基于距离和的隐写分析

刘祖根 平玲娣 史 烈 王继民 潘雪增
(浙江大学计算机学院,杭州 310027)

摘 要 为了攻击 GIF 格式图像中的隐秘术,提出了一种基于图像子块"距离和"的隐写分析算法。该算法中首先将距离用一个索引值同子块中其他索引值的差的绝对值表示,由于索引值的差值可正可负,因而将一个"距离和"区分为"正距离和"和"负距离和"2 个矢量,考虑到"正距离和"和"负距离和"两者代数和的符号,它们被归类为"主距离和"和"次距离和";接着采用直方图计算这些量的统计状态,并通过统计邻接"图像子块"的"距离和"共生矩阵来得到 32 个统计量;然后通过计算这些统计量的"直方图特征函数的块中心"来得到 56 维特征向量;最后运用支持向量机构造隐写分析算法。实验结果表明,该算法对 GIF 图像上多种隐秘术的检测性能均胜过传统算法。此外,"图像子块中不同索引值个数"还可用来改进抽取特征向量的方法。

关键词 隐写分析 距离和 特征向量 GIF
中图法分类号: TP309 **文献标识码**: A **文章编号**: 1006-8961(2009)02-0267-08

Steganalysis Based on Sum of Distances

LIU Zu-gen, PING Ling-di, SHI Lie, WANG Ji-min, PAN Xue-zeng
(*College of Computer Science and Technology, Zhejiang University, Hangzhou* 310027)

Abstract To attack steganographic schemes in graphics interchange format (GIF) images, a steganalytic algorithm was proposed based on sum of distances (SOD) of sub-block. The distance was computed as an absolute value of the difference between one index and other one in a sub-block of an image. The difference between two indices may be positive or negative so that an SOD was further classified into two kinds. Considering the sign of algebraic sum of positive and negative SODs in a sub-block, the two SODs were differentiated as primary and secondary SODs respectively. 32 statistics were computed using these quantities in an image and a 56-dimensional feature vector was obtained. A steganalytic algorithm was designed based on the feature vector and Support vector machine. Experimental results show that the presented algorithm outperforms traditional methods. The number of different indices in a sub-block was utilized to improve the extracting feature vectors techrique.

Keywords steganalysis, sum of distances, feature vector, GIF(graphics interchange format)

1 引 言

GIF(graphics interchange format)格式图像在网络环境中大量传输和应用,使不法分子有可能利用隐秘术在其中隐藏秘密信息来进行通讯。为维护互联网环境下的信息安全,需要有快速、高效的隐写分析系统,用来检测大量 GIF 格式图像中是否包含隐藏信息。

隐写分析分为专用隐写分析算法和盲检测算法两类,其中专用隐写分析算法是针对某种专门的隐秘术设计,而盲检测算法则可用于攻击多种隐秘术。GIF 格式图像上现有的高效隐写分析算法几乎都是针对特定隐秘术设计的,具有应用面窄和检测率低

基金项目: 浙江省自然科学基金项目(Y105355); 浙江省科技计划重大专项(2006C11105)
收稿日期:2007-05-22;**改回日期**:2007-08-01
第一作者简介:刘祖根(1971 ~),男。讲师,2007 年获浙江大学博士学位。主要从事信息安全研究。E-mail: lewissy2005@yahoo.com.cn

的缺点。Westfeld 等人应用“χ^2 检验”的方法对 EzStego 算法[1]进行隐写分析[2]。Fridrich 等人利用奇偶分析(RS)算法和“样本对分析”算法对 EzStego 算法及其改进算法进行了针对性研究[3-4]。Dumitrescu 等人给出了 RS 算法的理论分析[5]。Lyu 等人应用基于小波域特征向量的盲检测算法来测试 GIF 格式图像中是否存在利用 EzStego 隐藏的信息[6];然而,因为分解到小波空间不可避免地损失了 GIF 格式图像中隐藏数据的特定结构和相关信息,所以 Lyu 等人的算法对 EzStego 的检测率较低、误检率较高。

针对网络上传输的大量 GIF 格式图像都采用类似“样本对分析”的特定隐写分析方法进行分析,显然无法应对层出不穷、变化多端的新信息隐藏技术。更为重要的是,特定隐写分析方法无法满足对高速网络进行高效、实时监控的实用性要求。本文在分析 GIF 格式图像现有隐秘术的实现技术的基础上,提出了一种基于“图像子块距离和”的盲隐写分析算法。该盲隐写分析算法是根据图像子块“距离和”的概念、最佳奇偶分配的思想和图像子块中有不同颜色数的概念,从图像中抽取多种统计特征,并应用“支持向量机”分类算法来实现隐写分析。

2 用于 GIF 格式图像的信息隐藏技术

2.1 在调色板中隐藏信息

根据信息嵌入的方式,在调色板中隐藏信息的技术又分为修改调色板颜色的最不重要位(LSB)和改变调色板中颜色顺序嵌入信息 2 种实现手段。因为通过改变调色板颜色的 LSB 位来实现信息隐藏的技术具有更为有限的信息容量(至多 3 × 256 bits),所以其应用较少。GIFShuffle 算法[7]是通过改变调色板中颜色顺序的方式在 GIF 格式图像中嵌入信息的一个例子。该算法的优点是不会修改图像;缺点是非常脆弱,即重新存储会丢失其中隐藏的秘密信息(因许多图像处理软件都会对调色板按照颜色值排序)。此外,该算法在一幅 GIF 格式图像中最多可嵌入 210 Byte 的信息,信息容量有限,并且调色板中“无序”的颜色序列很容易引起怀疑。

