

# 基于 FCM 算法的隐写分析算法综合评估

龚 劬, 郭吉强

(重庆大学数理学院, 重庆 400044)

**摘 要:** 从与图像隐写分析算法评估相关的问题入手, 分析隐写分析算法评估的指标, 利用 FCM 算法实现对各种隐写分析算法的性能评估和比较。该评估算法不仅能对现有隐写分析算法进行评价, 以选出最优算法, 也适合对新的隐写分析算法进行性能评价。实验结果表明, 该评估算法是有效的。

**关键词:** 隐写分析; FCM 算法; 性能指标; 综合评估

## Comprehensive Evaluation of Steganalysis Algorithm Based on FCM Algorithm

GONG Qu, GUO Ji-qiang

(College of Mathematics & Physics, Chongqing University, Chongqing 400044)

**【Abstract】** Started with the issues related to evaluation of image steganalysis algorithm, the index for evaluation of steganalysis algorithm is analyzed. The evaluation and comparison to performance of steganalysis algorithm are implemented by using FCM algorithm. This evaluation algorithm can not only conduct evaluation to existed steganalysis algorithm, which chooses out the best one, but also conduct evaluation to new steganalysis algorithms. Experimental results show this evaluation algorithm is effective.

**【Key words】** steganalysis; Fuzzy C-Means(FCM) algorithm; performance index; comprehensive evaluation

### 1 概述

信息隐藏技术是种隐秘通信技术, 它将隐秘信息嵌入到原始载体中, 而在外表上与原始载体相似, 从而实现隐秘通信。随着信息技术的飞速发展, 隐写术作为信息隐秘技术的一个重要分支已取得了长足进步, 同时出现了很多针对不同隐写术的隐写分析算法。随着隐写分析技术的发展, 隐写分析算法的比较和评价也开始受到关注, 文献[1]用检出率和虚警率评价其提出的 LSB 隐写分析算法性能, 也有些学者利用检出率和虚警率分析了一些常见的隐写分析算法性能, 文献[2-4]分别对几种典型隐写分析算法作了分析和评价。因此, 有必要建立一个不仅可以宏观公正地比较各种隐写分析算法性能, 而且可以针对不同的实际需要已有隐写分析算法中选出最优算法的评估系统。

### 2 性能评估指标

评估隐写分析算法的首要问题是弄清楚在什么样的基准下对不同的算法进行评估, 而评估基准是要建立在评估标准, 即性能指标的基础之上的。性能一旦确定就可以确定具体评估的评估基准。研究者便可以使用该评估基准所形成的评估系统对所提出的隐写分析算法打出一个单独、量化的分数, 这个分数可以用来与其他类似的隐写分析算法进行比较。

#### 2.1 常用性能评估指标

对隐写分析算法性能评估最常用的指标有检出率、漏报率、虚报率、否定率, 下面给出其定义:

(1) 检出率  $P_1$ : 从隐蔽图像中检测出含有秘密信息的图像数  $M_1$  与隐蔽图像数  $M$  的比值, 即  $P_1=M_1/M$ 。

(2) 漏报率  $P_2$ : 隐蔽图像中检测出不含秘密信息的图像数  $M_2$  与隐蔽图像数  $M$  的比值, 即  $P_2=M_2/M$ 。

(3) 虚报率  $P_3$ : 非隐蔽图像中检测出含有秘密信息的图像数  $N_1$  与非隐蔽图像数  $N$  的比值, 即  $P_3=N_1/N$ 。

(4) 否定率  $P_4$ : 非隐蔽图像中检测出不含有秘密信息的图像数  $N_2$  与非隐蔽图像数  $N$  的比值, 即  $P_4=N_2/N$ 。

从以上 4 个性能指标定义中可以看出, 检出率和漏报率是从隐蔽图像的角度分析隐写分析算法性能; 虚报率和否定率是从载体图像的角度分析隐写分析算法性能。好的隐写分析算法应该有较大的检出率和否定率以及较小的漏报率和虚报率。

#### 2.2 进一步完善的性能评价指标

为更好地分析和反映隐写分析算法性能, 定义以下 3 种性能指标:

(1) 检测误差  $P_e$ : 假设用  $P(w_0)$ ,  $P(w_1)$  分别表示一张图片不含隐秘信息和含有隐秘信息的概率;  $P(e/w_0)$ ,  $P(e/w_1)$  分别表示隐写分析算法的误报率和漏报率, 则检测误差定义为

