保证信息的安全,人们广泛使用加密技术对信息加密后传输,但这种安全方式容易引起窃密者的拦截与破解,或恶意破坏.在这种情况下,一种新的信息安全技术——信息隐藏技术应运而生,成为举世关注的时代大课题,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.

在现有的数字密写算法中,最简单而又著名的方法就是最低有效位 (Least Significant Bit, LSB) 取代算法和基于 LSB 的密写算法^[1-3],LSB 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.2006 年 Zhang 与 Wang 两人提出 EMD (Exploiting Modification Direction) 信息隐藏方法^[4],该方法是利用模数运算的余数循环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,故有许多研究者都参考模数运算的这种特性提出改进式模数运算信息隐藏算法^[5,6],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.

2004 年,Chang 等人提出一种基于图像像素边缘匹配 (Side Match, SM) 的隐写算法^[7].它利用像素间灰度差值进行密写,通过相邻像素间的相关性来估计像素间是平滑的还是起伏剧烈的,在平滑区嵌入量少,而在起伏剧烈区则嵌入量大.但该算法嵌入量小,会引起像素灰度值直方图统计特性的异常,使差值直方图出现阶梯现

象^[8],容易被差值直方图分析检测.由于 SM 利用了人类视觉系统(Human Vision System, HVS)的特性,针对不同区域分别处理,因此,不少学者提出基于 SM 的改进隐写算法^[9~11],以改进 SM 性能.文献[9]算法,改变像素差的计算方法,使像素差与当前像素无关;文献[10]算法,动态地划分像素差的区间,以消除像素差值直方图异常;文献[11]应用 LSB 思想的嵌入算法代替原 SM 的嵌入算法,信息嵌入量大幅度增加.

完备的密写技术应该具备如下几方面条件:不可感知性、嵌入量大、不可检测性和嵌入算法的安全性等.目前很多信息隐藏研究的相关文献中只考虑前面两个条件,很少考虑第 3 条件,几乎没有考虑第 4 条件,这是很不够的.载密图像一旦被怀疑或被检测分析有信息隐藏,就被拦截和攻击;嵌入算法一旦公开,秘密信息将会被破解泄密.

提高载密图像的不可感知性的有效方法可以采用密写编码技术,因为这些编码技术是在信息嵌入时以占用较多的像素为代价,换取对像素的较少改动,因此失真较小,不可感知性就好.如文献[12]提出,在一个 $m \times n$ 的二值图像块中,最多改变 1 个像素即可嵌入最大信息量为 $\lfloor \log_2(mn + 1) \rfloor$ bit; Crandall^[13]首先提出矩阵编码可以应用到基于 LSB 的信息隐藏系统中以提高嵌入效率, Westfeld^[14]首次实现矩阵编码,提出可以在 $n = 2^k - 1$ 个像素中,最多改变 1 个像素的 LSB 便可以嵌入 k bit 信息; Zhang 与 Wang 两人提出基于稀疏表示的密写编码^[15],其编码性能优于矩阵编码.这些编码技术应用用于对像素值修改特别敏感的二值图像密写算法,其视觉质量将得到明显提高,如文献[16]提出的二值图像密写算法中就应用了矩阵编码.但这些编码使算法嵌入率降低,对于冗余空间较大的灰度图像密写来说,其应用价值并不大.

本文在研究现有的基于 SM 和 EMD 算法基础上,提出在不可感知性、嵌入量最大化、不可检测性和算法安全性等方面都有非凡表现的数字图像密写算法.

2 相关算法

SM 及基于 SM 改进算法,首先根据一个像素的相邻像素计算像素值差值,然后根据该差值决定该像素的信息嵌入量,最后给出信息的嵌入算法.这些算法,保持载体图像的第 1 行和第 1 列像素灰度值不变,从第 2 行第 2 列的像素开始进行光栅扫描,逐个像素嵌入信息.这些算法所描述的目标像素 $p_{i,j}$ 及其相邻像素关系如图 1 所示.

