

结合 Hilbert 曲线扫描与游程长度的图像隐写算法

陈贞佐¹, 杨任尔^{1*}, 陈 计²

(1. 宁波大学 信息科学与工程学院, 浙江 宁波 315211; 2. 宁波大学 理学院, 浙江 宁波 315211)

摘要: 针对游程长度隐写算法存在嵌入容量小的问题, 提出基于 Hilbert 曲线扫描改进的游程长度隐写算法, 该算法能增加可用于嵌入秘密信息的游程数量, 也因此有效地增大了嵌入容量. 新算法利用比特流中游程长度的奇偶特性来嵌入秘密信息. 嵌入过程首先使用 Hilbert 扫描曲线对载体图像的像素进行置乱, 再将置乱的载体图像分解为 8 个位平面, 然后通过分析置乱后得到的各个位平面比特流分布来确定可用于嵌入信息的游程, 最后修改在可嵌入游程的比特流中 0 和 1 交界处至多 1 个值来嵌入 1 bit 秘密信息. 结果表明, 基于 Hilbert 曲线扫描的游程长度隐写算法与已有基于游程长度隐写算法相比, 前者具有较大嵌入容量, 较好的视觉不可感知性.

关键词: 图像隐写术; Hilbert 曲线扫描; 游程长度; 隐写系统性能

中图分类号: TP391

文献标志码: A

文章编号: 1001-5132 (2018) 01-0041-05

数字图像隐写术算法一般可分为基于空间域和频域两大类^[1-3]. 其中空间域算法优势在于其嵌入算法与提取算法复杂度较低, 嵌入容量比较大, 但鲁棒性与抗统计检测性都比较低; 而不少频域隐写算法采用了与空间域算法类似的方案, 在频域量化后的系数上实施 LSB 算法, 嵌入容量远远小于空间域的算法, 但同样存在鲁棒性与抗统计性不高问题^[4-6]. 而基于游程长度的隐写算法(Run-Length Steganography, RLSteg)不同于空间域和频域隐写的算法, 它利用人眼对空间频率变化不敏感特点, 不再显式地对像素值以替换或者插入方式进行秘密信息的嵌入, 而是以对二值图像像素值变化位置和从此开始的持续像素值的个数即游程(Run-Length)编码微调方式对信息进行嵌入^[7]. 本文提出一种基于 Hilbert 曲线扫描的位平面游程长度的隐写算法 (Steganography based on Hilbert Curve and Bitplane Run-length, HCRLSteg), 通过对图像进行 Hilbert 曲线扫描, 改变了位平面比特流分布特性, 有效地提高可嵌入秘密信息的游程对, 因此提出的新算法可以在算法复杂度增加不大的情况下, 相较于原有 RLSteg 隐写算法, 不但能有

效提高增加嵌入容量, 还达到了较好的视觉不可感知性.

1 结合 Hilbert 曲线扫描和游程长度隐写算法

RLSteg 算法基本思想是将灰度图像或者彩色图像按位平面分为多个二值图像^[8], 最多改变二值图像的黑白交界处的 1 个像素值, 利用较长段游程的长度奇偶性来表示需要嵌入的信息 0 或者 1. 由于嵌入信息不局限于 LSB 最低位平面, 嵌入容量得到提高, 而且该隐写算法可实现盲提取, 信息嵌入时也不会造成最低平面的异常, 能有效地抵御各种针对 LSB 及其改进方法的隐写分析算法, 不会造成游程特征的异常, 因此能抵御基于游程隐写分析, 具有良好的安全性.

Hilbert 扫描曲线是由德国数学家 Hilbert 提出的一种可以不间断遍历 1 个正方形中所有点, 并能够充满整个空间的曲线^[8-9]. 该扫描曲线是一种有规分型结构, 符合分型结构中自相似原则和迭代生成原则, 其 N 级结构是由 $N-1$ 级结构以某种规则重复组成. Gostman 和 Lindenbaum 曾证明 Hilbert 曲线是所有曲线中具有保持空间局部连接性最完

收稿日期: 2017-05-03.