$$P_e = P(e/w_0) + P(e/w_1)$$

由文献[5]可知检测误差随着图像的隐藏平均信息能量增加而减少, 随着图像隐藏有效载荷容量的增加而增加。

(2) 检测复杂度(或检测耗时)  $P_{Com}$ : 检测算法检测出单位大小图片是否含有隐秘信息所需要的时间, 即

$$P_{Com} = \frac{1}{L} \sum_{i=1}^L \frac{T_i}{S_i}$$

其中,  $T_i$  表示检测  $L$  张图片中第  $i$  张图片的用时;  $S_i$  表示第  $i$  张图片的大小。

**作者简介:** 龚 劬(1963 -), 女, 教授、博士, 主研方向: 图论和小波分析; 郭吉强, 硕士研究生

**收稿日期:** 2008-08-10 **E-mail:** jiqiang8829@yahoo.com.cn

(3)检测适应性：由于隐蔽图像在传输过程中会受到干扰，从而导致一些原始隐蔽图像的改变，因此检测算法应能检测出经过干扰以后的隐蔽图像。而图像的改变可以用峰值信噪比 PSNR 和图像保真度来衡量。因此，定义检测算法的鲁棒性为：检测算法对经过一定干扰后隐蔽图像的检出率，记为  $P_5$ 。这里的干扰方式可以是压缩、滤波、加噪、剪贴、复制、旋转等攻击方式。

### 2.3 评语集

在本文的隐写分析算法评估体系中采用 4 级评语集，即评语集  $E=\{e_1(\text{优}), e_2(\text{良}), e_3(\text{中等}), e_4(\text{差})\}$

## 3 FCM 算法

设有  $n$  个待聚类样本(或模式)，类别个数为  $c$ ，特征数为  $s$ ，给出如下定义：

**定义 1** 样本集  $X=\{x_1, x_2, \dots, x_n\}$  是任一有限集， $x_i \in R^s, i=1, 2, \dots, n$ 。  $V_{cn}$  是  $c \times n$  阶实矩阵的集合； $c$  是整数，且  $2 \leq c \leq n$ ，则称下述集合为  $X$  的模糊  $c$  划分空间：

$$M_c = \{U \in V_{cn} \mid 0 \leq u_{ik} \leq 1, \forall i, k; \sum_{i=1}^c u_{ik} = 1, \forall k; \sum_{k=1}^n u_{ik} < n, \forall i\}$$

其中， $u_{ik}$  是隶属度矩阵  $U \in M_c$  的  $i$  行  $k$  列元素，表征  $x_k$  对于类  $i$  的隶属度值。

**定义 2** 设  $v_i \in R^s$  是类别聚类中心矢量。定义  $c$  聚类中心矩阵为

$$V = (v_1, v_2, \dots, v_c) \in R^{cs}$$

**定义 3** 模糊  $c$  均值聚类目标函数  $J_m : M \times R^{cs} \rightarrow R^+$  为

$$J_m(U, V) = \sum_{k=1}^n \sum_{i=1}^c (u_{ik})^m (d_{ik})^2$$

其中， $(d_{ik})^2 = \|x_k - v_i\|^2 = (x_k - v_i)^T (x_k - v_i)$ ； $m$  为加权指数，且  $m \in [2, \infty)$ 。

为得到样本集合  $X$  的最佳模糊  $c$  划分，通过如下迭代优化算法来使目标函数  $J_m(U, V)$  最小化：

- (1)确定聚类数目  $c, 2 \leq c \leq n$ ；确定参数  $m, 2 \leq m < \infty$ ；
- (2)确定初始隶属度矩阵  $U^{(0)} = (u_{ik}^{(0)})$ ；
- (3)令初始迭代次数  $b = 0$ ；
- (4)利用下式求各类的聚类中心  $v_i, i=1, 2, \dots, c$ ：

$$v_i = \sum_{k=1}^n (u_{ik})^m x_k / \sum_{k=1}^n (u_{ik})^m$$

(5)按如下方法计算新的隶属度矩阵  $U^{(b+1)}$ ，对  $k=1, 2, \dots, n$ ，计算  $I_k$  和  $\bar{I}_k$ ：

$$I_k = \{i \mid 1 \leq i \leq c; d_{ik} = \|x_k - v_i\| = 0\}$$

$$\bar{I}_k = \{1, 2, \dots, c\} - I_k$$

若  $I_k = \emptyset$ ，则  $u_{ik} = 1 / \sum_{j=1}^c (d_{ik} / d_{jk})^{2(m-1)}$ ；否则，对所有  $i \in \bar{I}_k$ ，置  $u_{ik} = 0$ ，并取  $\sum_{i \in I_k} u_{ik} = 1, k = k+1$ ；

(6)选用适宜的矩阵范数比较  $U^{(b)}$  和  $U^{(b+1)}$ ，若  $\|U^{(b)} - U^{(b+1)}\| < \varepsilon$ ，则停止；否则令  $b = b+1$ ，返回(4)。其中， $\varepsilon$  是收敛阈值。

## 4 算法的综合评估

第 2 节中给出了评价隐写分析算法的 7 种性能评估指标，可以将这 7 个指标看作是某一特定算法的特征向量  $x = \{P_1, P_2, P_3, P_4, P_e, P_{Com}, P_5\}$ ，其中， $P_1, P_2, P_3, P_4, P_e, P_{Com}, P_5$  分别代表检出率、漏报率、虚报率、否定率、检测误差、检测复杂度和检测鲁棒性，即可以将某一特定隐写分析算法看作是 7 维空间

