基于 Fisher 信息的最优隐写方法

孙怡峰[1,2]，刘粉林[1]，王 飞[3]，曾 颖[1]
（1. 信息工程大学 信息工程学院，郑州 450002；2. 信息工程大学 电子技术学院，郑州 450004；
3. 装备指挥技术学院 信息装备系，北京 101416）

摘 要：为了提高隐写算法的安全性，提出一种基于 Fisher 信息的最优隐写框架. 将隐写算法设计建模成以嵌入转移概率为决策变量、以 Fisher 信息最小化为目标的最优化问题. 推导出 Fisher 信息是嵌入转移概率的二次型，通过二次规划求解最优嵌入转移概率. 给出了一个最优隐写算法实例——最优 LSB matching 算法，实验结果表明，最优 LSB matching 算法的 Fisher 信息小于传统 LSB matching 算法，隐写安全性提高.

关键词：数字隐写；安全性；信息隐藏；二次规划
中图分类号：TP 391 **文献标志码**：A **文章编号**：0254－0037(2010)05－0689－05

数字隐写是指将秘密信息隐藏在可公开传输的多媒体数据中，利用多媒体表面意义的掩护使攻击者无法发现秘密信息的存在，从而保证秘密信息的安全. 随着基于统计的隐写检测技术发展，数字隐写的安全性受到挑战，如何提高隐写的安全性受到了学者的关注. Cachin[1] 使用 Kullback-Leibler divergence（KL 散度）定义了隐写系统的安全性. 文献[2-3]在嵌入中使用统计恢复来保证一阶和二阶统计意义上隐写安全（零 KL 散度）. 文献[4-5]将 KL 散度作为目标函数根据载体优化嵌入操作. 最近，文献[6-7]提出 KL 散度泰勒展开中的二次项系数（Fisher 信息）可用于度量隐写系统的性能，文献[8-9]给出了 Fisher 信息的估计法. 本文在此基础上提出了一种将 Fisher 信息作为目标函数的最优隐写框架. 推导得出 Fisher 信息是嵌入转移概率的二次型，通过二次规划求解最优嵌入转移概率. 实验测试了 LSB matching 嵌入算法最优化后的 Fisher 信息，验证了优化的有效性.

1 隐写安全与 Fisher 信息

与其他通信方式不同，数字隐写只要是被攻击方发现就会被认为是不安全的. 因此，隐写的安全性往往通过隐写系统对抗隐写检测的能力来度量. Cachin[1] 通过 KL 散度（也称为相对熵）从信息理论的角度度量隐写系统安全性. 将载体和载密体建模成某种随机过程的实现，设载体对象服从概率分布 $P(0)$，载密体服从概率分布 $P(\lambda)$，参数 λ 表征秘密信息的负载量（payload size）. 将隐写检测看成假设检验问题，假设检验的 2 类错误率：虚警率（false positive）和漏警率（false negative）在最好情况下与 KL 散度密切相关，因此 KL 散度可用于度量隐写系统的安全性. 记 λ 负载量下隐写系统的 KL 散度为 $D(P(0)) \| P(\lambda))$，如果 $D(P(0) \| (P(\lambda)) = 0$，称隐写系统是绝对安全的；如果 $D(P(0)) \| P(\lambda)) = \varepsilon$，称隐写系统是 ε 安全的.

为了方便描述，将载体对象记为长度为 n 的随机序列 $(X_1, \cdots, X_n)$，对应的载密体对象记为 $(Y_1, \cdots, Y_n)$，X_i 和 Y_i 均取值于有限集 χ，参数 n 的物理意义是一个多媒体载体对象中具体可用于嵌入秘密信息的数据个数，如图像空域像素的个数，或者离散余弦变换（DCT）系数的个数. 记随机矢量 $(X_1, \cdots, X_n)$ 的联合概率分布为 $P_0(\boldsymbol{X} = \boldsymbol{x})$，随机矢量 $(Y_1, \cdots, Y_n)$ 的联合概率分布为 $P_\lambda(\boldsymbol{Y} = \boldsymbol{y})$，其中用 $\boldsymbol{X}$ 代表 $(X_1, \cdots, X_n)$，

收稿日期：2009-12-10.
基金项目：国家自然科学基金资助项目（60970141，60902102）.
作者简介：孙怡峰（1976—），男，河南淇县人，讲师.