Chang 等人的 SM 算法^[7]、文献[10,11]算法的像素差值计算方法为

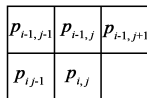


图1 目标像素及其相邻像素

$$d = (p_{i,j-1} + p_{i-1,j})/2 - p_{i,j} \quad (1)$$

这种差值的计算方法增加了嵌入算法的复杂性,为此文献[9]提出改进像素值差值计算方法,该算法用 $p_{i,j-1}, p_{i-1,j-1}, p_{i-1,j}, p_{i-1,j+1}$ 四个相邻像素的最大像素值与最小像素值之差作为当前像素 $p_{i,j}$ 的信息嵌入率参考依据.

限于篇幅,这些算法的嵌入算法的陈述从略,详见相应参考文献.

3 本文算法

为了弥补基于边缘匹配密写算法的嵌入率不可选、视觉质量不够理想,以及包括基于 EMD 算法等的嵌入率低、安全性差等欠缺或不足,提出本文算法.

本文算法可实现将 k 位二进制秘密信息嵌入到一个像素中.

3.1 目标像素差值及其信息嵌入方案

本文算法的像素差值的计算方法采用文献[9]的算法思想,但只计算目标像素的左三个相邻像素,因为文献[9]的四个相邻像素使计算像素的距离增大,像素最大值与最小值的差值也可能增大,致使临界像素被不合理地划分到过渡区或边缘区.目标像素的像素值差值定义为

$$d = p_{\max} - p_{\min} \quad (2)$$

式中, $p_{\max} = \max(p_{i,j-1}, p_{i-1,j-1}, p_{i-1,j})$, $p_{\min} = \min(p_{i,j-1}, p_{i-1,j-1}, p_{i-1,j})$.

参考文献[17]的 PVD(Pixel-Value Differencing)分区思想,将边缘匹配像素差值划分为平滑区、过渡区和边缘区三个区间.依据人的视觉特性,对平滑区改变较敏感,而对边缘区改变不敏感,确定在不同区间中的像素嵌入不同的信息量,如表 1 所示嵌入方案.

表 1 本文算法的信息嵌入方案(k bpp)

方案	平滑区[0,15]	过渡区[16,31]	边缘区[32,255]
1	1	2	3,4,5
2	2	3	4,5
3	3	4	4,5
4	4	4	5

根据像素差和表 1 嵌入方案,取相应的 k 位二进制信息,将其用十进制数 s 表示,然后根据下文的嵌入算法将 s 嵌入到目标像素中.

实际应用中,可以根据信息量、载密图像视觉质量要求,选择或设置不同的嵌入量方案.

3.2 嵌入算法

在现有基于模函数的信息隐藏算法基础上,应用模运算的周期特性特点,以及考虑算法的安全性而提出新的嵌入算法,嵌入信息函数为

$$f = (\alpha_{i,j} + p_{i,j} + x) \bmod 2^k \quad (3)$$

式中, k 为正整数, $\alpha_{i,j}$ 为随目标像素 $p_{i,j}$ 变化的安全系数, $\alpha_{i,j} \in [0, 2^k - 1]$, 由式(4)计算所确定, 式中 $rand_{i,j}$ 为随机整数; x 为使 $p_{i,j}$ 变化最小的 2^k 个整数, 取值范围为式(5)或式(6)所确定.

$$\alpha_{i,j} = rand_{i,j} \bmod 2^k \quad (4)$$

$$-2^{k-1} + 1 \leq x \leq 2^{k-1} \quad (5)$$

$$-2^{k-1} \leq x \leq 2^{k-1} - 1 \quad (6)$$

根据模函数运算特性, 满足式(5)或式(6)的 x , 一定使式(3)满足

$$\{f | f = (\alpha_{i,j} + p_{i,j} + x) \bmod 2^k\} = \{0, 1, 2, \dots, 2^k - 1\} \quad (7)$$

