

一种针对图像隐写软件的图谱评估方法^{*}

刘振华, 翟卫东, 吕述望, 陈庆元

(中国科技大学研究生院信息安全国家重点实验室, 北京 100039)

摘要: 提出一种基于图像统计特征的图谱评估方法, 可以有效地对图像隐写软件性能进行评估, 而且该方法准确稳定, 简单实用。

关键词: 信息隐藏; 隐写; 隐写软件; 图谱评估法

中图分类号: TN911.73 **文献标识码:** A **文章编号:** 0529-6579 (2004) S2-0076-04

20 世纪 90 年代中期以来, 随着计算机及互联网技术的高速发展, 信息隐藏技术得到了迅猛发展, 隐写及隐写分析技术作为其主要分支也得到了空前发展, 相关论文见诸于各种学术期刊, 多种隐写算法、隐写软件出现在互联网上, 可以十分方便地下载。那么, 诸多隐写软件当中, 性能孰优孰劣, 目前国内外尚无统一的、准确的评估标准。本文提出一种利用图像的统计特性、针对图像类隐写软件进行评估的“图谱”评估方法, 该方法揭示了图像隐写软件的固有特性, 操作简单, 实用性强, 评估效果准确稳定。

1 原理及方法简介

数字图像由像素构成, 相邻像素之间具有一定的相关性, 如何有效测度像素之间的相关性是检测图像是否“含隐”的基础, 也是图像隐写软件性能评估的基础。

设一 $M \times N$ 像素点的离散图像 X 在位置 (m, n) 的像素灰度值为向量 $X(m, n)$ (其中 M 为行数, N 为列数, $m = 1, 2, \dots, M, n = 1, 2, \dots, N$)。对于 24 位彩色图像而言,

$$X = (X_r(m, n), X_g(m, n), X_b(m, n))$$

其中, 3 个分量 $X_r(m, n), X_g(m, n), X_b(m, n)$ 分别代表位置 (m, n) 的像素点红、绿、蓝 3 色的不同灰度值, 颜色不加区分时, 可省略下标, 各分量均简记为 $X(m, n)$ 。图像非边界像素点 (也称中心像素点, 用 “*” 表示) 有 8 个相邻像素点 (用 “o” 表示), 如图 1 (a)。相邻像素点与中心像素点灰度值 $X(m, n)$ 之差, 从左上角按顺时针顺序分别为

$$X(m-1, n-1) - X(m, n), \dots, \\ X(m, n-1) - X(m, n)$$

简记为

$$U_1(m, n), U_2(m, n), \dots, U_8(m, n)$$

也可记为向量形式 $U = (U_1(m, n), U_2(m, n), \dots, U_8(m, n))$ 。若相邻像素点之中的 t ($t \leq 8$, 且 t 为整数) 个被选取, 则这 t 个像素点称为中心像素点的 t 阶邻域, 图 1 (b) 为中心像素点 $X(m, n)$ 的 4 阶邻域, 记为

$U = (U_2(m, n), U_4(m, n), U_6(m, n), U_8(m, n))$ 。若 $U(m, n)$ 中 t 个分量值相等, 则称其为 t 阶等邻域, 中心像素点称为 t 阶等邻域点。若 t 阶等邻域中各相邻像素点均为奇(偶)数, 则称其为 t 阶奇(偶)等邻域, 中心像素点也称为 t 阶奇(偶)等邻域点。等邻域中, 若 $U_i < 0$, 则称中心像素点为 T 点; 若 $U_i > 0$, 则称为 A 点。

