

针对 LSB 匹配隐写的评价策略与改进方法

方蒙蒙^{1,2}, 何加铭^{1,2*}, 金超³, 史智慧^{1,2}

(1. 宁波大学 通信技术研究所, 浙江 宁波 315211; 2. 浙江省移动网应用技术重点实验室, 浙江 宁波 315211;

3. 宁波大学 纵横智能软件研究所, 浙江 宁波 315211)

摘要: 以 Mielikainen 提出的 LSB 匹配算法为基础, 通过分析秘密信息对与载体像素对之间的不同匹配顺序对隐写算法性能的影响, 提出了一个三级得分评价策略. 根据此评价策略的指导, 采用粒子群优化算法找出最优的信息对嵌入顺序, 并在此基础上对 Mielikainen 的方法进行改进, 提出了一种新的隐写算法. 实验结果表明, 在嵌入相同大小秘密信息的条件下, 提出的算法减少了载体图像中灰度值发生变化的像素点数, 从而有效提高了隐秘图像的视觉感知质量.

关键词: 信息隐藏; LSB 匹配; 隐写; 评估; 粒子群优化算法

中图分类号: TN92

文献标志码: A

文章编号: 1001-5132 (2015) 03-0029-05

隐写术(Steganography)是信息隐藏技术的一个重要分支, 它是将特定的秘密信息隐藏在某种公开信息之中, 由于对外表现的是载体信号的内容和特征, 有公开信息作掩护, 因此第三方不会感觉到秘密信息的存在^[1]. 目前, 针对数字媒体提出的隐写算法中, 大多数是以图像为载体. 作为图像中一种重要的隐写方法, LSB 匹配虽然改善了 LSB 替换能轻易被传统隐写分析方法检测出来的弱点^[2-3], 但突出了其影响图像视觉感知质量的缺陷. 因此 Mielikainen 提出一种基于 LSB 匹配的改进算法^[4], 此方法减弱了隐写对图像视觉感知质量的不利影响, 同时进一步降低了 LSB 替换方法被检测的概率^[5-6].

笔者在对 Mielikainen 方法深入研究的基础上, 提出了一个三级得分评价策略, 此评价策略可以评价不同匹配顺序的 LSB 匹配算法的性能, 并可对秘密信息对与载体像素对之间的匹配情况进行打分, 得到一个得分矩阵; 并结合此得分矩阵, 将寻找秘密信息对的最佳嵌入顺序问题转化为一个高维优化问题. 在信息隐藏领域, 优化算法常被用来寻找最优解^[7-10]. 另外, Elbeltagi 等^[10]对遗传算

法(genetic)、蚁群算法(ant-colony)、Memetic 算法、蛙跳算法(Shuffled frog leaping)和粒子群算法(PSO)的性能进行了比较, 指出 PSO 算法在成功率及运行时间等方面要优于其他 4 种算法. 鉴于上述对优化算法的分析, 笔者使用粒子群优化算法寻找秘密信息对的最佳嵌入顺序, 并在此基础上提出了改进的 LSB 匹配隐写算法.

1 Mielikainen 的方法

文献[4]中, Mielikainen 提出一种配对 LSB 匹配算法, 其每次匹配的是成对的信息位与载体位. 假设矩阵 C 和 S 分别表示载体图像和秘密数据, 按从左往右、从上而下的方式将其转换为一串数据流, 记为 C' 和 S' , 可用下式表示:

$$\begin{aligned} C' &= [c_1, c_2, c_3, \dots, c_i, \dots, c_{n_c}], \\ S' &= [s_1, s_2, s_3, \dots, s_i, \dots, s_{n_s}], \end{aligned} \quad (1)$$

式中, n_c 为载体像素点数目; n_s 为秘密数据比特数.

假设任意两载体像素点分别表示为 c_i 和 c_{i+1} , 秘密信息对分别表示为 s_i 和 s_{i+1} , 隐秘图像像素点分别表示为 st_i 和 st_{i+1} .

收稿日期: 2014-05-26. 宁波大学学报(理工版)网址: <http://journalg.nbu.edu.cn/>

基金项目: 国家科技重大专项 (2011ZX03002-004-02); 浙江省重点科技创新团队项目 (2012R10009-19, 2012R10009-11); 浙江省移动网络应用技术重点实验室项目 (2010E10005).