宁波大学学报(理工版)网址: <http://journalg.nbu.edu.cn/>

基金项目: 国家自然科学基金 (61672302); 宁波市自然科学基金 (2015A610140); 浙江省信息与通信工程重中之重学科开放基金 (XKXL1524).

第一作者: 陈贞佐 (1992-), 女, 浙江宁波人, 在读硕士研究生, 主要研究方向: 数字图像隐写. E-mail: suke_zuo@qq.com

*通信作者: 杨任尔 (1968-), 女, 浙江宁波人, 副教授, 主要研究方向: 数字图像隐写. E-mail: yangrener@nbu.edu.cn

整的曲线. 张湛等采用 n -MC 模型研究以行列、zig-zag 和 Hilbert 曲线扫描方式扫描同幅图, 表明使用 Hilbert 曲线扫描得到一维比特流 S 所表示图像相关度特性保持最优. 利用 Hilbert 曲线对二维矩阵进行扫描, 是一种二维空间到一维空间的映射方法, 利用这种方式扫描连续色调图像(照片及绘画等), 由于它能尽可能地保持原有空间中相邻点的相关性, 因此目前已被广泛应用于图像扫描和图像压缩领域, 但其在图像隐写方面的应用研究涉及较少.

本文提出一种基于 Hilbert 曲线扫描和游程长度的隐写算法, 使用 Hilbert 曲线扫描生成 Hilbert 扫描矩阵, 对图像进行像素扫描, 使二维图像映射成一维的比特流. 与图像常规行列或者之字形扫描相比, Hilbert 曲线扫描得到不同的比特流随机特性, 因此提高了比特流的游程长度, 特别是增加了可嵌入有效游程长度的数量.

HCRLSteg 隐写算法流程框图如图 1 所示. 隐写算法首先选择一幅载体图像, 对其使用 Hilbert 曲线进行扫描, 形成 Hilbert 曲线扫描图像, 然后将扫描图像分解成 8 个位平面, 接着使用 RL 隐写算法将秘密信息比特按顺序嵌入到各个位平面的比特流中, 嵌入结束后, 把各个位平面组合成一个含密的 Hilbert 曲线扫描图像, 最后对含密图像通过 Hilbert 曲线逆扫描产生最终的隐写图像.

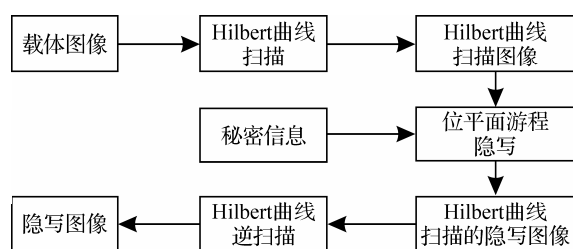


图 1 基于 Hilbert 扫描曲线和位平面游程隐写算法的框图

2 Hilbert 曲线扫描与逆扫描过程

高阶 Hilbert 曲线是通过对一个 2×2 阶结构自相似重复迭代形成, 图 2 表示了 2×2 阶 Hilbert 曲线通过规律变化迭代成为高阶曲线的过程. 若将图 2(a)记为 K , 那么图 2(b)是由 K 顺时针旋转 90° 后与原图拼接, 然后再做轴对称变换得到. 同理, 图 2(c)是由图 2(b)做相同变换得到. 对于 $4N$ 阶结构而言, 均可由 N 阶结构作同样的变换得到. 因此可根据

曲线迭代规则, 任意画出 $2^N \times 2^N$ 阶的 Hilbert 曲线.