也就是说, 对于用十进制信息 s 表示 k 位二进制数, 在式(5)或式(6)所表示的 x 范围内完全可以确定一个唯一的 x 值, 使 $f = s$. 这时, s 的载密像素 $p'_{i,j}$ 为

$$p'_{i,j} = p_{i,j} + x \quad (8)$$

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

$$\begin{cases} p'_{i,j} = p'_{i,j} + 2^k, & p'_{i,j} < 0 \\ p'_{i,j} = p'_{i,j} - 2^k, & p'_{i,j} > 255 \end{cases} \quad (9)$$

例如, 当 $k = 2$, $p_{i,j} = 51$, $\alpha_{i,j} = 3$, 二进制信息 $d_1 = (11)_2$ 时, 嵌入过程为

$$\text{Step 1 } f = (3 + 51 - 1) \bmod 4 = 1$$

$$\text{Step 2 } f = (3 + 51 - 0) \bmod 4 = 2$$

$$\text{Step 3 } f = (3 + 51 + 1) \bmod 4 = 3 = d_1$$

$$\text{Step 4 } x = 1, p'_{i,j} = p_{i,j} + x = 52$$

又例如, 当 $k = 3$, $p_{u,v} = 0$, $\alpha_{u,v} = 6$, 二进制信息 $d_2 = (100)_2$ 时, 嵌入过程为

$$\text{Step 1 } f = (6 + 0 - 3) \bmod 8 = 3$$

$$\text{Step 2 } f = (6 + 0 - 2) \bmod 8 = 4 = d_2$$

$$\text{Step 3 } x = -2, p'_{u,v} = p_{u,v} + x = -2 < 0$$

$$\text{Step 4 } p'_{u,v} = p'_{u,v} + 8 = -2 + 8 = 6$$

3.3 提取算法

从一个载密像素中提取十进制信息的函数为

$$f = (\alpha_{i,j} + p'_{i,j}) \bmod 2^k \quad (10)$$

例如, 在上面嵌入算法中的嵌入例子, 从载密像素 $p'_{i,j}$ 中提取的信息为 $d_1 = (3 + 52) \bmod 4 = 3 = (11)_2$; 从载密像素 $p'_{u,v}$ 中提取的信息为 $d_2 = (6 + 6) \bmod 8 = 4 = (100)_2$.

4 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 (Peak Signal to Noise Ratio, PSNR), 其计算公式为

$$\text{PSNR} = 10 \times \log_{10}(255^2 / \text{MSE}) \quad (11)$$

其中, MSE 是原图像与载密图像之间的均方差, 计算公

式为

$$\text{MSE} = \frac{1}{m \times n} \sum_{i=1}^m \sum_{j=1}^n [I(i,j) - I'(i,j)]^2 \quad (12)$$

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 $\text{PSNR} > 30\text{dB}$, 理想的图像视觉质量要求 $\text{PSNR} > 39\text{dB}$.

理想的算法是有较高的嵌入率的同时有较好的图像质量.

已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. 本次实验采用 Matlab2008b 平台, 实验图像选用大小都是 512×512 的 Lena, Airplane, Peppers 和 Baboon 的标准灰度图像, 如图 2 所示; 秘密信息是由 Lorenz 混沌序列处理得到的随机二进制信息, 式(4)中的随机整数 $rand_{i,j}$ 也由 Lorenz 混沌序列处理得到. 二进制随机信息嵌满载体图像的所有像素; 从载密图像提取的二进制随机信息与嵌入时的二进制随机信息完全一致.