用 $\boldsymbol{Y}$ 代表$(Y_1,\cdots,Y_n)$，$\boldsymbol{x}$ 和 $\boldsymbol{y}$ 代表集合叉积$\chi^n=\chi\times\chi\times\cdots\times\chi$ 中的元素.

采用独立嵌入模型[9]，即隐写算法按一定概率在密钥的指导下随机选择符号 $X_i, i=1,\cdots,n$ 用于承载秘密信息. 这个概率与最终的负载量紧密相关，将参数 λ 的物理意义限定为上述概率，并称为负载率(嵌入率)，$0\leqslant\lambda\leqslant1$. 当某个符号 X_i 被选中用于承载秘密信息时，根据嵌入规则将 X_i 修改成 Y_i，完成秘密信息的嵌入. 嵌入规则可用条件概率 $P(Y_i=y\mid X_i=x)=b_{xy}$ 描述，将其称为嵌入转移概率. 矩阵 $\boldsymbol{B}=(b_{xy})_{x\in\chi,y\in\chi}$ 决定了嵌入算法内部工作机理，将其称为嵌入矩阵. 矩阵 $\boldsymbol{B}$ 的任意行必须满足

$$\sum_{y\in\chi}b_{xy}=1. \tag{1}$$

这种嵌入模型可以描述非自适应隐写算法[9].

根据 KL 散度的定义式

$$D(P(0)\parallel P(\lambda))=\sum_{x\in\chi^n}P_0(\boldsymbol{X}=\boldsymbol{x})\log_2\frac{P_0(\boldsymbol{X}=\boldsymbol{x})}{P_\lambda(\boldsymbol{Y}=\boldsymbol{x})} \tag{2}$$

隐写系统的 KL 散度是 λ 和 n 的函数，但往往无法得到解析式[10]. 设载体数据个数 n 为固定值，可将 KL 散度值看成 λ 的一元函数，记为

$$D(P(0)\parallel P(\lambda))=\mathrm{d}_n(\lambda) \tag{3}$$

Filler 等[7]在 $\lambda=0$ 处将 KL 散度泰勒展开，得到

$$D(P_n(0)\parallel P_n(\lambda))=\frac{1}{2!}\mathrm{d}_n''(0)\lambda^2+O(\lambda^3) \tag{4}$$

当 $\lambda\to0$ 时，

$$D(P_n(0))\parallel P_n(\lambda))\approx\frac{1}{2}\mathrm{d}_n''(0)\lambda^2 \tag{5}$$

$\mathrm{d}_n''(0)$是 KL 散度对 λ 的二阶导数在 $\lambda=0$ 的取值，被称为 Fisher 信息(Fisher information). 从式(5)可见，在相同的 ε 安全限制下，即 $D(P_n(0)\parallel P_n(\lambda))\leqslant\varepsilon$ 时，Fisher 信息值越小，可获得的最大负载率 λ 就越大. 文献[6]给出负载率的平方根准则为

$$\lambda=\frac{C}{\sqrt{n}} \tag{6}$$

$$D(P_n(0)\parallel P_n(\lambda))\approx\frac{1}{2}\mathrm{d}_n''(0)\frac{C^2}{n}\leqslant\varepsilon \tag{7}$$

$$C\leqslant\sqrt{\frac{2\varepsilon}{\mathrm{d}_n''(0)/n}} \tag{8}$$

式中，$\mathrm{d}_n''(0)/n$ 被称为 Fisher 信息率，决定了相同风险下隐写算法的最大负载率 λ.

