基于相邻色的一种隐密分析算法

吴 珅 （上海交通大学软件学院）

摘要：本文着眼于研究检测 jpg 图片的隐写信息。LSB 匹配隐写算法吸引了众多研究者的目光，因为它们很易于实现。相对于 LSB 替换算法，LSB 匹配算法的检测要困难得多，这是由于它的隐写过程没有引入非对称性。本文根据 jpg 图片隐写后相邻色彩数显著增加的统计特性，介绍了平均相邻色彩检测，并且进行了实验，证明了该算法的优越性。

关键词：LSB 匹配 隐秘分析 相邻色彩数

1 引言

隐写术研究的是如何将信息隐藏于一个公开载体中而不被察觉其存在，是一种用于隐藏通信的手段。现代的隐写术的研究是以数字化的音频，视频，图片，文档等各种数字文件作为载体的信息隐藏方法。相对地，隐秘分析是对隐写术的攻击，旨在检测到秘密消息的存在以致破坏隐秘通信，隐秘分析是解决隐写术非法使用的关键技术。近年来恐怖主义频频利用隐写术互通消息，因此，隐秘分析也日益成为信息安全领域的研究热点。

现在国内外研究较多的是空域 LSB 替换隐写算法的隐秘分析方法，针对此隐写算法已有一些研究结果。Westfeld[1] 等最早提出通过分析像素对（PoVs）建立卡方统计量，可以有效地检测出秘密消息的存在性。但这种方法支队连续 LSB 替换算法有效。Fridrich[2] 等利用载密图像中的空域相关性，提出 RS（regular singular）隐写分析算法。Dumitrescu [3] 等基于基本集（primary set，PS）在自然图像模型的基础上建立了完整的 LSB 替换算法的数学模型。张涛等提出了一种基于差分直方图的隐写分析方法。这些方法对空域 LSB 替换隐写算法具有一定的效果，对 LSB 目前，针对 LSB 替换算法很多可靠的检测器。[1] 中最优的检测器可以可靠地检测出隐写率仅为 0.05bits/pixel 的隐藏数据，对于某些适宜的载体图像，隐写率低达.005bits/pixel 的情况也可以检出。虽然这一检测器对于 LSB 替换算法的可以可靠并且敏感地检测出隐藏数据，但是对于 LSB 匹配算法的检测效果就相去甚远了。

本文关注的是以 jpg 彩色图片为载体的空域 LSB 匹配隐写算法的隐秘分析，根据隐写前后图片相邻色个数会发生变化这一特性，引入了平均统计检测算法。并且进行了实验以及相关分析。文章的第二节给出了 LSB 匹配隐写，第三节给出了该隐写算法的检测方法，第四部分为实验和结论结果。

2 LSB 匹配隐写

LSB 隐写是一类常见的隐写技术。其中根据其修改的规则可以分为两类，即 LSB 替换（LSB Replacement）和 LSB 匹配（LSB Matching）。其中 LSB 匹配还被有些作者称之为 plus/minus 1 embedding（增减 1 嵌入）。顾名思义，这种算法不是简单地用秘密数据按测算法被提出。LSB 替换的灰度图象，[3] 中提出的检测器可以可靠位替换掉对应的载体信息的最低有效位，而是将秘密数据与对应的载体信息的最低位进行比较：如果他们互相匹配则保持载体信息不变，如果不匹配的话则载体的对应字节值加 1 或减 1（除非像素值是 0 或者 256 这样的饱和值）。虽然两种算法在嵌入的时候都给载体图像添加了同等级别的噪声，区别在于 LSB 替换时，载体图像偶数值的像素要么保持不变，要么值加 1，但绝对不会减小；奇数值的像素恰恰相反。但是，这种情况在 LSB 匹配算法中则不会出现。而文献[1][2][3] 中的检测器都利用了上述 LSB 替换的这种非对称性。

3 相邻色统计检测

3.1 相邻色

这种检测算法是基于这样一个假设的，即载体图

像中所包含的相对色彩数十比较小的，这与 Fridrich 提出用于 LSB 替换的检测器十分相似。4 LSB 匹配算法在嵌入过程中会把单个色彩转变成了大量的色彩值相邻的色彩簇。