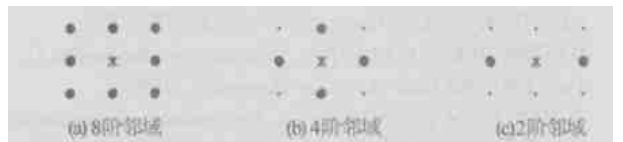


图 1 部分常用 t 阶邻域

Fig 1 some useful t -rank neighborhood

可以将差值、奇偶性不同的等邻域点的频次记为 S_{ij} , 其中 i 表示差值, j 表示奇偶性 ($j = 0$ 表示偶等邻域点; $j = 1$ 表示奇等邻域点), 则等邻域点中应包括如下 4 类: 偶等 T 点 ($S_{i0}, i < 0, S_{T0}$); 偶等 A 点 ($S_{i0}, i > 0, S_{A0}$); 奇等 T 点 ($S_{i1}, i < 0, S_{T1}$); 奇等 A 点 ($S_{i1}, i > 0, S_{A1}$)。

* 收稿日期: 2004-08-18

基金项目: 国家“973”重点基础研究发展规划项目 (TG1999035804)

作者简介: 刘振华 (1941 年生), 女, 教授; E-mail: zhenhualiu@ustc.edu.cn

由文[1, 2] 可知, 向量 U 近似服从广义高斯分布, 其概率密度函数呈对称分布, 对称点为均值, 且均值为 0。对于原始图像, 有结论:

$$S_{-j} \approx S_{ij},$$
$$i = 0, 1, 2, \dots, 255, j = 0, 1 \quad (1)$$

目前一般隐写软件的作业模式为代替作业模式, 即用秘密信息比特来取代 (代替) 图像相应比特的模式。在代替作业模式隐写过程中, 有如下结论:

随着秘密信息嵌入量的增加, 图像原本保持统计平衡的等邻域点中 (如 (1) 式) 的奇等 A 点和偶等 T 点数量增加。这些增加的等邻域点与影响隐写嵌入效果的三因素之一的隐写嵌入算法具有强相关性, 而与其它两个因素即秘密信息和载体图像相关性较弱。

利用这个与隐写嵌入算法具有强相关性的统计特性, 可以设计出评估隐写软件性能的评估方法, 我们称之为“图谱”评估法。不同的隐写软件在嵌入秘密信息数据时表现出不同的“图谱”, 而载体图像的改变以及所嵌入秘密信息的改变则不足以显著改变“图谱”形状, 所以可以认为图谱特征揭示了隐写算法的固有特性。

以随着嵌入量增加而不断增加的奇等 A 点和偶等 T 点作为统计对象, 构造隐写软件 (算法) 图谱, 秘密信息嵌入率从 0 ~ 100% 等间隔取 n 个点, 统计值记为 p_i ($i = 0, 1, 2, \dots, n - 1$)。然后将含隐位面比特变反统计, 秘密信息嵌入率从 100% ~ 0 等间隔取 n 个点, 统计值记为 p_i ($i = n, n + 1, \dots, 2n - 1$)。构造的图谱与前 n 个点基本保持对称。然后对图谱归一化处理,

$$p'_i = \frac{p_i - p_0}{\max(p_i) - p_0}, i = 0, 1, \dots, 2n - 1$$

处理后即可反映出图像隐写软件的隐写性能。当然, 也可利用诸如斜率均值等方法进一步求出统一的量化值进行评估比较, 总之, 方法多样, 这里不一赘述。

2 实验及结果分析

实验以 $S_{11} + S_{-10}$ 作为统计对象, 秘密信息嵌入率从 0 ~ 100%, 每 5 个百分点采样一次。

理想状态下, 可以得到最优隐写软件图谱和最差隐写软件图谱, 见图 2 和图 3。

图 2 中有 $S_{10} + S_{-11} = S_{-10} + S_{11}$, 即产生的图谱前半部相互重合; 图 3 中除原始载体图像所在点外, 其它任何嵌入率的隐写有 $S_{11} + S_{-10} \gg S_{10} +$