第一作者: 方蒙蒙 (1988-), 女, 安徽安庆人, 在读硕士研究生, 主要研究方向: 信息隐藏算法及评价. E-mail: fmm1026@163.com

*通信作者: 何加铭 (1949-), 男, 浙江杭州人, 博导/教授, 主要研究方向: 移动互联网技术. E-mail: hejiaming@nbu.edu.cn

另外, 二进制函数定义如下:

$$f(c_i, c_{i+1}) = \text{LSB}\left(\left\lfloor \frac{c_i}{2} \right\rfloor + c_{i+1}\right). \quad (2)$$

相应方法原理如下: 将 s_i 与 c_i 的最低位进行比较, 若相等, 则载体像素值 c_i 保持, 即令 $st_i = c_i$; 否则, 载体像素值 c_{i+1} 保持, 即令 $st_{i+1} = c_{i+1}$. 若已令 $st_i = c_i$, 则将 s_{i+1} 与 (2) 式的 $f(c_i, c_{i+1})$ 比较, 若相等, 则 $st_{i+1} = c_{i+1}$; 否则, 载体像素值 c_{i+1} 随机加减 1 作为 st_{i+1} 的值. 若已经令 $st_{i+1} = c_{i+1}$, 则将 s_{i+1} 与 $f(c_i - 1, c_{i+1})$ 进行比较, 若相等, 则 $st_i = c_i - 1$; 否则, $st_i = c_i + 1$. 方法的具体流程如图 1 所示.

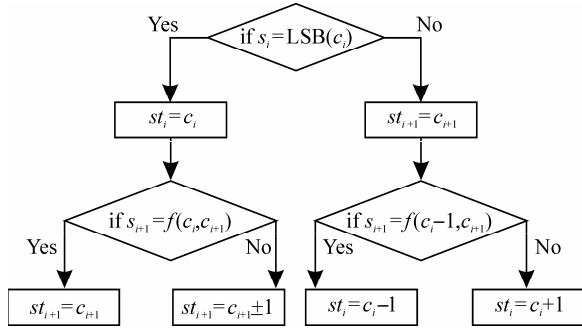


图 1 Mielikainen 方法流程

2 LSB 匹配隐写算法的评价与改进

2.1 三级得分评价策略

从图 1 中我们可以看出, 一种最佳的匹配状态便是 $s_i = \text{LSB}(c_i)$ 和 $s_{i+1} = f(c_i, c_{i+1})$, 此时的载体像素值没有发生任何改变, 隐秘图像质量最好. 次佳的匹配状态便是流程图中剩下的另外 3 种情况, 即 1 对载体像素点至少有 1 个载体像素值发生了改变, 此时隐秘图像便会产生失真. 为了减少这种失真, 应尽量减少次佳匹配状态的发生频率, 提高最佳匹配状态的发生频率. 笔者针对 $s_i \neq \text{LSB}(c_i)$ 这种情况, 采用了换序匹配的方式来间接达到最佳匹配.

于是, 在考虑尽可能达到秘密信息对与载体像素对之间的最佳匹配的条件下, 三级得分评价策略设计如下:

若 $s_i = \text{LSB}(c_i)$ 且 $s_{i+1} = f(c_i, c_{i+1})$, 则此次匹配得分 N_1 ; 若 $s_i = \text{LSB}(c_i)$ 且 $s_{i+1} \neq f(c_i, c_{i+1})$, 则记匹配得分为 N_2 . 若 $s_i \neq \text{LSB}(c_i)$, $s_{i+1} = \text{LSB}(c_i)$ 且 $s_i = f(c_i, c_{i+1})$, 则将两信息位交换顺序 $s_i \leftrightarrow s_{i+1}$, 重新按图 1 的流程来配对, 此时匹配得分为 $-N_1$; 否则,

若 $s_i \neq \text{LSB}(c_i)$ 且 $s_{i+1} \neq \text{LSB}(c_i)$ 或 $s_{i+1} \neq f(c_i, c_{i+1})$, 则仍按图 1 流程来配对, 此时匹配得分记为 N_2 .

为了区分不同匹配情况下隐写性能的好坏, 文中记 $N_1 > N_2$.

2.2 寻找最优信息对嵌入顺序

2.2.1 得分矩阵和得分函数

根据上述评价原则, 对每个秘密信息对与载体像素对进行匹配打分, 所有的分数可以构成一个得分矩阵, 本中定义的得分矩阵 SM 如下式:

$$SM_{L_s \times L_c} = \begin{cases} sm(i, j) | sm(i, j) \in \{N_1, N_2, -N_1\} \\ 1 \leq i \leq L_s, 1 \leq j \leq L_c \end{cases}, \quad (3)$$

式中, $L_s = n_s / 2$, 为信息比特对数目; $L_c = n_c / 2$, 为载体像素对数目.