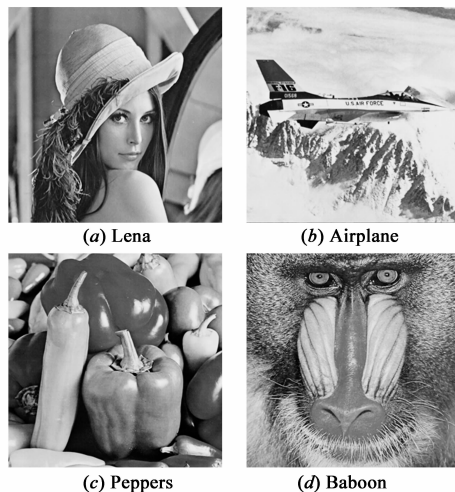


图2 原图像

4.1 嵌入率和不可感知性

4.1.1 本文算法

对于不同的载密图像的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.

由于表 2 的 PSNR 值不能反映载密图像平滑区的视觉质量, 也就不能从量上去理解载密图像的不可感知性. 为此测试平滑区的视觉质量, 方法是: 不分区, 直接用嵌入算法对每一像素进行等嵌入率下的 PSNR 值测试. 实验项目和数据如表 3 所示. 表 3 中 PSNR 值就是表 2 中对应嵌入率的平滑区 PSNR 值, 即平滑区的视觉质量.

当嵌入方案 Payload = (3, 4, 5) bpp 时, 平滑区 PSNR

大于理想值 39dB,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.

接近 35dB,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.

当嵌入方案 Payload = (4,4,5)bpp 时,平滑区 PSNR

表 2 不同嵌入方案下的嵌入量和图像质量

载体图像	嵌入方案(1,2,3)		嵌入方案(2,3,4)		嵌入方案(3,4,5)		嵌入方案(4,4,5)	
	嵌入量/bit	PSNR/dB	嵌入量/bit	PSNR/dB	嵌入量/bit	PSNR/dB	嵌入量/bit	PSNR/dB
Lena	310057	48.988	572521	43.613	840545	37.546	1058818	34.163
Airplane	320447	48.393	582829	42.945	849647	36.909	1065445	33.894
Peppers	307900	49.092	570954	43.739	840889	37.613	1057549	34.222
Baboon	499538	44.339	763244	38.505	1036653	32.347	1136801	31.677

表 3 载体图像等嵌入率下的图像质量

嵌入率 (bpp)	峰值信噪比 PSNR(dB)			
	Lena	Airplane	Peppers	Baboon
1	51.130	51.130	51.136	51.148
2	46.376	46.363	46.373	46.363
3	40.719	40.726	40.723	40.721
4	34.791	34.796	34.806	34.808

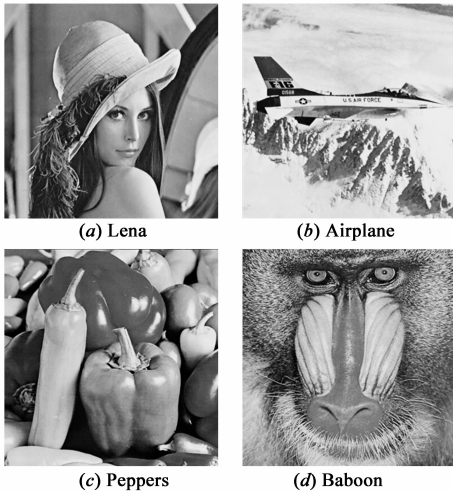


图3 载密图像 Payload=(3,4,5)bpp

4.1.2 图像像素分区的计算与载密图像质量

本次实验是为了实证不同算法的平滑区、过渡区和边缘区的像素计算的科学性.首先计算文献[11]算法分区法、文献[9]的四相邻像素差值计算方法下的本文分区法(简称四相邻像素法)和本文算法的三相邻像素差值计算分区法(简称三相邻像素法)下的像素分布情况,为说明问题仅以平滑区与边缘区分布情况具有普遍性的 Lena 图像为例,实验数据如表 4 所示.