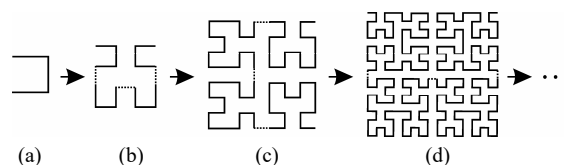


图 2 N 阶 Hilbert 扫描曲线生成过程

根据 Hilbert 曲线遍历平面所有点的过程得到 Hilbert 扫描矩阵, 以 4×4 矩阵为例得出扫描矩阵, 图 3(a)为 Hilbert 曲线扫描图像过程, 图 3(b)为图像扫描所得的一维数据流. Hilbert 扫描矩阵中, 第 i 行第 j 列上的数值 k 为二维空间对应到一维空间的位置. 对载体图像 $C(i, j)$ 进行 Hilbert 扫描得到一维 S ,

$$\begin{aligned} M(i, j) &= S(k), i \text{ 为奇数,} \\ M(i, n-j+1) &= S(k), i \text{ 为偶数,} \end{aligned} \quad (1)$$

其中, $k = (i-1) \times 512 + j$.

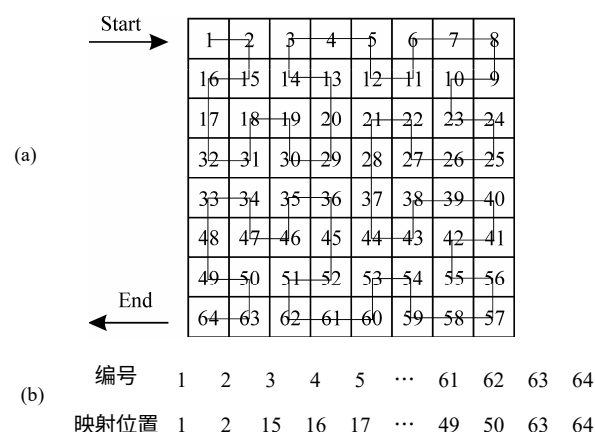


图 3 Hilbert 扫描曲线生成映射位置

本文通过上述方法生成 512×512 的 Hilbert 扫描矩阵, 并对实验图像进行 Hilbert 扫描, 得到一维的数据流, 再进行信息的嵌入. 对于嵌入之后的数据流, 利用以下公式:

$$\begin{aligned} M(i, j) &= S(k), i \text{ 为奇数,} \\ M(i, n-j+1) &= S(k), i \text{ 为偶数,} \end{aligned} \quad (2)$$

最后形成隐写图像.

3 HCRLSteg 隐写算法实现过程

步骤 1 图像预处理. 首先对载体图像进行 Hilbert 曲线扫描, 形成置乱图像, 然后再对置乱图像进行位平面分解, 得到多个二值图像, 并用行列扫描成一维 0-1 比特流 S .

步骤 2 像素扫描. 将 S 的第 1 个值记为 s , 此处不失一般性假设, $s=1$. 对 S 进行游程扫描, 扫描方式如图 4 所示. 从第 1 个像素开始, 扫描相邻一段 1 和一段 0, 编码为 (n_i, m_i) , n_i 为 1 的长度, m_i 为 0 的长度, i 为扫描的段数.

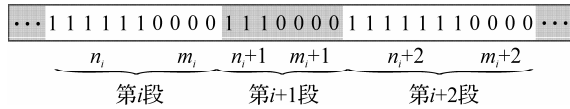


图 4 游程编码示意图

步骤 3 比较 n_i 和 m_i 大小, 并用 $M_{\text{mark},i}$ 记录较长一段的像素值.

$$\begin{aligned} n_i \geq m_i, M_{\text{mark},i} &= 1(s), \\ n_i < m_i, M_{\text{mark},i} &= 0(1-s). \end{aligned} \quad (3)$$

步骤 4 判断当前段的游程是否可以嵌入信息. 将嵌入平面阈值设定为 t , 用于控制秘密信息嵌入率. 对于第 i 对游程, 如果 n_i 与 m_i 中较小的值大于阈值 t , 则该段游程中可以嵌入秘密信息, 接着转入下一步, 否则断定该对游程不可用, 则需对第 $i+1$ 段游程进行判断, 直至该平面游程全部判断完毕, 然后转至步骤 6.