得到得分矩阵 SM 后, 为了完成最佳匹配, 需要从不同的行和列中选取 L_s 个元素, 且每 1 行和列至多只选取 1 个元素. 为了描述不同的选择, 笔者定义 1 个调整向量 R :

$$R_{1 \times L_c} = \{r_1, r_2, r_3, \dots, r_i, \dots, r_{L_c}\}, \quad (4)$$

式中, r_i 表示第 i 列第 $|r_i|$ 行的元素. 当 $L_s < L_c$ 时, 即非满嵌情况下, 将有 $L_c - L_s$ 个像素点不携带秘密信息, 此时调整向量 R 中将有 $L_c - L_s$ 个元素置为 0. 若从矩阵 SM 选取的元素 $sm(i, j) < 0$, 此时则相应地调整向量中 $r_j = -i$; 否则, $r_j = i$. 调整向量中的负号是为了说明该信息对的比特位除了位置调整外, 还要彼此交换顺序.

根据以上描述可知, 调整向量 R 随着矩阵维数的增加有很多种组合, 那么不同组合都有 1 个得分. 文中定义归一化得分函数如下:

$$f(R) = \frac{1}{f_{s_max}} \sum_{r(i) \neq 0} |sm(|r_i|, i)|, \quad (5)$$

$$f_{s_max} = L_s \times N_1,$$

式中, $|\cdot|$ 表示绝对值, f_{s_max} 表示最大得分.

2.2.2 应用 PSO 寻找最优的调整向量 R

根据三级得分评价策略可知, 使 (5) 式的归一化得分最高的那组调整向量被认为是最优的调整向量 R , 也即最优的信息对嵌入顺序. 为了得到较优的调整向量 R , 笔者采用粒子群算法 (PSO) 来完成寻优.

在 PSO 算法中^[7], 假设搜索空间为 D 维, 每个粒子的位置就是问题的一种可能解. 第 i 个粒子位置记为 $X_i = (x_{i1}, x_{i2}, \dots, x_{iD})$, 其速度记为 $V_i = (v_{i1},$

$v_{i2}, \dots, v_{iD}$). 每个粒子的好坏都由 1 个适应度函数来评价. 在 D 维问题空间中搜索时, 每个粒子通过跟踪自己当前最优位置 $p_{best,i}$, 以及群体最优位置 g_{best} 来完成自身位置的更新. 粒子根据(6)~(8)式来完成自身位置与速度的更新:

$$V_i = w \times V_i + c_1 \times R_{rand,1} \times (p_{best,i} - X_i) + c_2 \times R_{rand,2} \times (g_{best} - X_i), \quad (6)$$

$$X_i = X_i + V_i, \quad (7)$$

$$w = w_{max} - n \cdot \frac{w_{max} - w_{min}}{i_{ter_max}}, \quad (8)$$

式中, V_i 为粒子速度; X_i 为粒子位置; w 为惯性权重, 随迭代次数的增加而线性递减, $w \in (w_{min}, w_{max})$; c_1 和 c_2 为加速度系数, 通常取为 2; $R_{rand,1}$ 和 $R_{rand,2}$ 是 $[0,1]$ 之间的随机数; n 为当前迭代次数; i_{ter_max} 为最大迭代次数. 另外, 粒子速度的每一维都被限制在 $[-v_{max}, v_{max}]$ 之间.

在文中的方案中, 1 个好的粒子就对应 1 个调整向量 R . 一般的粒子群优化问题都是在连续实数空间里, 而本文的优化问题是在离散整数空间, 即每个粒子的位置为 $\{1, 2, \dots, L_c\}$ 的不同组合. 并根据文献[7], 将每次得到的粒子位置 $X_i = (x_{i1}, x_{i2}, \dots, x_{iD})$ 从小到大映射到 $\{1, 2, \dots, L_c\}$, 即最小值映射为 1, 最大值映射为 L_c . 并采用(5)式作为适应度函数, 用以评价粒子优劣.

相关步骤如下:

步骤 1 初始化. 随机产生 K 个粒子 $X_i (i = 1, 2, \dots, K)$, 每个粒子获得 1 个随机的初始速度 V_i , 并计算每个粒子的适应度值 $f(X_i)$, 将拥有最大的适应度值的粒子位置赋给 g_{best} .

步骤 2 每个粒子根据(6)~(8)式来更新位置和速度.

步骤 3 计算粒子 X_i 的映射值及其适应度值 $f(X_i)$, 如果其大于粒子当前的最优适应度值, 则 $p_{best,i} = X_i$; 如果其也大于全局的最优适应度值, 则 $g_{best} = X_i$.

步骤 4 若达到最大迭代次数, 算法终止并输出结果; 反之, 继续执行步骤 2.