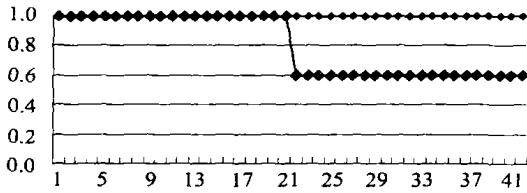


图 2 理想状态最优隐写软件图谱
Fig. 2 The best figure spectrum in ideal state

S_{-11} , 对于产生最差图谱的隐写软件, 可以检测到最少 1 bit 的隐写嵌入。

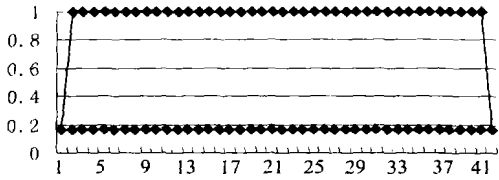


图 3 理想状态最差隐写软件图谱
Fig. 3 The worst figure spectrum in ideal state

这里针对 3 种不同隐写软件 Hide4pgp1.0、2.0 及 stools4.0 (Hide-4pgp1.0 和 2.0 两版软件采用不同隐写算法) 进行图谱估计实验; 载体图像为 2 幅不同的数字图像 ml.bmp 和 water.bmp, 见图 4 和图 5; 因一般隐写软件在秘密信息嵌入图像前都要对其进行压缩或加密处理, 故实验用秘密信息为经混乱处理后的中英文明文数据。对不同图像嵌入不同数量的秘密信息后, 归一化图谱见图 6。



图 4 ml.bmp (480× 640× 24b)
Fig. 4 ml.bmp (480× 640× 24b)

从图 6 中可以看出, 相同的隐写软件, 在不同的载体图像, 嵌入不同的秘密信息后, 所产生的“图谱”相似。大量实验表明了, 不同隐写软件 (算法) 具有不同的图谱, 不随载体图像和嵌入秘密信息的变化而产生显著变化, 可以说图谱不同则反映了隐写软件的不同。另外, 从 2 个不同隐写软件的图谱来看, 图 6 (a) 虽然总体上看曲线变化



图 5 water. bmp (1024× 768× 24b)
Fig. 5 water. bmp (1024× 768× 24b)

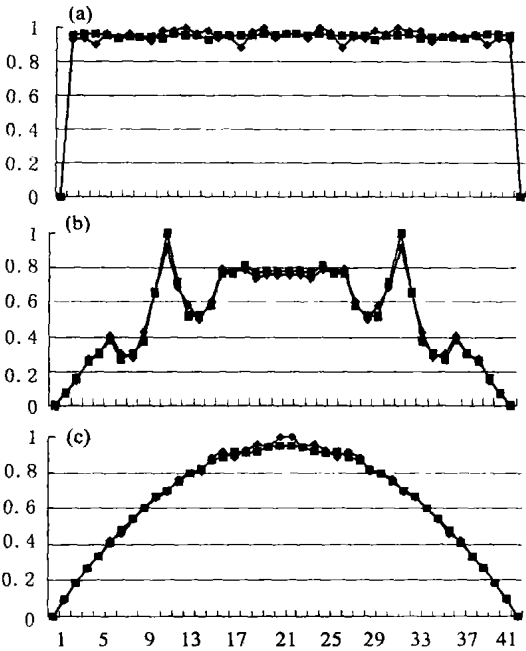


图 6 利用不同软件对 m1. bmp、 water. bmp 隐写产生的归一化图谱
Fig. 6 The unitary figure spectrum of m1. bmp and water which are the stego images that generated from different softwares
菱形为 m1. bmp, 正方形为 water. bmp
(a) hide4pgp1. 0; (b) hide4pgp2 0; (c) stools4. 0

较缓慢, 但由原始载体图像到嵌入秘密消息后的载秘图像的统计值有较大的突变, 统计值与图 6 (b) 的极大值近似。因此可以得出结论, 即 hide4pgp1. 0 显然不如 hide4pgp2. 0 隐写软件 (算法) 的隐写效果好。但 hide4pgp2. 0 (图 6 (b)) 和 stools4. 0 (图 6 (c)) 相比隐写效果哪个更好则很