表 4 Lena 图像的像素区域分布情况

分区算法	平滑区	过渡区	边缘区
文献[11]	246056	11880	2674
四相邻像素	188591	44465	27554
三相邻像素	218151	29519	12940

表 4 数据表明,文献[11]算法所划分的过渡区、边缘区像素过少,致使信息嵌入量少;四相邻像素算法所

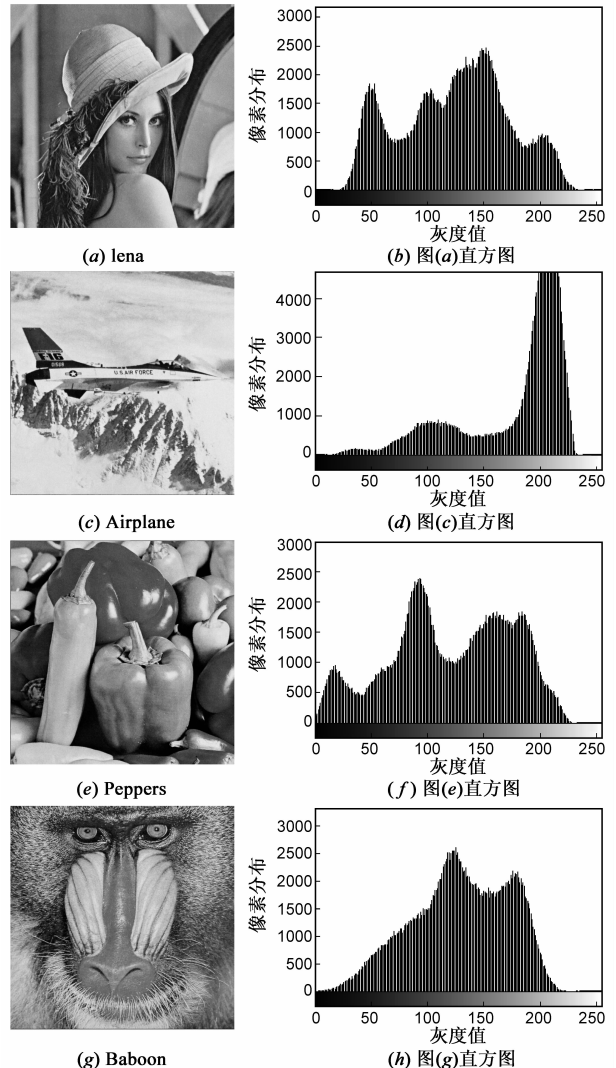


图4 载密图像及直方图 Payload=(4,4,5)bpp

确定的平滑区像素过少,占像素总数的 72.3%,临界像素被不合理地划分到过渡区或边缘区,这将会导致在过渡区和边缘区嵌入率高时因图像失真而容易被侦测;三相邻像素算法所确定的三个区域的像素分布比较合理,其像素差计算接近原 SM,平滑区像素值范围与文献[17]等众多基于 PVD 算法的一致,其平滑区像素

占 83.7% .

为实证上面对四相邻像素算法和三相邻像素算法的科学分析,测试 Lena 图像在嵌入方案(3,4,5)下两种算法的载密图像质量比较,实验结果如图 5 所示(载密图像放大至 2 倍后的截图).很明显,四相邻像素算法下的 Lena 鼻梁和脸部边缘失真比三相邻像素算法的要严重得多.



图 5 不同像素区域计算方法下的载密图像质量比较

4.1.3 与文献[11]算法比较

(1) 像素值最大修改量

设一个像素嵌入 k 位二进制信息,则 LSBs 的像素值最大修改量为 $2^k - 1$,而本文算法的像素值最大修改量为 2^{k-1} .显然,当 $n=1$ 时,两者的像素值最大修改量均为 1,当 $k \geq 2$ 时, $2^k - 1 > 2^{k-1}$,即 LSBs 的像素值最大修改量大于本文算法的像素值最大修改量,随着嵌入率的增大,差距增幅变化越大,当 $k=4$ 时,LSBs 最大修改量为 15,而本文算法仅为 8,如图 6 实验曲线.这就是 LSBs 当嵌入率达到 4 时,载密图像严重失真的原因.