步骤 5 秘密信息嵌入. 对已经判断为可嵌入信息的第 i 对游程嵌入秘密信息. 当长游程长度奇偶性与秘密信息奇偶性一致时, 无需对游程进行调整, 嵌入完成; 当秘密信息与长游程奇偶性不一致时, 对该段游程 0-1 交界处进行 1 bit 的信息修改, 修改原则是使较长游程的奇偶性与嵌入信息一致. 具体嵌入方案见表 1 和表 2, 表格内容为对游程对 (n_i, m_i) 修改后的值. 完成第 i 对游程的嵌入(或者无效修改)后, 转入步骤 4.

步骤 6 把秘密信息全部嵌入完毕后, 再将新的游程编码信息 (n_i, m_i) 复原成一维比特流, 并对含密图像进行 Hilbert 逆变换, 得到隐写图像.

4 秘密信息提取算法

步骤 1 图像预处理. 将灰度图像(或者彩色图像)进行位平面分解, 得到多个二值图像, 对二值图像进行 Hilbert 扫描, 获得一维 1-0 像素流 S' .

步骤 2 像素扫描. 进行游程扫描, 扫描方式如下: 从第 1 个像素开始, 扫描相邻一段 1-0 段, 编码为 (n_i, m_i) .

步骤 3 秘密信息的提取. 当长游程的长度大

表 1 对于 $M_{\text{mark},i}=1$ 时的情况

游程对情况	长游程奇偶性	待嵌入秘密信息	
		0	1
$m_i > n+1$	奇	(n_i+1, m_i-1)	(n_i, m_i)
	偶	(n_i, m_i)	(n_i+1, m_i-1)
$m_i = n+1$	奇	(n_i+1, m_i-1)	(n_i, m_i)
	偶	(n_i, m_i)	(n_i+1, m_i-1)
$n_i > n+2$	奇	无法嵌入, 进行无效化修改	
	偶	(n_i, m_i)	(n_i+1, m_i-1)
$m_i = n+1$	奇	(n_i+1, m_i-1)	(n_i, m_i)
	偶	(n_i, m_i)	(n_i+1, m_i-1)
$n_i = n+2$	奇	无法嵌入, 进行无效化修改	
	偶	(n_i, m_i)	(n_i+1, m_i-1)

表 2 对于 $M_{\text{mark},i}=0$ 时的情况

游程对情况	长游程奇偶性	待嵌入秘密信息	
		0	1
$m_i > n+1$	奇	(n_i, m_i)	(n_i+1, m_i-1)
	偶	(n_i+1, m_i-1)	(n_i, m_i)
$m_i = n+1$	奇	(n_i, m_i)	(n_i+1, m_i-1)
	偶	(n_i+1, m_i-1)	(n_i, m_i)
$n_i > n+2$	奇	(n_i, m_i)	无法嵌入, 进行无效化修改
	偶	(n_i+1, m_i-1)	(n_i, m_i)
$m_i = n+1$	奇	(n_i, m_i)	(n_i+1, m_i-1)
	偶	无法嵌入, 进行无效化修改	(n_i, m_i)
$n_i = n+2$	奇	(n_i, m_i)	(n_i+1, m_i-1)
	偶	(n_i+1, m_i-1)	(n_i, m_i)

于阈值 n 时, 则说明该游程段中嵌入了 1 bit 的信息量, 长游程的奇偶性为所嵌入的信息, 如果长短游程长度相同, 则选择前一段:

$$w(j) = \max(n_i, m_i) \bmod 2. \quad (4)$$

5 实验结果及分析

为检验 Hilbert 曲线图像置乱效果, 对 Lena 灰度图像(图 5(a))进行 Hilbert 曲线图像置乱. 将 Lena 图像用 Hilbert 扫描矩阵置乱后得到一维数据流, 其置乱后图像如图 5(b)所示. 从图 5(b)中可见, 像素灰度值变化连续性很强. 图 5(c)为原图像一维比特流的灰度值曲线, 表示原 Lena 图像横向扫描所得到的灰度值变化情况, 其值的变化是根据原有图像特性以 512(图像宽度值)为周期的一个变化曲

