文章编号:1001-5132（2007）04-0421-04

基于 MSE 下限的 LSB 隐藏算法的分析与性能评价

严迪群，王让定

（宁波大学 纵横智能软件研究所， 浙江 宁波 315211）

摘要：LSB 算法是信息隐藏的基础方法之一. 以往对经典 LSB 隐藏算法进行研究评价时，往往不考虑隐秘信息长度对算法性能指标的动态影响. 针对该问题，对最差情况下隐秘信息长度与经典 LSB 隐藏算法性能之间的关系进行了分析讨论，并给出了性能评价的一般表达式. 最后通过实验验证了所提出性能评价表达式的正确性，对进一步提高 LSB 算法性能有一定的指导意义.

关键词：信息隐藏；LSB；性能评价

中图分类号：TP319 文献标识码：A

信息隐藏是利用多媒体信息中的冗余空间携带隐秘信息，达到信息伪装传输的目的[1]. 由于信息隐藏技术利用了人类感官的冗余，所以隐藏后的多媒体信息外部特征并无明显变化，可以使主观难以察觉. 目前已出现了多种信息隐藏算法，其中基于LSB的信息隐藏算法是最简单，同时也是最常用的一种方法. 由于其具有计算复杂度低、隐藏容量大及通用性强等特点，因此依然是目前公认较为成熟的信息隐藏算法之一[2-4].

无论是经典LSB算法，还是诸多改进的LSB算法[5-7]，当隐藏深度增加时，算法的不可感知性和抵抗攻击的能力会随之下降. 但目前在对LSB算法进行性能评价时，往往只从所替换LSB位平面个数的角度，考察隐秘信息长度对算法性能的影响，但在实际应用过程中，经常会有隐秘信息的长度与载体LSB位平面的个数不匹配的问题，即不能完整地替换LSB位平面，以往的研究对此缺乏合理的考虑. 针对这一问题，本文深入分析了隐秘信息长度与算法性能之间的关系，并推导了评价LSB算法性能的一般表达式，实验测试结果验证了本文所推导表达式的正确性.

1 经典LSB隐藏算法[8]

图像中每个像素点数值的某一位共同构成 1 个新的二值图像，称为该图像的 1 个位平面图像. 对于 256 级灰度图像，一般定义第 0 位平面到第 7 位平面依次为最不重要位平面(LSB)到最重要位平面(MSB). 而经典 LSB 隐藏算法通过替换 LSB 位平面达到信息隐藏的目的. 图像通常都存在一定的噪声，而由于 LSB 替换而引起的变化可以被噪声所掩盖，这是利用替换 LSB 位平面实现信息隐藏的基本依据.

令 $\{f_1, f_2, \cdots, f_n\}$ 为从原始载体图像中选出作为隐藏保密信息的像素点集合，$\{b_1, b_2, \cdots, b_n \mid b_i \in \{0,1\}\}$ 为待隐藏保密信息，则将 b_i 隐藏至像素点 f_i

收稿日期：2007-06-21. 宁波大学学报（理工版）网址：http://3xb.nbu.edu.cn
基金项目：国家自然科学基金（60672070）；宁波大学学科项目（2006980）.
作者简介：严迪群（1979－），男，浙江余姚人，助理实验师，主要研究方向：信息隐藏及语音编码. E-mail: yandiqun@nbu.edu.cn

最低位的 LSB 替换过程可描述为：

$$c^1\{f_i\} \leftarrow b_i, \tag{1}$$

其中，算子 $c^1\{\cdot\}$ 表示取像素点最低位. 上述的隐藏过程可扩展到替换最低 p 位，

$$c^{1\sim p}\{f_i\} \leftarrow b_{p*(i-1)+1}, b_{p*(i-1)+2}, \cdots, b_{p*i}. \tag{2}$$

如 $p=4, i=1$ 时，$c^{1\sim 4}\{f_1\} \leftarrow b_1, b_2, b_3, b_4$，表示像素点 f_1 的最低 1 至 4 位分别被隐秘信息 b_1, b_2, b_3, b_4 替换. i 取其他值时，可依次类推.