2.2 在图像数据中隐藏信息

2.2.1 减少颜色深度再扩展

S-Tools 算法是采用减少颜色深度和再扩展的方法在图像数据中嵌入信息的[8],即先将 256 色折叠到 128 色;然后通过“包含近邻颜色(改变蓝色信道的 LSB)”的方式将这 128 色扩展为 256 色;最后将二进制信息嵌入到随机选择像素位置的蓝色信道的 LSB 中。当从隐密图像中恢复信息时,只需要抽取出蓝色信道的 LSB 即可。

2.2.2 利用调色板重排序的索引值来隐藏信息

EzStego 算法的信息嵌入机制是该方法的体现[1]。EzStego 算法首先对调色板按照亮度进行排序;然后将位置紧邻的 2 个颜色索引值的“奇偶位”用来表示二进制的“0”和“1”;最后秘密信息被嵌入到顺序选择的图像索引值中。该方法的特点是不改变调色板中的颜色值。

2.2.3 利用颜色奇偶位隐藏信息

Fridrich 等人提出了最佳奇偶分配(OPA)法[9],该方法的设计基于这样的假设:距离最近的两个颜色被赋给相对的奇偶位时,因嵌入信息导致的能量变化最小。假设图像的调色板中包含 c_1, $c_2,\cdots,c_N$ 共 N 种不同颜色,且颜色的奇偶位用 ω_i ($\omega_i \in \{0,1\}$)表示,则最佳奇偶分配的步骤如下:

① 在 RGB(或 YUV)空间计算颜色对之间的欧氏距离 $d_{i,j}=|c_i-c_j|$,设集合 $\boldsymbol{C}$ 为“空”。

② 按升序对距离进行排序得到距离序列 $\{d\}=d_{i(1)j(1)}\leqslant d_{i(2)\,j(2)}\leqslant\cdots$。

③ 选择距离序列 $\{d\}$ 中的第 1 个距离 $d_{k,l}$,并将它从 $\{d\}$ 中删除。如果 $c_k\notin\boldsymbol{C}$,并且 $c_l\notin\boldsymbol{C}$,则将第 k 个颜色 c_k 和第 l 个颜色 c_l 的奇偶位分别设置为 0 和 1(或相反),并将 c_k 和 c_l 加入集合 $\boldsymbol{C}$。如果 $c_k\notin\boldsymbol{C}$,而 $c_l\in\boldsymbol{C}$,则置 $\omega_k=1-\omega_l$,并将 c_k 加入集合 $\boldsymbol{C}$;反之,置 $\omega_l=1-\omega_k$,将 c_l 加入集合 $\boldsymbol{C}$。

④ 重复步骤③,直到 $\boldsymbol{C}$ 中包含 N 种颜色。

按照上述步骤改变调色板中的颜色后,在嵌入信息时,再比较嵌入位和被选择索引值指向颜色的奇偶位,如果二者相同,则无需进一步操作;否则,将该索引值改为“OPA”序列中,其对应颜色的最近邻颜色的索引值。如果需要从隐密图像中恢复“秘密”信息,那么只需将那些嵌入像素位置的颜色“奇偶位”依次取出即可。

2.2.4 更安全的信息隐藏方式

张新鹏等人指出,OPA 算法在嵌入信息时,由于“最近邻颜色”产生机制的缺陷,可能会产生“奇异”颜色[10],即类似“颜色 c_1 可转换成 c_2,而没有颜色又会转换成 c_1”的异常情况,若使用“针对性”的隐写分析算法来考察图像中“奇异”颜色的统计概

率时,则可能比较容易检测到利用 OPA 算法产生的隐密图像。张新鹏等人的改进方案是使用同“奇异”颜色的“奇偶位”不同,且欧氏距离最近邻的颜色指向它。当需要将与“奇异”颜色的“奇偶位”相同的“秘密”信息位嵌入该颜色时,则可随机选择“奇异”颜色或用另一颜色替代它。

2.2.5　嵌入信息的位置选择

在将信息嵌入图像时,可用顺序、随机和自适应 3 种方式来选择嵌入位置。其中,顺序方式就是在图像中按“行”或者“列”的顺序,依次对每个像素亮度或者索引嵌入信息,顺序嵌入的特点是变化集中发生在图像数据的首部;随机方式是使用关键字产生的随机数序列指示用于嵌入信息的像素或索引序列,使用随机数序列的优点是可以将“秘密”信息均匀地嵌入到图像中。Fridrich 等人提出的“自适应”算法[9]是与载体图像质量相关的信息嵌入方式。同前述算法比较,“自适应”算法的不同之处是,选择嵌入信息像素的方式,即先给出“好”像素的如下定义:当一个 2×2 pixels 的图像子块中至少具有 3 种不同颜色时,则该图像子块是“好”的;只有一个 3×3 pixels 的图像子块包含的 4 个 2×2 pixels 的图像子块都是“好”图像子块时,该 3×3 pixels 的图像子块中心的像素才是“好”像素。应用自适应方式嵌入信息时,先从图像中选择“好”像素集合,然后用随机数序列选择该集合中的像素用于嵌入信息。

2.2.6　隐秘术例子

利用 Ezstego 和 OPA 隐藏数据方式和选择嵌入位置方法组合,即可得到表 1 所示的 5 种隐秘术。

表 1　实验中测试的隐秘术

Tab. 1　Steganographies tested in experiments

隐秘术名称	数据嵌入方式	像素选择方式
EzStego	改变索引值	顺序
EzStego_RAN	改变索引值	随机
EzStego_ADA	改变索引值	自适应
OPA_RAN	改变颜色	随机
OPA_ADA	改变颜色	自适应