Fisher 信息 $\mathrm{d}_n''(0)$是比较隐写算法性能的一种客观指标[9]，并且 $\mathrm{d}_n''(0)$与负载率 λ 无关，相对于 KL 散度而言容易计算. Ker[9]给出了 Fisher 信息的一种估计方法为

$$\mathrm{d}_n''(0)=\sum_{y\in\chi^n}\frac{A(\boldsymbol{y})^2}{P_0(\boldsymbol{X}=\boldsymbol{y})}-n^2 \tag{9}$$

$$A(\boldsymbol{y})=\sum_{i=1}^{n}\sum_{u\in\chi}P_0(\boldsymbol{X}=\boldsymbol{y}[u/y_i])b_{uy_i} \tag{10}$$

式中，$\boldsymbol{y}[u/y_i]$代表取值$(y_1,\cdots,y_{i-1},u,y_{i+1},\cdots,y_n)$，即用 u 代替 $\boldsymbol{y}$ 中的子项 y_i. 从式(9)和式(10)可见，只需要知道载体的数据联合概率分布和嵌入规则 $\boldsymbol{B}=(b_{xy})$，就可以求解出 Fisher 信息. 因此，嵌入系统的性能也是由载体分布特性和嵌入方法共同决定.

2 最优隐写框架

对嵌入算法而言，Fisher 信息越小越好. 由式(9)，当载体分布特性已确定时，Fisher 信息是嵌入规则矩阵 $\boldsymbol{B}$ 中元素 $b_{xy}(x\in\chi,y\in\chi)$的函数. 最优隐写的基本思想就是假定载体数据联合概率分布已知，求解

使 Fisher 信息最小的嵌入矩阵

$$\boldsymbol{B}_{\text{optimal}} = \arg \min_{\boldsymbol{B}=(b_{xy})} \sum_{\boldsymbol{y}\in\chi^n} \frac{A(\boldsymbol{y})^2}{P_0(\boldsymbol{X}=\boldsymbol{y})} - n^2 \tag{11}$$

约束条件为

$$\begin{cases} \sum\limits_{y\in\chi} b_{xy} = 1, x \in \chi \\ b_{xy} \geqslant 0 \end{cases} \tag{12}$$

为了进一步观察 Fisher 信息与 $\boldsymbol{B}$ 中元素的关系，做如下展开

$$\begin{aligned} \sum_{\boldsymbol{y}\in\chi^n} \frac{A(\boldsymbol{y})^2}{P_0(\boldsymbol{X}=\boldsymbol{y})} = & \sum_{u\in\chi}\sum_{v\in\chi}\sum_{i=1}^{n}\sum_{j=1}^{n}\sum_{\boldsymbol{y}\in\chi^n} \frac{P_0(\boldsymbol{X}=\boldsymbol{y}[u/y_i])P_0(\boldsymbol{X}=\boldsymbol{y}[v/y_j])}{P_0(\boldsymbol{X}=\boldsymbol{y})} b_{uy_i}b_{vy_j} = \\ & \sum_{u\in\chi}\sum_{v\in\chi}\sum_{a\in\chi}\sum_{\substack{b\in\chi\\ b\neq a}} \left(\sum_{i=1}^{n}\sum_{\substack{j=1,\\ j\neq i}}^{n}\sum_{\substack{\boldsymbol{y}\\ \text{except}\\ y_i,y_j}} \frac{P_0(\boldsymbol{X}=\boldsymbol{y}[u/y_i,b/y_j])P_0(\boldsymbol{X}=\boldsymbol{y}[a/y_i,v/y_j])}{P_0(\boldsymbol{X}=\boldsymbol{y}[a/y_i,b/y_j])} \right) b_{ua}b_{vb} + \\ & \sum_{u\in\chi}\sum_{v\in\chi}\sum_{a\in\chi} \left\{ \sum_{i=1}^{n}\sum_{\substack{j=1\\ j\neq i}}^{n}\sum_{\substack{\boldsymbol{y}\\ \text{except}\\ y_i,y_j}} \frac{P_0(\boldsymbol{X}=\boldsymbol{y}[u/y_i,a/y_j])P_0(\boldsymbol{X}=\boldsymbol{y}[a/y_i,v/y_j])}{P_0(\boldsymbol{X}=\boldsymbol{y}[a/y_i,a/y_j])} + \right. \\ & \left. \sum_{i=1}^{n}\sum_{\substack{\boldsymbol{y}\\ \text{except}\ y_i}} \frac{P_0(\boldsymbol{X}=\boldsymbol{y}[u/y_i])P_0(\boldsymbol{X}=\boldsymbol{y}[v/y_i])}{P_0(\boldsymbol{X}=\boldsymbol{y}[a/y_i])} \right\} b_{ua}b_{va} \end{aligned} \tag{13}$$