难直观判断, 为此, 可以进一步计算出斜率均值等参数加以比较, 表 1 为不同隐写软件的斜率均值。可以看出, hide4pgp2. 0 的斜率均值要略小于 stools4. 0, 即其隐写效果更优一些。图 7 为 3 种隐写软件的图谱, 从图中也可看出除个别点外, hide4pgp2. 0 的值均小于 stools4. 0, 更小于 hide4pgp1. 0, 即 3 种隐写软件的隐写效果依据归一化图谱判断, 优劣依次为 hide4pgp2. 0, stools4. 0, hide4pgp1. 0。

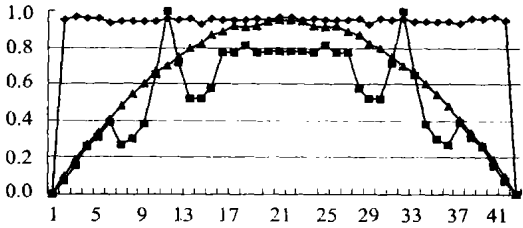


图 7 3 种不同隐写软件归一化图谱
Fig. 7 The different kinds of unitary figure spectrum
菱形为 hid4pgp1. 0; 正方形为 hide4pgp2 0;
三角形为 stools4. 0

表 1 不同隐写软件的斜率均值
Table. 1 The average value of slopes in different Stego softwares

软件名称	斜率均值
Hide4pgp1. 0	0.95
Hide4pgp2. 0	0.54
Stools4. 0	0.65

3 结 论

由上述实验及分析可知, 利用不同隐写软件嵌入图像后表现出的不同“图谱”特性, 可以对不同隐写软件 (算法) 进行有效评估, 从而选择出优质的隐写软件或隐写算法。

参考文献:

[1] 翟卫东, 吕述望, 刘振华. 基于广义高斯分布的彩色图像空域隐写检测算法[J]. 通信学报, 2004, 25(2): 33—42.
[2] 翟卫东, 刘振华, 吕述望. 应用于隐写检测中的几个统计学结论[J]. 通信技术, 2003, 4: 75—77.
[3] FRIDRICH J, GOLJAN M. practical steganalysis of digital images-state of the Art[C]. SPIE Photonics West, 2002, 1: 1—13.

(下转第 82 页)

Digital Image Watermarking Resistant to RST Attacks Based on Feature Points and Self similarities within Images

WANG Li, ZHAO Yao

(Institute of Information Science, Beijing Jiaotong University, Beijing 100044, China)

Abstract: A novel image watermarking scheme based on feature points and the self similarities of the images is proposed. In the embedding, the gravity centers of the 3 most significant bit planes are calculated and construct a feature triangle. According to the watermark bit, we determine the searching area and look for the most similar triangle of the feature triangle. Then the feature triangle is replaced with the matching triangle and thus finish the embedding. In the detection, the feature triangle is obtained and the algorithm search for the most similar one within the whole image. Then the watermark bit can be decided according to the matching triangle position. Experimental results show that the scheme is robust to RST attacks as well as compression, filtering, cropping and additive noise.

Key words: digital image watermarking; robustness; RST attacks; self similarity; feature point

(上接第 78 页)

A Figure Spectrum Estimate Method to Steganography Software in Images

LIU Zhen hua, ZHAI Wei dong, L ÜShu wang, CHEN Qing yuan

(State Key Laboratory of Information Security, Graduate School of USTC, Beijing 100039, China)

Abstract: A figure spectrum estimate method which is based on statistical properties in images is proposed. This method can effectively estimate the properties of steganography software in images and can be implemented conveniently. It can also be produced steady and precise results.

Key words: information hiding; steganography; steganography software; figure spectrum estimate method