隐秘信息提取时，根据替换位数，直接提取含秘载体像素点的 LSB 位，然后按替换顺序排列，即可得到隐秘信息.

通常用峰值信噪比 *PSNR* 来评价嵌入隐秘信息后载体图像的质量，*PSNR* 越大，含秘载体图像的保真度越高，其可定义为[9]：

$$PSNR = 10 \times \lg\left(\frac{255^2}{MSE}\right) \text{dB}, \tag{3}$$

其中，*MSE* 表示均方误差，其定义为：

$$MSE = \frac{\sum_{i=1}^{L}(f_i - f_i')^2}{L}, \tag{4}$$

其中，L 为载体图像像素点总数，f_i 和 f_i' 分别为原始像素点和含隐秘信息像素点的数值.

定义 MSE_{worst} 和 $PSNR_{\text{worst}}$ 为最坏情况下(即 0 替换为 1 或 1 替换为 0)的均方误差和峰值信噪比，则：

$$\begin{aligned} MSE_{\text{worst}} &= \frac{\sum_{i=1}^{L}(2^p-1)^2}{L} = (2^p-1)^2, \\ PSNR_{\text{worst}} &= 10 \times \lg\left(\frac{255^2}{MSE_{\text{worst}}}\right) \text{dB}, \end{aligned} \tag{5}$$

表 1 为 $PSNR_{\text{worst}}$ 在替换深度下的理论值. 从表 1 中可以发现，当替换 LSB 的位数 $p \geq 4$ 时，含隐秘信息的载体图像质量将急剧下降.

表 1 经典 LSB 替换 $p=1\sim5$ 时的 $PSNR_{\text{worst}}$ 理论值

P	$PSNR_{\text{worst}}$
1	48.13
2	38.59
3	31.23
4	24.61
5	18.30

2 LSB 算法性能评价

假设待隐藏信息为 $M=\{b_1, b_2, \cdots, b_n \mid b_i \in \{0, 1\}\}$，载体图像为 $I=\{f_1, f_2, \cdots, f_L \mid f_i \in \{0, 1, \cdots, 2^k-1\}\}$. 长度为 n 比特；长度为 L，每个像素点由 k 比特表示. 为了使隐秘信息 M 完全隐藏于 I 中，至少需要载体图像最低 $l=\lceil n/L \rceil$ 个位平面，其中 $\lceil\ \rceil$ 表示向上取整，令 $r=n/L$，为隐秘信息长度与载体像素点总数之比. 本文根据 MSE_{worst} 的定义，通过推导得到了经典 LSB 算法性能评价的一般表达式.

当 $0 \leq r \leq 1$ 时，即隐秘信息的长度小于载体像素点总数，在最差情况下，将有 n 个像素点的最右边的 LSB 位发生翻转，而其余 $L-n$ 个像素点的 LSB 位将保持原始值不变. 因此，MSE_{worst} 可按下式计算：

$$MSE_{\text{worst}} = \frac{1}{L} \times \left(\sum_{i=1}^{n} 1^2 + \sum_{j=1}^{L-n} 0^2\right) = \frac{n}{L} = r.$$

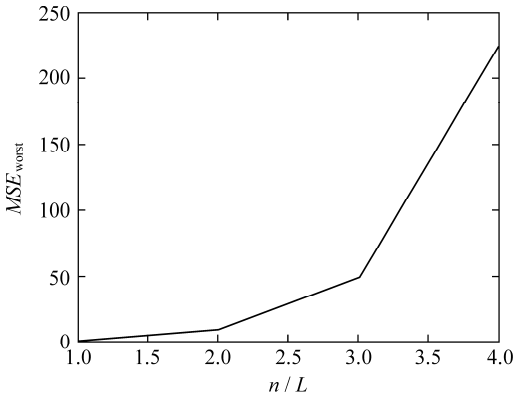
同理，当 $1 < r \leq 2$ 时，

$$MSE_{\text{worst}} = \frac{1}{L} \times \left\{\sum_{i=1}^{n-L} 3^2 + \sum_{j=1}^{2L-n} 1^2\right\} = 8r - 7.$$