式中，$\boldsymbol{y}[a/y_i,b/y_i]$代表用 a 代替 $\boldsymbol{y}$ 中的子项 y_i，用 b 代替 $\boldsymbol{y}$ 中的子项 y_j. 从式(13)可见，Fisher 信息是嵌入转移概率 b_{xy}的二次型，二次项 $b_{ua}b_{vb}$的系数由载体数据的联合概率分布 $P_0(\boldsymbol{X}=\boldsymbol{x})$确定，这与文献[7]中的定理 2 相吻合，且式(13)更易计算. 因此，可用二次规划求解使 Fisher 信息最小的 b_{xy}.

3　最优空域 LSB matching 隐写算法

LSB matching 隐写算法也被称为 ±1 嵌入，其基本思想是当待嵌入的秘密信息比特与(按负载率)选中的载体数据最低比特位(LSB)不相等时，随机选择加 1 或减 1 操作使载体数据 LSB 等于秘密信息比特(饱和数据除外). 在图像空域数据中应用 LSB matching 算法实施嵌入，此时$\chi = \{0,1,\cdots,255\}$. 设秘密信息在嵌入前已被加密为伪随机比特流，可以认为大约一半的载体数据 LSB 与秘密信息比特相同，即 $b_{x,x} = 0.5$. 优化前的 LSB matching 嵌入矩阵为

$$\boldsymbol{B} = \begin{pmatrix} 0.5 & 0.5 & 0 & \cdots & 0 & 0 & 0 \\ 0.25 & 0.5 & 0.25 & \cdots & 0 & 0 & 0 \\ 0 & 0.25 & 0.5 & \cdots & 0 & 0 & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & 0 & \cdots & 0.5 & 0.25 & 0 \\ 0 & 0 & 0 & \cdots & 0.25 & 0.5 & 0.25 \\ 0 & 0 & 0 & \cdots & 0 & 0.5 & 0.5 \end{pmatrix} \tag{14}$$

应用最优化隐写框架，若秘密信息比特与载体数据 x 的 LSB 不等，将嵌入规则改为：当 x 不等于 0 和 255 时，以概率 $b_{x,x+1}$加 1，以概率 $b_{x,x-1}$减去 1. 对应嵌入矩阵为

$$\boldsymbol{B} = \begin{pmatrix} 0.5 & 0.5 & 0 & \cdots & 0 & 0 & 0 \\ b_{1,0} & 0.5 & b_{1,2} & \cdots & 0 & 0 & 0 \\ 0 & b_{2,1} & 0.5 & \cdots & 0 & 0 & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & 0 & \cdots & 0.5 & b_{253,254} & 0 \\ 0 & 0 & 0 & \cdots & b_{254,253} & 0.5 & b_{254,255} \\ 0 & 0 & 0 & \cdots & 0 & 0.5 & 0.5 \end{pmatrix} \tag{15}$$

$\boldsymbol{B}$ 中的未知嵌入转移概率通过式(11)所示的优化问题来确定,但约束条件改为

$$\begin{cases} b_{x,x+1}+b_{x,x-1}=0.5, b_{x,x+1}\geqslant 0, b_{x,x-1}\geqslant 1, x\in\chi, x\neq 0, x\neq 255 \\ b_{x,x}=0.5, x\in\chi \\ b_{0,1}=0.5, b_{255,254}=0.5 \\ \text{其他 } b_{x,y}=0 \end{cases} \tag{16}$$

当得到最优嵌入矩阵 $\boldsymbol{B}=(b_{xy})$ 后,嵌入信息时应根据 b_{xy} 指示的转移概率对载体进行修改.