3　基于图像子块距离和的特征

3.1　“图像子块距离和”定义和计算方法

在一个分辨率为“$N \times N$”的“图像子块”中嵌入一个信息“位”时(不失一般性,假设在左上角像素 P 的位置嵌入),在肉眼可分辨的情况下,将像素颜色改变为其空间位置的“邻域”内的其他颜色时,其引起怀疑的可能性更小;因此该像素颜色将变为其他 N^2-1 个像素颜色之一(而在 GIF 格式的图像中则为颜色索引值的变化),而像素 P 的颜色变为“图像子块”中其他颜色时的“距离和(SOD)”,则可用下式表示:

$$f_{NN} = \sum_{i=1}^{N}\sum_{j=1}^{N} |v(1,1) - v(i,j)| \qquad (1)$$

式中,对 GIF 格式的图像而言,$v(i,j)$ 表示图像中位置 (i,j) 处的索引值。“图像子块距离和”的物理意义是反映“图像子块”内因嵌入信息而导致的变化。

3.2　“正距离和”和“负距离和”

由像素 P 的颜色 c 改变为“图像子块”中的其他颜色 $\tilde{c}$,可能是“减小”,也可能是“增大”的变化。而将所有因“减小”变化得到的“距离”累加在一起,便得到“正距离和”p_{NN};反之,就得到“负距离和”n_{NN}。为更精确地捕捉隐藏信息对“图像子块”的影响,将“距离和”分为 p_{NN} 和 n_{NN}2 部分。

3.3　“主距离和”和“次距离和”

如果将式(1)中“取绝对值”的符号去掉,则可得到“正距离和”和“负距离和”的代数和 $\hat{f}_{NN}$。$\hat{f}_{NN}$ 反映了颜色 c 变为其他颜色 $\tilde{c}$ 的总趋势是“减少”还是“增加”,这就是像素 P 所在的“$N \times N$ 分辨率的图像子块”的性质。$\hat{f}_{NN}$ 符号为“正”时,由于“正距离和”代表了变化的“主要”趋势,因而是“主距离和”m_{NN};而“负距离和”代表的则是变化的“次要”趋势,所以是“次距离和”s_{NN}。反之,“负距离和”则是“主距离和”,而“正距离和”则成为“次距离和”。

3.4　用于计算特征向量的统计量

N 值分别取为 2 和 3,用于计算前述各种“距离和”。实验表明,对于 3×3 pixels 的图像子块,像素 P 选择为左上角位置时的检测性能比选择位于“中心”位置的像素更好。“2×2 pixels 的图像子块”的像素 P 也选择为左上角位置。由 2.1 节和 2.2.3 节可知,因为很多隐秘术在嵌入信息过程中会改变调色板,所以根据 GIF 格式图像的索引值计算“距离和”时,要先对调色板排序,并将图像中的索引值转换成颜色在“排序后调色板”中的索引值。

下面给出统计量的计算公式。为方便叙述,将 f_{NN} 表示为式(2),用于计算左上角坐标位置为 (a,b) 的“$N \times N$ pixels 大小的图像子块”的距离和。

$$f_{NN}(a,b) = \sum_{i=1}^{N}\sum_{j=1}^{N} |v(a,b) - v(a+i-1,b+j-1)| \quad (2)$$

$\hat{f}_{NN}$、p_{NN}、n_{NN}、m_{NN}和s_{NN}的计算方法与此类似。

3.4.1 1维统计量

f_{NN}和$\hat{f}_{NN}$在整幅图像中的分布状态计算公式如下：

$$\boldsymbol{h}_{NN}[x,\alpha,\gamma] = \sum_{i=1}^{R-1}\sum_{j=1}^{C-1}\varphi(x,\alpha)\cdot\varphi(\tau,\gamma) \quad (3)$$

式中，$0\leqslant\alpha\leqslant765$，$0\leqslant\gamma\leqslant1$，$x=f_{NN}$或$\hat{f}_{NN}$，$\varphi(x,\alpha)$和$\varphi(\tau,\gamma)$的更一般形式是$\varphi(\alpha,\beta)$，当$\alpha=\beta$时，则$\varphi(\alpha,\beta)$值为“1”，否则为“0”；$\tau$是位置$(i,j)$处索引$I(i,j)$指向的颜色的奇偶位；$\gamma$用来将SOD按照颜色奇偶位分为2类。用$R$和$C$表示的灰度图像的分辨率是“$R\times C$”，图像中每个像素索引值用“8 bits”二进制信息表示。例如，在$x=f_{22}$，并且$\gamma=0$时，则用式(3)即可计算所有2×2 pixels图像子块左上角索引指向的颜色为偶数的f_{22}的分布状态，从而得到8个1维统计量。

3.4.2 2维统计量

使用“共生”矩阵$\boldsymbol{H}_{NN}[\alpha,\beta,\gamma]$计算一个像素位置处“正距离和”和“负距离和”同时出现的分布。

$$\boldsymbol{H}_{NN}[\alpha,\beta,\gamma] = \sum_{i=1}^{R-1}\sum_{j=1}^{C-1}\varphi(p_{NN},\alpha)\cdot\varphi(n_{NN},\beta)\cdot\varphi(\tau,\gamma) \quad (4)$$