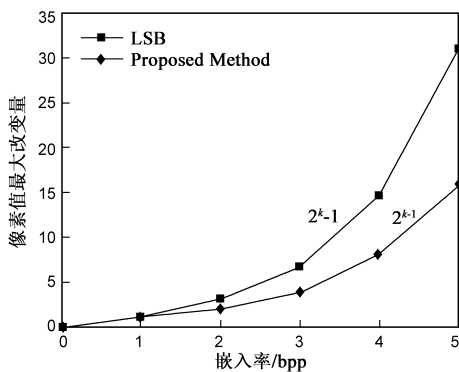


图 6 像素值最大改变量比较曲线

(2) 嵌入量和不可感知性比较

文献[11]对 LSBs 嵌入后的像素值进行了优化调整 (Optimal Pixel Adjustment Process, OPAP),使像素值最大修改量也为 2^{k-1} ,使平滑区的 PSNR 值仅略低于本文算法,但由于其像素区域计算不合理,致使载密图像的“嵌入量—视觉质量”性能不够理想.其信息嵌入量和图像视觉质量的实验数据如表 5 所示,限于篇幅,表中仅列出部分嵌入方案下的实验数据.

表 5 文献[11]算法的嵌入量和图像质量

载体图像	嵌入方案(1,2,3)		嵌入方案(3,4,5)	
	嵌入量/bit	PSNR/dB	嵌入量/bit	PSNR/dB
Lena	278523	50.126	800639	38.438
Airplane	284411	49.699	805766	37.941
Peppers	278988	50.068	801741	38.336
Baboon	379042	46.262	902943	33.036

表 2 与表 5 的对应实验数据表明,本文算法与文献[11]算法相比,信息嵌入量大幅度提高,而 PSNR 却下降得很少.如在嵌入方案(1,2,3)下, Lena 嵌入量提高 11.32%, PSNR 值仅降低 2.27%; Airplane 嵌入量提高 12.67%, PSNR 值仅降低 2.63%; Peppers 嵌入量提高 10.36%, PSNR 值仅降低 1.95% Baboon 嵌入量提高 31.79%, PSNR 值仅降低 4.16%.而这些 PSNR 值的降低是发生在边缘区,人的视觉对其不敏感,不影响载密图像的不可感知安全性.

综合分析和实验结果表明,本文算法的“嵌入量—视觉质量”性能远优于文献[11]算法.此外,文献[11]算法在目标像素嵌入信息后要保证差值范围不变而需要大量的计算量,OPAP 调整像素值也消耗大量的计算时间,故其总消耗时间远大于本文算法.

4.2 安全性

4.2.1 密钥空间分析

算法的安全性由控制安全系数 $\alpha_{i,j}$ 的密钥空间决定.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} .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 3.17×10^{34} 年.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,仅以等嵌入率为 k 为例,则计算次数为

$$\begin{aligned}
 NC &= 2^{mn} + 2^{2mn} + \dots + 2^{kmn} \\
 &= 2^{mn} (2^{kmn} - 1) / (2^{mn} - 1)
 \end{aligned} \quad (13)$$

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.

4.2.2 像素差值直方图分析

由图 4 的载密图像的像素直方图表明,本文算法抗直方图分析.鉴于文献[8]对 SM 像素对差值直方图异常分析结果,本实验检测本算法的相邻像素的最大值与最小值的差值直方图,图 7 为 Baboon 相邻像素值差值直方图,不仅没有任何异常,而且与原图像的极为一致.其他实验图像也是同样的实验结论.