上的一个元素。

将要评估的所有算法的特征向量组成数据样本集  $X$ ，再结合聚类类别数目  $c$ (这里取值为 4)与加权指数  $m$ ，就可以通过迭代确定出最佳聚类矩阵和聚类中心，从而实现最优聚类评判。

下面以基于 LSB 的隐写分析算法为例，验证本文评价方法的有效性。LSB 隐写是种简单有效的数据隐藏技术，具有简单、快速、信息隐藏容量大等特点。现在网上公开可得隐写软件大都是基于 LSB 隐写技术进行设计的。因此，目前的隐写分析算法也大都集中在针对 LSB 隐写术的特定隐写分析算法研究上。选用信息量估计法<sup>[5]</sup>( $F_1$ )、RS 分析法( $F_2$ )、基于差分直方图的分析法<sup>[6]</sup>( $F_3$ )、GEFR 分析法<sup>[7]</sup>( $F_4$ )、点对分析法<sup>[8]</sup>( $F_5$ )这 5 种常见的 LSB 隐写分析算法以供本文算法对隐写分析算法进行评估的实验使用。

为利用上述 5 种隐写分析算法验证本文算法，在 4 000 幅大小为  $1\ 536 \times 1\ 024$  的 12 bit 灰度图像库里，选择第 1 幅~第 100 幅图像进行实验，实验采用二值序列作为隐秘信息，随机嵌入到所选择的图片中，且嵌入率为 50%。在检测鲁棒性实验中，采用干扰率为 5% 的 JPEG 压缩，得到每种算法对应的性能指标数据如表 1 所示。

表 1 算法性能指标值

	$P_1$	$P_2$	$P_3$	$P_4$	$P_e$	$P_{Com}$	$P_5$
$F_1$	0.968	0.032	0.039	0.961	0.071	$1.792 \times 10^{-4}$	0.856
$F_2$	0.971	0.029	0.025	0.975	0.054	$1.767 \times 10^{-4}$	0.892
$F_3$	0.985	0.015	0.014	0.986	0.029	$1.553 \times 10^{-4}$	0.913
$F_4$	0.993	0.007	0.027	0.973	0.034	$2.115 \times 10^{-4}$	0.915
$F_5$	0.995	0.005	0.024	0.976	0.029	$1.052 \times 10^{-4}$	0.905

在得到每种算法所对应的性能指标后，就能利用第 3 节中的 FCM 算法求出隶属度矩阵，从而对这些算法进行评估。这里， $c=4, m=2$ ，得到的隶属度矩阵元素值如表 2 所示。

表 2 隶属度矩阵

	$F_1$	$F_2$	$F_3$	$F_4$	$F_5$
$e_1(\text{优})$	3.582 1e-009	0.901 92	$1.195 \times 10^{-7}$	$9.004 \times 10^{-5}$	0.921 8
$e_2(\text{良})$	3.248 4e-009	0.098 1	0.999 84	$7.033 8 \times 10^{-6}$	0.055 1
$e_3(\text{中})$	1	3.732 8e-007	7.7176e-006	$5.344 \times 10^{-7}$	0.005 6
$e_4(\text{差})$	1.111 2e-008	3.942 1e-007	3.1089e-005	$1.794 \times 10^{-7}$	0.017 5

从表 2 可以看出， $F_2, F_4, F_5$  这 3 种算法隶属于  $e_1(\text{优})$  的隶属度大于隶属于其他类的隶属度，因此，算法的检测性能  $F_5$  优于  $F_2$ ，而  $F_2$  优于  $F_4$ ；算法  $F_3$  隶属于  $e_2(\text{良})$  的隶属度大于隶属于其他类的隶属度；算法  $F_1$  隶属于  $e_3(\text{中})$  的隶属度大于隶属于其他类的隶属度；因此，从隶属度矩阵的值来看，这 5 种算法的检测性能由高到低依次为  $F_5, F_2, F_4, F_3, F_1$ 。

由于在利用隐写分析算法检测图像之前，随机地对载体图像嵌入了秘密信息。因此使随机嵌入检测准确率最高的  $F_5$  算法得到最优解。对于  $F_2$  和  $F_4$ ，其隐写分析检测指标很接近，所以，最后得到的隶属度也很相近，但由于  $F_4$  的运行时间多于  $F_2$ ，因此整体上还是  $F_2$  优于  $F_4$ 。而  $F_3$  的检测准确率低于  $F_4$ ，尽管  $F_3$  的运行效率好于  $F_4$ ，但在实验结果中偏重于检测的准确率，因此， $F_4$  优于  $F_3$ 。由于  $F_1$  算法成立的前提条件并不很严格，在实际检测中实验结果不稳定，因此对它的评估结果最差。综合以上数据可以看出，本文的评估方法是有效的。

## 5 结束语

基于图像的隐写分析对于发展我国自主信息安全技术有一定的实际意义。图像作为信息隐藏的良好载体，已在很多

(下转第 179 页)