式中，$0\leqslant\alpha,\beta\leqslant765$，$0\leqslant\gamma\leqslant1$。

当α和β从0变化到765时，即可在被处理图像的同一位置(i,j)计算得到“正距离和”p_{NN}和“负距离和”n_{NN}。当i从1变化到$R-1$，并且j从1变化到$C-1$时，就可得到图像中p_{NN}和n_{NN}的共生矩阵。τ和γ的定义同式(3)。在N和γ变化时，利用式(4)即可计算4个2维统计量。

$\boldsymbol{G}_{NN}[X_{NN},\alpha,\beta,\gamma]$是计算水平位置邻接的2个“图像子块”距离和$X_{NN}$的共生矩阵。

$$\boldsymbol{G}_{NN}[X_{NN},\alpha,\beta,\gamma] = \sum_{i=1}^{R-1}\sum_{j=1}^{C-2}\varphi(X_{NN}(i,j),\alpha)\cdot\varphi(X_{NN}(i,j+1),\beta)\cdot\varphi(\tau,\gamma) \quad (5)$$
$$0\leqslant\alpha,\beta\leqslant765,0\leqslant\gamma\leqslant1$$

式中，X_{NN}等于f_{NN}、$\hat{f}_{NN}$、m_{NN}和s_{NN}四者之一，α、β、τ和γ的定义同式(4)。在X_{NN}表示f_{NN}，且N和γ变化时，即可计算4个2维统计量。因此，式(5)可用于计算16个2维统计量。

$\boldsymbol{Q}_{NN}[\alpha,\beta,\gamma]$是计算图像中相同像素位置处$f_{NN}$和$\hat{f}_{NN}$的共生矩阵，即

$$\boldsymbol{Q}_{NN}[\alpha,\beta,\gamma] = \sum_{i=1}^{R-1}\sum_{j=1}^{C-1}\varphi(f_{NN},\alpha)\cdot\varphi(\hat{f}_{NN},\beta)\cdot\varphi(\tau,\gamma) \quad (6)$$

式中，$0\leqslant\alpha\leqslant765$，$-765\leqslant\beta\leqslant765$，$0\leqslant\gamma\leqslant1$，$\alpha$、$\beta$、$\tau$和$\gamma$的定义同式(3)，因此，式(6)可用于计算4个2维统计量。

3.5 特征值计算

利用3.4节中的相关公式即可得到8个直方图和24个共生矩阵这样32个统计量。再求这些统计量的“直方图特征函数”(HCF)的“块中心”(COM)[11-12]，就得到了相应的特征。由直方图和共生矩阵计算特征的公式如下：

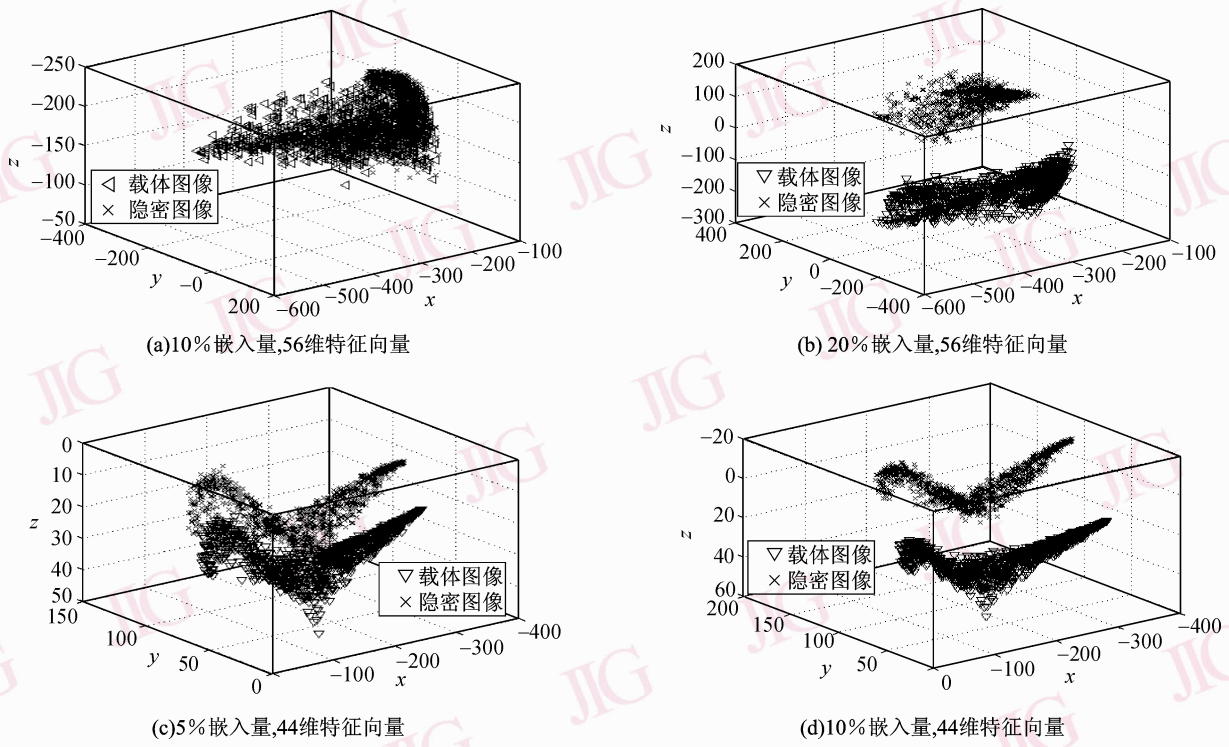
$$\boldsymbol{M}_1 = \frac{\sum_{k=0}^{K/2-1}k\cdot a(k)}{\sum_{k=0}^{K/2-1}a(k)} \quad (7)$$

$$\boldsymbol{M}_2 = \frac{\sum_{k_1=0}^{\zeta/2-1}\sum_{k_2=0}^{\eta/2-1}(k_1,k_2)\cdot a_2(k_1,k_2)}{\sum_{k_1=0}^{\zeta/2-1}\sum_{k_2=0}^{\eta/2-1}a_2(k_1,k_2)} \quad (8)$$