4.2.3 不可侦测性

RS (Regular Singular) 检测方法是由著名隐写分析专家 Jessica Fridrich 等人于 2001 年提出的一种隐写分析

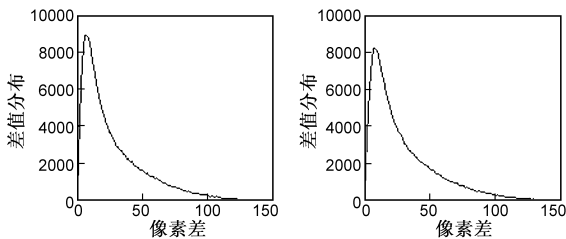


图7 (3,4,5)bpp方案Baboon相邻像素值差值直方图

算法^[18],具有较高的可靠性和灵敏度.对于一般未嵌信息的自然图像中, $R_m \approx R_{-m}$, $S_m \approx S_{-m}$; RS 嵌入率估计量约小于 5%, 即 RS 方法检测的精确度为 5%^[19].应用本文算法(3,4,5),以 10% 的像素载密率为增量依次嵌入不同的信息量到载体图像中,以此用 RS 分析方法进行检测分析.其中,载密 Lena 的 RS 曲线图如图 8 所示,RS 相关检测数据如表 6 所示.由图 8 的 RS 曲线和表 6 中的实验数据显示, $R_m \approx R_{-m}$, $S_m \approx S_{-m}$; 嵌入率估计 < 0.05 , RS 分析估计不出是否有信息嵌入.其他的实验图像的 RS 分析也是同样实验结果.由此表明,本文算法完全可以抵御 RS 隐写分析.

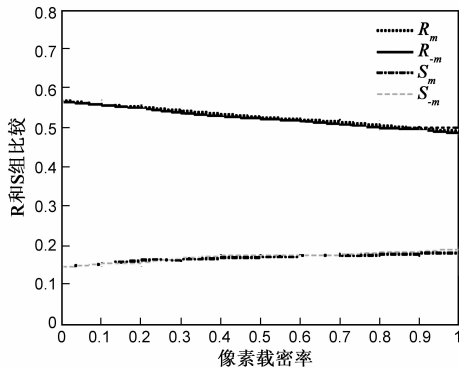


图8 (3,4,5)bpp方案lena RS曲线图

表 6 RS 检测在不同载密率下的相关检测数据(3,4,5)

像素载密率	$ R_m - R_{-m} $	$ S_m - S_{-m} $	RS 估算值
0	0.0015	0.0002	-0.016151
0.1	0.0017	0.0005	0.009552
0.2	0.0020	0.0042	0.016559
0.3	0.0049	0.0046	0.010669
0.4	0.0059	0.0071	0.010052
0.5	0.0046	0.0034	0.017373
0.6	0.0029	0.0002	0.017960
0.7	0.0056	0.0012	0.017395
0.8	0.0083	0.0044	0.021141
0.9	0.0049	0.0083	0.017877
1.0	0.0085	0.0103	0.016352

5 结束语

理论分析与实验结果表明,本文算法与基于 SM 密写算法及众多的信息隐藏算法相比,具有主要的如下三个重要特点:

- (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,且嵌入率可以调整;
- (2)引入随机安全系数,增强了算法的安全性;
- (3)不仅隐蔽性好,而且抗图像直方图、像素差值直方图统计分析,抗 RS 隐写分析.