线. 因此在阈值较大时, 在一定长度内, 数值变化大, 可用的有效游程数量就少. 图 5(d)为 Hilbert 一维比特流的灰度值曲线, 由图可知, 其数值上连续性较图 5(c)更好, 可得到位平面上连续游程的平均长度更长. 因此在 RLSteg 隐写中, 对于 Hilbert 曲

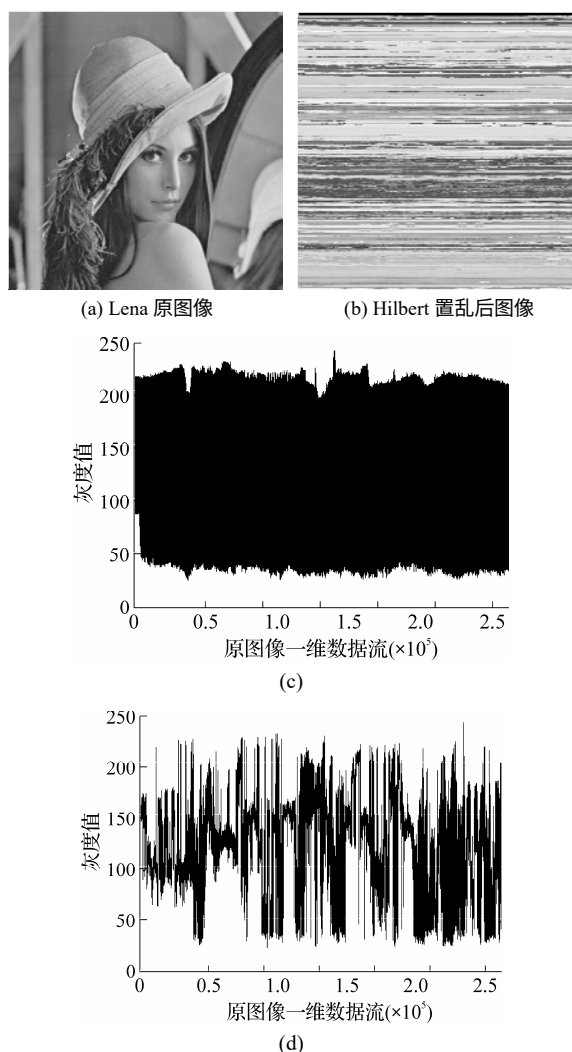


图 5 原始图像及其 Hilbert 扫描置乱图像

线置乱后的可用的位平面上有效游程数多.

本文实验采用图 6 中大小为 512×512 的 6 幅灰度图像作为载体图像, 嵌入的秘密信息是由伪随机数发生器生成的随机比特流, 并用峰值信噪比(PSNR)来评价隐写图像的视觉不可感知性. 其中 RLSteg 隐写算法由低到高的 8 个位平面阈值分别为 2, 2, 2, 2, 10, 15, 30, 45.



图 6 测试图像

表 3 是本文提出的 HCRLSteg 隐写算法与文献 [6] 中 RL 隐写算法性能比较结果. 实验结果表明, 与 RL 隐写算法相比较, HCRLSteg 隐写算法不但嵌入容量有不同程度提高, 隐写图像的信噪比也有较大程度提高, 嵌入容量最大提升率达到 11.4%, 信噪比最大提升率达到 15.7%.