式中，$a=|\mathrm{DFT}(\boldsymbol{h})|$，DFT表示“1维离散傅里叶变换”，$a(k)$表示与频率$k$对应的振幅；$K$是频率最大值，由于DFT具有对称性，因此只需要计算范围$(0,K/2-1)$内的统计矩即可得COM；$a_2=|\mathrm{DFT}_2(\boldsymbol{h}_2)|$，$\mathrm{DFT}_2$表示“2维离散傅里叶变换”，用于计算在$k_1$和$k_2$这2个方向的“块中心”。这样从32个统计量即可得到56维特征向量。

4 改进统计量的计算方法

由图1(b)可见，56维特征向量的方法可将载体图像同其隐密图像完全分开。其中的载体图像是1 096幅CorelDraw图像，隐密图像是采用OPA_RAN方法嵌入图像最大容量的20%信息后得到的。其中，三角形代表载体图像，叉号代表隐密图像。这里图像的最大容量用每个像素位置嵌入一个二进制位表示，即每个索引值嵌入1 bit。由图1(a)可见，嵌入10%的信息时，“56维特征向量”方法的区分



(a)10%嵌入量,56维特征向量　(b) 20%嵌入量,56维特征向量

(c)5%嵌入量,44维特征向量　(d)10%嵌入量,44维特征向量

图 1　1 096 幅 CorelDraw 图像及其隐密图像的特征云图

Fig. 1 Clouds of features from 1 096 CorelDraw covers and their stegos

能力变得很差。图 1(a)和图 1(b)的得到过程如下:首先用“主元分析法”将一幅图像的 56 维特征向量降为 3 维,使之对应空间坐标系中 x、y 和 z 轴的坐标,该图像即可表示为按 3 个坐标值画出的一点;然后将两类图像对应的特征均依此办理,每幅图像对应空间坐标系中一点,即得到图 1 所示的“特征云图”。

为得到更好的分类效果,本文考虑了“图像子块”中不同颜色的个数。也就是说,式(3)中的 $\varphi(\tau,\gamma)$ 将 SOD 按照图像子块中不同索引数进行分布;此时,τ 表示像素 P 所在的当前子块中不同索引值的个数,γ 值在 1 到 $N\times N$ 之间变化(2 × 2 pixels 大小的图像子块对应为 4,3 × 3 pixels 大小的图像子块对应为 9)。考虑到更高维的统计量可能具有更好的区分效果,因此可将式(3)看作是关于 α 和 γ 的 2 维统计量。在 $x=f_{N,N}$,且 $N=2$ 时,α 和 γ 分别在范围 $0\leqslant\alpha\leqslant765$ 和 $1\leqslant\gamma\leqslant4$ 之间变化;同时,利用式(3)可得到 $f_{2,2}$ 的 2 维统计量。当 x 和 N 变化时,则可利用式(3)得到 4 个“2 维统计量”。类似地,可利用式(4)~式(6)得到 12 个“3 维统计量”。若先使用式(8)计算 2 维统计量的特征值,然后用式(9)计算 3 维统计量的特征值,则最后可得到一个 44 维的特征向量,

$$\boldsymbol{M}_3=\frac{\sum_{k_1=0}^{\zeta/2-1}\sum_{k_2=0}^{\eta/2-1}\sum_{k_3=0}^{\xi/2-1}(k_1,k_2,k_3)\cdot a_3(k_1,k_2,k_3)}{\sum_{k_1=0}^{\zeta/2-1}\sum_{k_2=0}^{\eta/2-1}\sum_{k_3=0}^{\xi/2-1}a_3(k_1,k_2,k_3)} \tag{9}$$

式中,$a_3=|\mathrm{DFT}_3(\boldsymbol{h}_3)|$,$\mathrm{DFT}_3$ 表示“3 维离散傅里叶变换”,$\boldsymbol{h}_3$ 表示“3 维统计量”。

图 1(c)和图 1(d)分别给出了采用 OPA_RAN 方法嵌入“最大容量”的 5% 和 10% 的信息时,载体图像和隐密图像的特征云图。由该图可以看出,“44 维特征向量”对信息嵌入量为 5% 的情况已经具有很好的可分性;当嵌入信息为“最大容量”的 10% 时,则载体图像和隐密图像之间的可分性更好。对比图 1(a)和图 1(d)可见,44 维特征向量对 OPA_RAN 隐秘术产生的隐密图像具有更好的区分性。

5　实验组织和结果数据分析

5.1　图像库和针对的隐秘术

5.1.1　图像库

CorelDraw 软件[13]的 10.0 版 CD#3 中包含有以 WI 格式存储的 1 096 幅分辨率为 512 × 768 pixels

或 768×512 pixels 的彩色图像,图像的内容有休闲、处所、动物、食物、风景和建筑等。如果先使用 Corel Photo Paint 10 软件[13]将这些图像批处理转换为彩色 BMP 图像,然后使用 Matlab[14]中的 rgb2gray. m 和 gray2ind. m 程序将其转换为灰度 GIF 格式图像,则可得到载体图像库。