用户可以根据实际应用要求选择或设置嵌入率,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

- [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]. IEE Proceedings Vision, Image & Signal Processing, 2005, 152(5): 611 - 615.
- [3] 刘劲,康志伟,何怡刚.一种基于小波对比度和 LSB 的密写[J].电子学报,2007,35(7):1391 - 1393.
LIU Jing, KANG Zhi-wei, HE Yi-gang. A steganographic method based on wavelet contrast and LSB [J]. Acta Electronica Sinica, 2007, 35(7): 1391 - 1393. (in Chinese)
- [4] Zhang X P, Wang S Z. Efficient steganographic embedding by exploiting modification direction [J]. IEEE Communications Letters, 2006, 10(11): 781 - 783.
- [5] 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.
- [6] 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.
- [7] Chang C C, Tseng H W. A steganographic method for digital images using side match [J]. Pattern Recognition Letters, 2004, 25(12): 1431 - 1437.
- [8] 王威娜,张新鹏,王朔中.针对边缘匹配嵌入法的密写分析以及嵌入率估计[A].第十二届全国图形图像学学术会议集[C].北京,2005.105 - 108.
Wang Wei-na, Zhang Xin-peng, Wang Shuo-zhong. Detection of hidden data embedded with side match steganography and estimation of payload [A]. Processing of the 15th National Conference on Image and Graphics [C]. Beijing, 2005. 105 - 108. (in Chinese)
- [9] Park Y R, Kang H H, Shin S U, et al. An Image steganographic using pixel characteristics [J]. Lecture notes in computer science, 2005, 3802: 581 - 588.
- [10] 张晓燕,张汗灵,刘劲.抗差值直方图分析的边缘匹配密写[J].计算机工程,2008,34(1):161 - 163.
Zhang Xiao-yan, Zhang Han-ling, Liu Jing. Side match

- steganography against pixel-value difference histogram analysis [J]. *Computer Engineering*, 2008, 34(1): 161 – 163. (in Chinese)
- [11] 彭程, 秦拯, 刘鹏, 等. 基于边缘匹配与最低有效位的图像隐写方法[J]. *计算机工程*, 2011, 37(14): 106 – 108.
Peng Cheng, Qin Zheng, Liu Peng, et al. Image steganography method based on side match and least significant bit [J]. *Computer Engineering*, 2011, 37(14): 106 – 108. (in Chinese)
- [12] 郭萌, 张鸿宾, 魏磊. 二值图像中的数据隐藏算法[J]. *电子学报*, 2009, 37(11): 2409 – 2415.
Guo Meng, ZHANG Hong-bin, WEI Lei. Data hiding in binary images [J]. *Acta Electronica Sinica*, 2009, 37(11): 2409 – 2415. (in Chinese)
- [13] Crandall R. Some notes on Steganography [EB/OL]. <http://www.dia.unisa.it/~ads/corso-security/www/CORSO-0203/steganografia/LINKS%20LOCALI/matrix-encoding.pdf>, 1998.
- [14] Westfeld A. F5-a steganographic algorithm: High capacity despite better steganalysis [J]. *Lecture notes in computer science*, 2001, 2137: 289 – 302.
- [15] 张新鹏, 王朔中. 基于稀疏表示的密写编码[J]. *电子学报*, 2007, 35(10): 1892 – 1896.
Zhang Xin-peng, Wang Shuo-zhong. Steganographic encoding based on sparse representation [J]. *Acta Electronica Sinica*, 2007, 35(10): 1892 – 1896. (in Chinese)
- [16] 林代茂, 郭云彪, 胡 岚, 等. 一种安全的信息隐藏范式及其在二值图像上的实现[J]. *电子学报*, 2005, 33(9): 1537 – 1540.
Lin Dai-mao, Guo Yun-biao, Hu Lan, et al. A secure paradigm of information hiding and the realization in binary images [J]. *Acta Electronica Sinica*, 2005, 33(9): 1537 – 1540. (in Chinese)
- [17] Yang C H, Weng C Y, Wang S J. Adaptive data hiding in edge areas of images with spatial LSB domain systems [J]. *IEEE Transactions on Information Forensics and Security*, 2008, 3(3): 488 – 497.
- [18] Fridrich J, Goljan M, Du R. Detecting LSB steganography in color and grayscale images [J]. *IEEE Multimedia*, 2001, 8(4): 22 – 28.
- [19] 李晓霞, 王建军. 一种抗 RS 攻击的隐写算法[J]. *系统工程与电子技术*, 2007, 29(8): 1358 – 1361.
Li Xiao-xia, Wang Jian-jun. Steganographic method robust to RS steganalysis [J]. *Systems Engineering and Electronics*, 2007, 29(8): 1358 – 1361. (in Chinese)

作者简介



廖琪男 男, 1964 年 4 月出生, 广西钟山人. 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