为了求解上述优化问题,需要首先确定 n 维联合概率分布 $P_0(\boldsymbol{X}=\boldsymbol{x})$,其中 n 代表载体数据的个数. 针对图像空域隐写,n 为图像中像素点的个数,分辨率为 1 024 × 768 图像的值将高达 78 万. 实际中无法估计超过 4 维的联合概率分布[9],一种解决方法就是将图像看成是由很多个相互独立的像素组组成[8]. 统计这些组直方图就可以得到对应 $n=2,3,4$ 的 $P_0(\boldsymbol{X}=\boldsymbol{x})$.

像素组可由 2、3、4 个相邻像素组成. 不同像素的相邻方式以及像素组中像素的个数将决定最优嵌入算法的安全性适用范围. Ker[9] 指出,基于像素组的 Fisher 信息约束了基于同样像素组隐写检测算法的性能上限. 因此,最优嵌入算法将在对抗基于相同像素组的隐写检测算法方面达到较好的性能.

4 实验与分析

实验采用 NRCS 图像库[11],共有 3 048 幅图像. 图像文件为彩色 TIF 格式,利用 Advanced Batch Converter 软件转换为8 位灰度 BMP 格式. 根据灰度图像统计组直方图,即估计 $P_0(\boldsymbol{X}=\boldsymbol{x})$. 像素组采用最简单的组成方式——由 2 个水平相邻像素构成. 根据估计出的 $P_0(\boldsymbol{X}=\boldsymbol{x})$ 进行嵌入矩阵 $\boldsymbol{B}=(b_{xy})$ 的最优化.

由于需要根据最优嵌入矩阵指示的转移概率对载体进行修改,最优隐写算法的复杂度取决于最优化过程的计算量. 这里的优化是二次规划问题,二次规划的复杂度取决于待优化参数的个数. 若对空域 LSB matching 嵌入算法进行优化,则待优化参数个数为 254 × 2 个,用 Matlab 中的二次规划函数就可快速求解;若假设 $\boldsymbol{B}=(b_{xy})$ 所有元素都通过优化确定,将有 256 × 256 个待优化参数,PC 机无法直接存储 Hessen 矩阵(需要 4 G 内存),最优化过程的复杂度将较高. 而文献[4-5]中隐写算法待优化参数个数等于要嵌入的秘密信息比特数,当嵌入较多秘密信息时其复杂度将较高.

图 1 比较了 LSB matching 嵌入算法优化前后的性能,以 Fisher 信息作为度量标准. 图中横坐标为统计像素组直方图所用的图像数,纵坐标为 Fisher 信息值. 从图可见,最优 LSB matching 对应的 Fisher 信息明显小于优化前. 此外,统计直方图的图像数量越多,估计出的 $P_0(\boldsymbol{X}=\boldsymbol{x})$ 越准确,优化后的 Fisher 信息值也就越小.

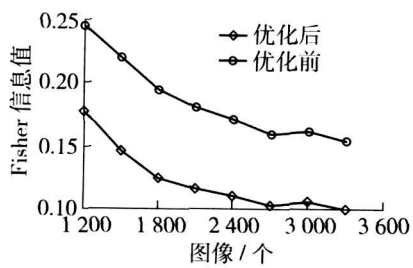

图 1 优化后的 Fisher 信息值

Fig. 1 Fisher information value after optimization

隐写系统的安全性除了受到嵌入规则的影响,还取决于负载率. 最优隐写在负载率较小时,根据计算出的 Fisher 信息值和式(5),可以估算最优嵌入的实际 KL 散度值,但若负载率比较大,由于 KL 散度的泰勒展开式中的拉格朗日余项 $O(\lambda^3)$ 值仍较大,通过式(5)计算出的 KL 散度与实际安全性存在一定误差.