5.1.2 隐秘术

本文测试的隐秘术如表 1 所示。此外,还测试了 GIFShuffle[7]。

5.2 实验组织和测试结果

5.2.1 隐密图像的产生

利用 GIFShuffle[7]在灰度 GIF 格式的图像中嵌入信息时,图像的最大容量是 210 Byte(lb (256!)/8)。在图像中应用隐秘术能够隐藏数据的最大容量是,每个像素隐藏"1 bit"二进制信息。使用"自适应"方式能够选择的嵌入像素的个数取决于图像的质量,这从客观上限制了嵌入信息的容量。然而,为与相关研究保持可比性,本文仍以 bpp(一个像素嵌入 1 bit)的最大嵌入容量标准为基准来衡量隐秘术选择的"嵌入信息量"。

产生隐密图像的方式有以下 2 种:(1)采用 GIFShuffle 隐藏信息时,嵌入信息量分别为最大信息量的 50% (105 Byte)和 100% (210 Byte);(2)采用其他隐秘术时,可分别嵌入最大嵌入量("像素数"个位)的 5%、10%、15% 和 20% 的信息。利用 EzStego_ADA 隐秘术嵌入信息时,可分别得到 1 096、1 093、1 086 和 1 076 幅隐密图像;而利用 OPA_ADA 隐秘术嵌入信息时,则可分别得到1 096、1 095、1 092 和 1 087 幅隐密图像。利用其他隐秘术嵌入信息时,每幅载体图像均能产生对应的隐密图像。

5.2.2 实验中采用的对比"隐写分析"算法

用于对比的算法分别是:RS 算法[3]、"样本对分析"算法[4]和 Lyu 等人提出的 72 维特征向量算法[6]。为体现对比的公平性,均采用 LibSVM[15]这一"支持向量机(SVM)"软件来训练特征向量。训练用的 SVM 类型设置为"C_SVC",核函数选为 RBF (radial basis function),训练时,先使用 LibSVM 程序包中的工具 grid. py,通过 5 重交叉验证得到 RBF 参数 γ 和 C 的值;然后使用达到最大检测精度的 γ 和 C 值来完成训练取得模板,并进行开放测试。

5.2.3 训练和测试方案

在进行模式分类相关的研究中,为保证测试结果可信,"开放测试"样本数必须大于或等于所采用特征向量维数的 10 倍。假设特征向量的维数是 x,而采用某种隐秘术嵌入某一定量信息后得到的隐密样本数用 Y 表示,则用于训练的样本对的个数是集合$\{100, 200, \cdots, Y-10x\}$中的元素之一;剩下的样本用于"开放测试"。

5.2.4 测试结果

表 2 是几种隐写分析算法的测试结果(以"检测率/误检率"衡量)。从表 2 可见,RS 算法已能以高检测率、低误检率攻击 GIFShuffle 隐秘术;然而,在嵌入信息量较少的情况下,RS 算法几乎不能检测其他隐秘术产生的隐密图像。"像素对分析"(PairAnalysis)算法虽然对大多数隐秘术的误检率较低,然而检测率也较低。Lyu 等人提出的算法对不同格式图像中的许多隐秘术进行检测均获得了令人印象深刻的检测性能;在检测 EZStego、EZStego_RAN 和 EzStego_ADA 隐秘术产生的图像时,其性能比 RS 算法和像素对算法更好;它攻击 EzStego_ADA 隐秘术产生的图像的效果甚至比本文算法更好。

由 RS 算法和"像素对分析"算法的比较结果可见,56 维特征向量算法可更高效地攻击 6 种隐秘术。同 Lyu 等人提出的算法比较,56 维特征向量算法对 EzStego_ADA 隐秘术的检测性能差一些,但对其他 5 种算法的检测效果更好。44 维特征向量算法相对 56 维特征向量算法可获得更好的分类效果。