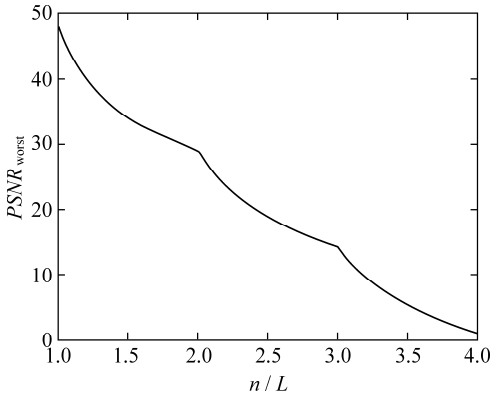
当 $k-1 < r \leq k$ 时，

$$\begin{aligned} MSE_{\text{worst}} = \frac{1}{L} \times \Bigg\{ & \sum_{i=1}^{n-(\lceil r \rceil -1)\times L} (2^{\lceil r \rceil}-1)^2 + \\ & \sum_{j=1}^{\lceil r \rceil \times L - n} (2^{\lceil r \rceil -1}-1)^2 \Bigg\} = (2^{\lceil r \rceil}-1)^2 \times (r - \\ & \lceil r \rceil + 1) + (2^{\lceil r \rceil -1}-1)^2 \times (r - \lceil r \rceil). \end{aligned} \tag{6}$$

(6)式即为经典的 LSB 算法性能评价指标 MSE_{worst} 关于参数 r 的一般表达式. 根据隐秘信息和载体像素点个数之间的比例，可分 2 个步骤计算 MSE_{worst}. (1)替换深度为 $\lceil r \rceil$ 的像素点对应的均方误差，由(6)式加号左侧部分表示. (2)替换深度为 $(\lceil r \rceil - 1)$ 的像素点对应的均方误差，由(6)式右侧部分表示. 再结合(3)式可以得到 $PSNR_{\text{worst}}$ 表达式. 图 1 则为经典 LSB 算法 MSE_{worst} 和 $PSNR_{\text{worst}}$ 指标随参数 r 变化的理论曲线.



(a) MSE_{worst}理论曲线



(b) $PSNR_{worst}$理论曲线

图 1　经典 LSB 算法性能理论曲线

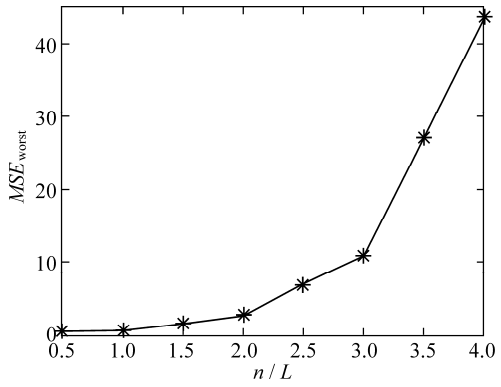
3　实验测试结果

为了验证本文所推导表达式的正确性，用经典 LSB 算法作了相关算法测试. 测试载体图像为 128*128，256 级灰度的 Lena 图像；隐秘信息选择不同长度且取值为 0 和 1 的二值随机序列.

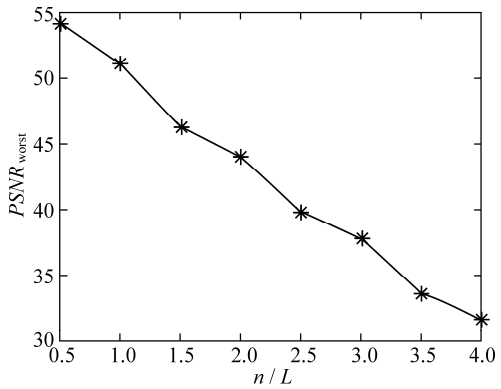
表 2 为采用经典 LSB 算法在载体图像 Lena 嵌入不同长度隐秘信息的实验结果. 图 2 则为 Lena 载体图像在嵌入不同长度隐秘信息时测试得到的 MSE 和 PSNR 实验曲线，可以发现图 2 的曲线与之前给出的图 1 的理论曲线相吻合，从而验证了本文所推导评价表达式的正确性. 图 3 则为经典 LSB 算法在隐秘信息取不同长度情况时，含隐秘信息的载体图像.