2.3 改进的隐写算法

根据上述三级得分评价策略的指导, 笔者在 Mielikainen 的 LSB 匹配算法基础上提出一种改进的隐写算法.

2.3.1 嵌入过程

步骤 1 读入载体图像和秘密信息.

步骤 2 根据三级得分评价策略计算得分矩阵 SM .

步骤 3 应用粒子群优化算法来求解最优的调整向量 R , 也就是寻找秘密信息对最佳的嵌入顺序.

步骤 4 根据步骤 3 中的调整向量 R 来调整秘密信息对的嵌入顺序, 得到新的秘密信息. 最后, 根据 Mielikainen 的方法进行嵌入, 并最终得到载密图像.

2.3.2 提取过程

在提取秘密信息前, 需先将编码秘密图像和调整向量的密钥等信息发送给接收方.

步骤 1 读入载密图像, 按从上往下、从左向右方式扫描得到行向量, 2 个连续像素点分为一组.

步骤 2 第 i 组载密像素对记为 st_i 和 st_{i+1} , 若调整向量 R 中 $r_i \neq 0$, 则计算可得 $s_i = \text{LSB}(st_i)$, $s_{i+1} = f(st_i, st_{i+1})$; 否则, 此组载密像素对未携带秘密信息. 提取完成后, 得到行向量记为 S .

步骤 3 当按步骤 2 提取了所有信息对, 我们将根据调整向量来调整秘密信息对顺序. 若调整向量 R 中元素的符号为负, 则其对应信息对除了位置调整外还要彼此交换顺序. 调整结束后, 即可得到信息行向量 S' .

3 实验结果及分析

为从视觉效果方面来评价笔者所提出的隐写算法的性能, 对提出的基于三级得分评价策略改进配对 LSB 匹配隐写算法(以下简称 PSO-LSBMR)进行仿真实验, 实验所用图像为 96×96 的标准灰度图像. 本中采用 Lena、Peppers、Barbara、Camera-man、Baboon、Woman 和 Boat 作为测试图像, 秘密信息为一段英文文本(图 2).

通过将 PSO-LSBMR 与其他的 LSB 匹配算法(如 Mielikainen's 和文献[10]的方法, 以下分别简称 LSBMR 和 GA-LSBMR)在不同嵌入率下的图像视觉质量进行比较, 来评价隐写算法隐写性能. 实验利用峰值信噪比 PSNR(Peak Signal-to-Noise Ratio)作为图像视觉质量的评价指标.

表 1 和表 2 分别为嵌入率为 100%和 50%的各



图2 测试图片及秘密信息

表1 嵌入率为 100%的视觉效果(PSNR)比较

载体图像	LSBMR ^[4] /dB	GA-LSBMR ^[10] /dB	PSO-LSBMR/dB
Lena	52.35	54.40	56.39
Peppers	52.41	54.40	56.38
Barbara	52.37	54.39	56.42
Cameraman	52.45	54.41	56.36
Baboon	52.38	54.47	56.45
Woman	52.35	54.36	56.34
Boat	52.40	54.43	56.43
Average	52.39	54.41	56.40

表2 嵌入率为 50%的视觉效果(PSNR)比较

载体图像	LSBMR ^[4] /dB	GA-LSBMR ^[10] /dB	PSO-LSBMR/dB
Lena	55.36	57.59	59.67
Peppers	55.38	57.48	59.54
Barbara	55.43	57.58	59.67
Cameraman	55.48	57.54	59.53
Baboon	55.45	57.60	59.57
Woman	55.43	57.52	59.54
Boat	55.47	57.55	59.69
Average	55.43	57.55	59.60

算法的视觉效果比较。实验结果表明, GA-LSBMR 的视觉效果要优于 Mielikainen 的方法, 笔者提出的 PSO-LSBMR 的视觉效果最优。例如当满嵌时, GA-LSBMR 和 PSO-LSBMR 算法的平均 PSNR 分别为 54.41 dB 和 56.40 dB, PSNR 提高了 1.99 dB; 当嵌入率为 50% 时, GA-LSBMR 和 PSO-LSBMR 算法的平均 PSNR 分别为 57.55 dB 和 59.60 dB, PSNR 提高了 2.05 dB。在嵌入相同容量秘密信息的条件下, 新算法减少了载体图像中灰度值发生变化的像素点数, 有效提高了隐秘图像的视觉感知质量。

图 3 描述的是随着迭代次数的增加, PSO 算法的收敛情况。实线表示当前迭代次数的平均适应度值, 虚线表示当前迭代次数的最大适应度值。由图可知, 随着迭代次数的增加, 此算法能寻找到更优的适应度值。