图 2 为 5 种隐写分析算法对 OPA_RAN 隐秘术

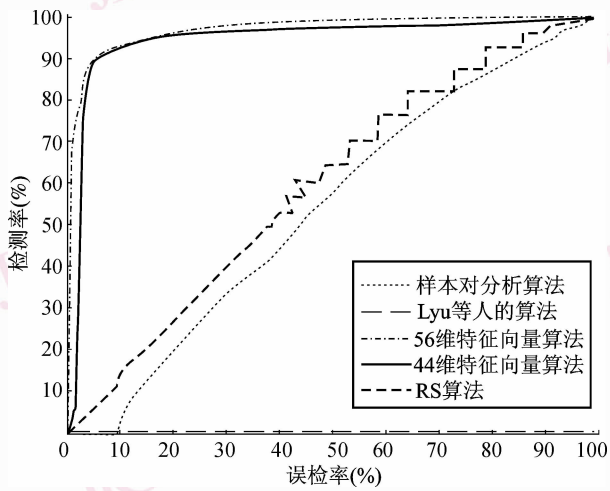


图 2 5 种隐写分析算法对 OPA_RAN 隐秘术的 ROC 图

Fig. 2 ROC figure of 5 steganalytic techniques for OPA_RAN steganography

表 2　实验检测结果

Tab. 2　Detecting results in experiments

隐秘术算法	嵌入率	几种隐写分析算法的检测率 / 误检率(%)				
		RS 算法	PairAnalysis 算法	Lyu 的算法	56 维特征向量	44 维特征向量
GIFShuffle	50	90.07/16.85	47.89/5.72	49.22/49.22	82.7/ 5.03	82.76/ 3.16
	100	88.76/6.33	54.92/3.92	49.22/49.22	100/ 0	100/ 0.2
EZStego	5	89.32/81.03	55.12/22.19	59.34/35.06	67.2/25.13	79.02/ 13.26
	10	92.28/57.05	46.39/6.73	74.12/31.4	68.2/11.81	81.2/ 4.87
	15	91.06/38.65	45.98/4.12	80.53/22.74	76/ 7.66	88.42/ 3.69
	20	94.6/36.31	74.66/20.64	80.92/21.65	81.4/ 5.15	90.77/ 4.36
EZStego_RAN	5	96.89/96.29	7.53/5.22	76.26/22.99	74/ 22.99	86.75/ 10.4
	10	89.86/80.52	9.43/5.32	88.94/19.1	84.05/ 13.57	92.82/ 6.61
	15	93.98/78.31	11.35/4.72	91.33/15.58	89.29/11.83	92.52/ 5.03
	20	92.57/54.82	11.35/3.51	87.19/9.3	91.46/ 7.54	96.55/ 5.75
EZStego_ADA	5	97.39/96.08	30.15/27.64	64.84/34.26	27.81/26.4	69.8/ 66.4
	10	92.94/87.64	33.73/25.13	77.55/25.6	62.74/49.85	58.34/ 40.64
	15	89.76/71.5	45.39/29.69	82.06/21.37	63.23/37.66	68.08/ 31.92
	20	90.97/56.77	41.67/23.63	84.79/17.01	70.62/30.41	74.56/ 30.92
OPA_RAN	5	33.42/34.3	4.32/2.71	50.83/42.79	81.47/21.43	90.1/ 7.4
	10	9.06/7.89	5.62/3.01	62.44/42.71	80.22/7.93	95.83/ 4.74
	15	86.06/85.05	7.03/3.79	69.6/36.68	93.97/7.29	97.27/ 3.3
	20	83.43/78.31	10.78/5.6	72.11/31.53	96.1/7.04	97.56/ 2.59
OPA_ADA	5	85.23/85.07	1.0/1.0	53.68/46.76	63.9/43.84	78.19/ 30
	10	96.47/96.47	98.88/98.77	62.01/44.91	71.82/30.4	84.17/ 15.4
	15	43.07/39.53	7.2/7.7	57.62/40.25	78.66/24.1	89.7/ 7.26
	20	30.24/32.02	4.96/5.07	61.88/39.14	84.1/19.9	90.97/ 5.11

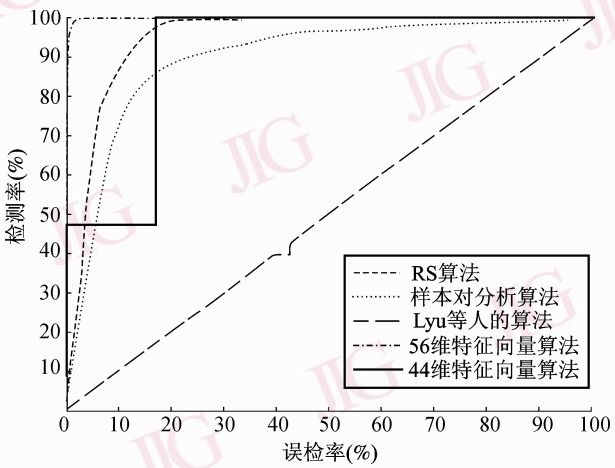


图 3　5 种隐写分析算法对 Gif_shuffle 隐秘术的 ROC 图

Fig. 3　ROC figure of 5 steganalytic techniques for Gif_shuffle steganography

嵌入最大信息量的 20% 信息后的隐密图像进行检测的 ROC(receive operating characteristic) 曲线。图 3 是 5 种隐写分析算法检测 GIFShuffle 隐秘术嵌入最大量信息后的隐密图像的 ROC 曲线。两图直观地反映了表 2 中对应“行”的检测性能。

从本文算法的分类性能可得到关于设计 GIF 格式的图像的安全隐秘术的以下 3 个结论:

① 通过打乱调色板实现信息隐藏会导致不安全;

② 通过改变索引实现信息隐藏的隐秘术比通过修改颜色实现信息隐藏的隐秘术更安全。

③ 在顺序、随机和自适应 3 种“嵌入位置”选择方法中,自适应法最安全,而顺序法最不安全。

5.3 特征向量中各种统计量对分类结果的贡献

为考察 44 维特征向量的 16 个统计量对分类的贡献,本文检查了这 16 组特征统计量用于区分载体图像和隐密图像的性能。隐密图像是采用 OPA_RAN 算法在 1 096 幅 CorelDraw 载体图像中嵌入最大信息量的 20% 信息后得到的。训练和检测方法同前,表 3 为衡量 16 组统计量的检测效果的"检测率/误检率(TP/FP)"数据。

从大多数统计量的检测结果可见,虽然它们的检测率已经很高,然而误检率也较高。所有统计量的检测率均达到了 97.56% ,而误检率只有 2.59% 。因此,多个特征量结合,在提高检测率的同时,可降低误检率。从表 3 还可看出,由 3×3 pixels 图像子块得到的统计量比由 2×2 pixels 图像子块得到的统计量更高效。