5 结论

本文提出了一种最优隐写框架,将 Fisher 信息作为目标函数,嵌入转移概率作为待优化参数. 推导出 Fisher 信息是嵌入转移概率的二次函数,最优化是二次规划问题. 实验测试了最优空域 LSB matching 嵌入算法的 Fisher 信息,验证了优化算法的有效性. 需要指出的是,本文得到的最优隐写算法是局部最优的.

在优化前往往对嵌入矩阵进行了限制，如 LSB matching 算法就限定了 $\boldsymbol{B}=(b_{xy})$ 矩阵的每行只有 3 个转移概率取非 0 值，在此条件下的最小 Fisher 信息值是局部极值.

参考文献：

[1] CACHIN C. An information-theoretic model for steganography[C]// Proceedings of IH'98, LNCS 1525. Heidlberg: Springer-Verlag, 1998: 306-318.

[2] SOLANKI K, SULLIVAN K, MADHOW U, et al. Provably secure steganography: Achieving zero K-L divergence using statistical restoration[C]// Proceedings of ICIP'06. Piscataway: IEEE Signal Processing Society, 2007: 125-128.

[3] SARKAR A, SOLANKI K, MADHOW U, et al. Secure stegnography: statistical restoration of the second order dependencies for improved security [C]// Proceedings of ICASSP'07. Piscataway: IEEE Signal Processing Society, 2007: II-277- II-280.

[4] GUO Y, KONG X, YOU X. Secure steganography based on binary particles swarm optimization[J]. Journal of Electronics (China), 2009, 26(2): 285-288.

[5] LIU G, ZHANG Z, DAI Y, et al. GA-based LSB-matching steganography to hold second-order statistics[C]// Proceedings of MINES'09. Los Alamitos: IEEE Computer Society, 2009: 510-513.

[6] FILLER T, KER A D, FRIDRICH J. The square root law of steganographic capacity for Markov covers[C]// Proceedings of Media Forensics and Security'09, SPIE 7254. Bellingham: SPIE Press, 2009: 08-1 - 08-11.

[7] FILLER T, FRIDRICH J. Fisher information determines capacity of-secure steganography[C]// Proceedings of IH'09, LNCS 5806. Heidlberg: Springer-Verlag, 2009: 31-47.

[8] KER A D. Estimating steganographic fisher information in real images[C]// Proceedings of IH'09, LNCS 5806. Heidlberg: Springer-Verlag, 2009: 73-88.

[9] KER A D. Estimating the information theoretic optimal stego noise[C]// Proceedings of IWDW'09, LNCS 5703. Heidlberg: Springer-Verlag, 2009: 184-198.

[10] SILVA J, NARAYANAN S. Upper bound kullaback-leibler divergence for transient hidden Markov models[J]. IEEE Transactions on Signal Processing, 2008, 56(9): 4176-4187.

[11] NSDA. NRCS Photo gallery[EB/OL]. [2010-03-05]. http://photogallery. nrcs. usda. gov/

Optimal Steganography Based on Fisher Information

SUN Yi-feng[1,2], LI U Fen-lin[1], WANG Fei[3], ZENG Ying[1]

(1. Institute of Information Engineering, Information Engineering University, Zhengzhou 450002, China;
2. Institute of Electronic Technology, Information Engineering University, Zhengzhou 450004, China;
3. Department of Information Equipment, Institute of Equipment Command and Technology, Beijing 101416, China)

Abstract: This paper proposes an optimal steganography framework based on Fisher Information. An embedding algorithm is designed to solve the optimization problem whose objective is minimizing the Fisher Information of a steganographic system. The Fisher Information is the quadratic form of the embedding transferring probabilities. The problem of optimal embedding transferring probabilities is solved by quadratic programming. Then the optimal LSB matching algorithm, which is an instance of the optimal steganographic algorithm, is given. The experimental results show that the Fisher Information of the optimal LSB matching is smaller than that of the conventional LSB matching and the security of the optimal LSB matching is better.

Key words: steganography; security; information hiding; quadratic programming

（责任编辑　苗艳玲）