6 结论

为了提高 RLSteg 隐写算法的嵌入容量, 本文使用 Hilbert 曲线扫描图像置乱技术, 新隐写系统既具有较高嵌入容量, 又达到较好视觉不可感知性. 因此下一步研究方向是尝试将 Fibonacci 变换、Arnold 变换、幻方变换(Magic square transformation)

表 3 RL 隐写算法与 HCRLSteg 隐写算法性能比较

测试图像	嵌入容量/bit			PSNR/dB		
	RLSteg	HCRLSteg	容量提升	RLSteg	HCRLSteg	PSNR 提升
1	9 686	10 795	1 109	43.80	50.68	6.88
2	10 765	11 481	716	46.78	50.75	4.36
3	10 230	10 809	579	46.06	50.23	4.17
4	10 004	10 380	376	43.47	50.67	6.88
5	10 850	11 246	396	46.75	50.72	3.97
6	10 653	11 156	503	47.65	50.69	3.04

等图像置乱技术与 RLSteg 隐写算法结合起来的隐写系统以及具体性能. 本文在实现 RLSteg 隐写算法时, 只对各个位平面指定的一组阈值进行研究, 进一步研究可以探索如何找到各个位平面最佳阈值组合, 进一步地达到更好性能的隐写系统.

参考文献:

- [1] Kareemjuma N. Hiding of random permuted encrypted text using LSB steganography with random pixels generator[J]. International Journal of Computer Applications, 2015, 113(13):20-27.
- [2] Mao Q. A fast algorithm for matrix embedding steganography[J]. Digital Signal Processing, 2014, 25:248-254.
- [3] 王超, 张卫明, 刘九芬. 基于比特控制的快速矩阵嵌入[J]. 电子与信息学报, 2011, 33(9):2169-2174.
- [4] 谢建全, 阳春华, 黄大足, 等. 一种大容量的DCT域信息隐藏算法[J]. 中国图像图形学报, 2009, 14(8):1542-1546.
- [5] Baby D, Thomas J, Augustine G, et al. A novel DWT based image securing method using steganography[J]. Procedia Computer Science, 2015, 46:612-618.
- [6] 陈涨胜, 杨任尔, 陈贞佐, 等. 基于视觉模型与菱形编码的图像隐写算法[J]. 宁波大学学报(理工版), 2017, 30(4):68-73.
- [7] 谢建全, 谢勃, 黄大足. 一种基于游程长度的高安全性图像信息隐藏算法[J]. 计算机科学, 2014, 41(3):172-176.
- [8] 戴跃伟, 刘光杰, 叶曙光. 基于 Hilbert 填充曲线的自适应隐写[J]. 电子学报, 2008, 36(1):35-38.
- [9] Yang X L, Tan Y. An arithmetic-analytical expression of the Hilbert-type space-filling curves and its applications [J]. Bulletin of the Malaysian Mathematical Society, 2015, 38(2):841-854.

A novel image steganography based on Hilbert curve scanning algorithm and run-length

CHEN Zhen-zuo¹, YANG Ren-er^{1*}, CHEN Ji²

(1.Faculty of Electrical Engineering and Computer Science, Ningbo University, Ningbo 315211, China;

2.Faculty of Science, Ningbo University, Ningbo 315211, China)

Abstract: The Run-Length steganography, referred to as RLSteg, has a problem with low embedding rate. To address this problem, based on Hilbert curve scanning algorithm, we put forward an improved RLSteg algorithm, which can increase the number of runs available for secret message embedding and thus effectively improve the embedding capacity. The presented algorithm uses the parity of run length in the bit stream to embed the secret message. The embedding process can be described as follows: the cover image is first decomposed into eight binary bitplanes, then Hilbert curve scanning algorithm is used to scramble the pixels of each bitplane. By analyzing each scrambled bitplane bit stream, the run available for secret message embedding is determined. At the edge of available run of bit stream 0, 1, at most one value is modified, hence 1 bit secret message is successfully embedded. Experimental results show that, compared with the classical RLSteg algorithm, the presented RLSteg algorithm has the advantages of larger embedding capacity and better visually imperceptible performance.

Key words: image steganography; Hilbert curve scanning; run-length; steganographic system performance

(责任编辑 章践立)