表 3 16 组统计量对分类的贡献

Tab. 3 Constribution of 16 statistics for classification

统计量	TP/FP (%)
$\boldsymbol{h}_{22}[f_{22},\alpha,\gamma]$	97.24/83.42
$\boldsymbol{h}_{22}[\hat{f}_{22},\alpha,\gamma]$	86.68/44.35
$\boldsymbol{H}_{22}[\alpha,\beta,\gamma]$	80.32/33.94
$\boldsymbol{G}_{22}[f_{22},\alpha,\beta,\gamma]$	75.50/49.00
$\boldsymbol{G}_{22}[\hat{f}_{22},\alpha,\beta,\gamma]$	80.82/10.04
$\boldsymbol{G}_{22}[m_{22},\alpha,\beta,\gamma]$	74.20/15.86
$\boldsymbol{G}_{22}[s_{22},\alpha,\beta,\gamma]$	61.31/35.55
$\boldsymbol{Q}_{22}[\alpha,\beta,\gamma]$	52.21/3.51
$\boldsymbol{h}_{33}[f_{33},\alpha,\gamma]$	79.92/40.36
$\boldsymbol{h}_{33}[\hat{f}_{33},\alpha,\gamma]$	88.25/29.22
$\boldsymbol{H}_{33}[\alpha,\beta,\gamma]$	88.17/19.75
$\boldsymbol{G}_{33}[f_{33},\alpha,\beta,\gamma]$	84.80/15.33
$\boldsymbol{G}_{33}[\hat{f}_{33},\alpha,\beta,\gamma]$	90.29/12.83
$\boldsymbol{G}_{33}[m_{33},\alpha,\beta,\gamma]$	87.94/12.06
$\boldsymbol{G}_{33}[s_{33},\alpha,\beta,\gamma]$	61.81/25.25
$\boldsymbol{Q}_{33}[\alpha,\beta,\gamma]$	79.91/16.29

5.4 SOD 是 GIF 载体图像和隐密图像的函数

为什么基于 SOD 的算法在攻击以 GIF 格式的图像为载体的隐秘术时,能得到这样好的分类效果?对于 GIF 格式的图像中的一个索引值来说,其邻近的索引可看作是它的近似值。无疑近邻索引的平均值是它的一个更好的估计量。由于所有索引的估计量形成了与隐密图像对应的载体图像的近似版本,因此,隐密图像中的一个索引的 SOD 是该索引和载体图像中同一位置处索引的函数。由此可见,图像中所有索引的 SOD 是 GIF 载体图像及其隐密版本的函数。综上所述,可以得出以下结论:由 SOD 捕捉到的嵌入信息所导致的差异,使得本文算法可获得非常好的检测性能。

6 结 论

本文提出了 SOD 的概念,并使用 SOD 来构造载体图像和隐密图像之间的函数,同时基于支持向量机设计了两个高效的盲检测算法。

算法的改进可考虑多种特征向量的融合、特征向量的降维,以及高效特征选择方案的研究等。

参考文献(References)

1 Westfeld A, Pfitzmann A. Attacks on steganographic systems: breaking the steganographic utilities EzStego, Jsteg, Stegnos and S-Tools and some lessons learned[A]. In: Proceedings of Information Hiding-Third International Workshop[C], Dresden, Germany, 1999: 61-75.

2 Machado R. EzStego[CP/OL]. 1996, http://www.stego.com, 2006-06-10.

3 Fridrich J, Goljan M, Du R. Detecting LSB steganography in color and gray-scale images[J]. Magazine of IEEE Multimedia Special Issue on Security, 2001, **8**(4): 22-28.

4 Fridrich J, Goljan M, Soukal D. Higher-order statistical steganalysis of palette images[A]. In: Proceedings of SPIE Electronic Imaging[C], Santa Clara, CA, USA, 2003: 178-190.

5 Dumitrescu S, Wu Xiao-lin, Wang Zhe. Detection of LSB steganography via sample pair analysis[J]. IEEE Transactions on Signal Processing, 2003, **51**(7):1995-2007.

6 Lyu S, Farid H. Detecting hidden messages using higher-order statistics and support vector machines[A]. In: Proceedings of 5th International Workshop Information Hiding[C], Noordwijkerhout, Netherlands: Springer-Verlag, 2003: 340-354.

7 Kwan M. GIFShuffle[CP/OL]. 1998, http://www.darkside.com.au/ GIFShuffle/, 2006-06-10.

8 Brown A. S-Tools[CP/OL]. 1998, http://idea.sec.dsi.uimi.it/pub/ security/crypt/code/s-tools3.zip, 2006-06-10

9 Fridrich J, Rui D. Secure steganographic methods for palette images[A]. In: Proceedings of Information Hiding-Third International Workshop[C], Dresden, Germany, 1999: 47-60.

10 Zhang Xin-peng, Wang Shuo-zhong. Detection of OPA stego-data and secure steganography in palette images[J]. Acta Electronica Sinica, 2004, **32**(10): 1702-1705.[张新鹏,王朔中. 对 OPA 密写的检测和增强安全性的调色板图像密写方案[J]. 电子学报, 2004, **32**(10):1702-1705.]

11 Harmsen J, Pearlman W. Steganalysis of additive noise modelable information hiding[A]. In: Proceedings of SPIE Electronic Imaging 5022[C], Santa Clara, CA, USA, 2003: 21-24.

12 Harmsen J, Bowers K, Pearlman W. Fast additive noise steganalysis[A]. In: Proceedings of the SPIE International Society for Optical Engineering[C], San Jose, CA, USA, 2004, **5306**, 489-495.

13 CorelDraw image library[DB/OL]. http://www.corel.com, 2006-03-12.

14 MATLAB[CP/OL]. http://www.mathworks.com/, 2005-09-20.

15 Chang Chih-chung, Lin Chih-jen. LIBSVM: a library for support vector machines, 2001 [EB/OL]. http://www.csie.ntu.edu.tw/~cjlin/LibSVM, 2005-09-20.