表 2　LSB 算法测试数据

n/L	0.5	1.0	1.5	2.0
MSE_{simp}	0.249 8	0.494 0	1.508 1	2.545 8
$PSNR_{simp}$	54.154 6	51.193 4	46.346 5	44.072 5
n/L	2.5	3.0	3.5	4.0
MSE_{simp}	6.697 5	10.664 9	27.101 3	43.605 5
$PSNR_{simp}$	39.871 7	37.851 3	33.800 9	31.735 4



(a) *MSE* 测试曲线



(b) *PSNR* 测试曲线

图 2　经典 LSB 算法性能测试曲线

(a) LSB $r=0.5$　　(b) LSB $r=2$

(c) LSB $r=3.5$　　(d) LSB $r=4$

图 3　不同嵌入比的 Lena 图像

4 结论

本文对经典 LSB 隐藏算法进行了研究，着重分析隐秘信息长度与算法性能之间的关系，并推导得出经典 LSB 算法性能评价的一般表达式，最后通过实验测试验证了该表达式的正确性，对今后进一步改进和提高 LSB 算法性能有一定的指导意义.

参考文献：

[1] 钮心忻. 信息隐藏与数字水印[M]. 北京: 北京邮电大学出版社, 2004.

[2] Cox I, Miller M. Electronic watermarking: the first 50 years[C]//Proc 4th IEEE workshop on multimedia signal processing. France: Cannes, 2001:225-230.

[3] Liu S H, Chen T H, Yao H X, et al. A variable depth LSB data hiding technique in images[C]//In proceedings of the third international conference on machine learning and cybernetic. Shanghai, 2004:3 990-3 994.

[4] Bender W, Gruhl D, Morimoto N. Techniques for data hiding[J]. IBM Systems Journal, 1996, 35(3/4):313-336.

[5] Wang R Z, Lin C F, Lin J C. Image hiding by optimal LSB substitution and genetic algorithm[J]. Pattern Recognition, 2001, 34(3):671-683.

[6] Chang Chinchen, Yuan Ju, Hsiao. Finding optimal least-significant-bit substitution in image hiding by dynamic programming strategy[J]. Pattern Recognition, 2003, 36 (7):1 583-1 595.

[7] Cvejic N, Seppanen T. Increasing robustness of LSB audio steganography using a novel embedding method[C] //In proceedings of IEEE international conference on information technology: coding and computing, 2004, 2: 533-537.

[8] 王育民, 张彤, 黄继武. 信息隐藏—理论与技术[M]. 北京: 清华大学出版社, 2006.

[9] CHAN C K, CHENG L M. Hiding data in images by simple LSB substitution[J]. Pattern Recognition, 2004, 37 (3):469-474.

The Restudy on Performance Evaluation of LSB Image Hiding Algorithm

YAN Di-qun, WANG Rang-ding

(CKC Software Lab, Ningbo University, Ningbo 315211, China)

Abstract: LSB (Least Significant Bits) algorithm is commonly used in information hiding. However, previous studies lack sufficient consideration for dynamic effects of payload length on performance evaluation index of standard LSB algorithm. To redress this issue, in this paper the function between payload length and performance evaluation index is analyzed for the worst case, and the general expression of performance evaluation is derived. The experiment results validate the proposed analytical expression. The research effort made in this paper is expected to render some technical insights into further investigation in the related area.

Key words: information hiding; LSB; performance evaluation

CLC number: TP319 **Document code:** A

（责任编辑 章践立）