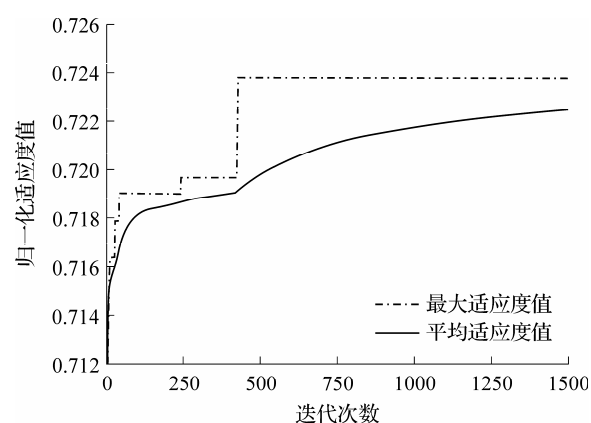


图3 PSO 算法收敛曲线

4 结语

提出了一种三级得分评价策略, 并基于此评价策略改进的配对 LSB 匹配方案可以获得更高的

PSNR 值, 改善了隐写性能. 虽然本文方案的计算过程比较耗时, 但实验结果表明, 在不同的嵌入率下, 新算法取得了比 LSBMR 和 GA-LSBMR 更好的图像质量, 具有更好的隐写性能. 未来我们可以进一步研究比较不同优化算法在寻找最优调整向量方面的性能.

参考文献:

- [1] 刘粉林, 刘九芬, 罗向阳等. 数字图像隐写分析[M]. 北京: 机械工业出版社, 2010:49-60.
- [2] Ker A D. Improved detection of LSB steganography in grayscale images[C]. Information Hiding, Springer Berlin Heidelberg, 2005:97-115.
- [3] Chan C K, Cheng L M. Hiding data in images by simple LSB substitution[J]. Pattern recognition, 2004, 37(3): 469-474.
- [4] Mielikainen J. LSB matching revisited[J]. IEEE Signal Processing Letters, 2006, 13(5): 285-287.
- [5] Fridrich J, Goljan M, Soukal D. Higher-order statistical steganalysis of palette images[C]. Security, Steganography, and Watermarking of Multimedia Contents, 2003: 178-190.
- [6] Fridrich J, Soukal D, Goljan M. Maximum likelihood estimation of length of secret message embedded using $\pm k$ steganography in spatial domain[C]. Security, Steganography, and Watermarking of Multimedia Contents, 2005:595-606.
- [7] Soleimanpourmoghaddam M, NezamabadiH, Farsangi M M, et al. A more secure steganography method based on pair-wise LSB matching via a quantum gravitational search algorithm[C]. 2012 16th CSI International Symposium on Artificial Intelligence and Signal Processing, 2012:34-38.
- [8] Xu H, Wang J, Kim H J. Near-optimal solution to pair-wise LSB matching via an immune programming strategy[J]. Information Sciences, 2010, 180(8):1201-1217.
- [9] Khosravi M, Soleymanpourmoghaddam S, Mahyabadi M. Improved pair-wise LSB matching steganography with a new evaluating system[C]. 2012 Sixth International Symposium on Telecommunications, 2012:982-986.
- [10] Elbeltagi E, Hegazy T, Grierson D. Comparison among five evolutionary-based optimization algorithms[J]. Advanced engineering informatics, 2005, 19(1): 43-53.

Evaluation and Improvement for LSB Matching Steganography

FANG Meng-meng^{1,2}, HE Jia-ming^{1,2*}, JIN Chao³, SHI Zhi-hui^{1,2}

(1.Institute of Communication Technology, Ningbo University, Ningbo 315211, China; 2.Key Laboratory of Mobile Internet Application Technology of Zhejiang Province, Ningbo University, Ningbo 315211, China; 3.CKC Institute of Artificial Intelligence and Software Engineering, Ningbo University, Ningbo 315211, China)

Abstract: By analyzing the performance impact of different matching orders between secret messages and carrier pixels on the algorithm, this paper proposes a three-level score evaluating strategy based on the pair-wise LSB matching method proposed by Mielikainen. Using the new evaluating strategy, a particle swarm optimization algorithm is applied to search for an optimal solution among all such permutation orders, based on which a novel steganographic algorithm is presented aiming at improving Mielikainen's method. The experimental results indicate that, with the same amount of secret information, the proposed method further reduces the number of pixels with changed gray-values in the carrier image after embedding the secret messages. Therefore, the stegano image achieves higher visual perceptual quality using the proposed method than Mielikainen's method.

Key words: information hiding; LSB matching; steganography; evaluation; particle swarm optimization algorithm

(责任编辑 章践立)