假设一个像素用一个 1×3 的向量表示为(r,g,b)，其中的 r,g,b 分别表示像素的红绿蓝分量。

定义 两个色彩(r1, g1, b1)和(r2, g2, b2)是一对相邻色，如果|r1 − r2| ≤ 1, |g1 − g2| ≤ 1, and |b1 − b2| ≤ 1，即满足 $(r1-r2)^2+(g1-g2)^2+(b1-b2)^2 \leq 3$

根据上述定义，不难计算出对于任意一个非边缘色彩(ri,gi,bi)的相邻色最多个数为 26 个，这样它们就构成了一个相邻色邻域空间 RC：

$$\{(r,g,b)\,|\,r\in\{r_i-1,r_i,r_i+1\},g\in\{g_i-1,g_i,g_i+1\},b\in\{b_i-1,b_i,b_i+1\}\}$$

3.2 平均相邻色检测

一般载体图像中，大部分色彩的相邻色彩数是较少的。Westfeld [4] 指出"载体中的色彩平均只有 4 至 5 个相邻色彩。"而且 JPEG 图像中一般没有哪个色彩的相邻色超过 9 个。但是，在 LSB 匹配嵌入了信息之后，即使嵌入的信息很少，也会产生很多新的色彩，致使载体的平均相邻色彩数有了相当的增加，甚而某些色彩的相邻色达到 26 个。

令一幅图像的唯一色彩数为 U，一个色彩的相邻色个数记为 n，易知 $n\in[0,26]$。C_i 表示所有相邻色个数 n 等于 i 的色彩的总个数。

不难得知

$$U=\sum_{i=0}^{26}C_i$$

那么一幅图中相邻色个数 n 的出现频率

$$P_n=\frac{C_n}{U}=\frac{C_n}{\sum_{i=0}^{26}C_i}$$

由此，可以计算出相邻色个数 n 的均值

$$\bar{n}=\sum_{n=0}^{26}nP_n$$

图 1 展示的是一幅 JPEG 图像在嵌入信息前后相邻色个数的频率分布的直方图。可以看到在嵌入信息之后，统计量 n 的分布扩散开来，均值 $\bar{n}$ 由 2.22 增加到 5.60。

图 1 中虚线部分表示的是未隐写过密信的载体图片的平均相邻色彩数 $\bar{n}$ 的概率密度函数为 $f_{\mu,\sigma}$ 的高斯分布 $N(\mu,\sigma)$；而实线表示的则是隐秘图片 $\bar{n}$ 的概率密度函数为 $f_{\mu(s),\sigma(s)}$ 的高斯分布 $N(\mu(s),\sigma(s))$。图 2 中曲线分别表示的是 $f_{\mu,\sigma}$ 和 $f_{\mu(s),\sigma(s)}$。

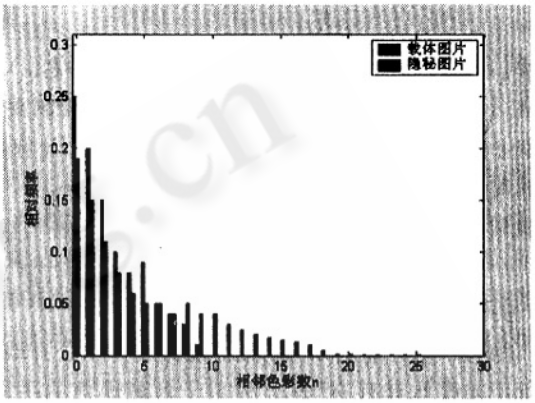

图 1

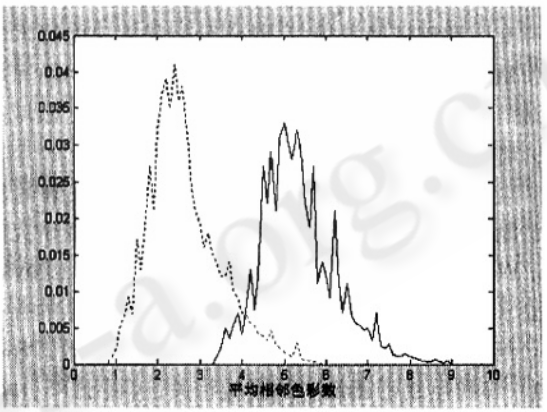

图 2

3.3 门限的选择

决定如何门限选择之前，首先定义概率非零两种错误。当图片并未嵌入任何信息的时候检测出其含有隐秘信息定义为第一类错误，而隐秘图片被漏检了则为第二类错误。

第一类错误：误检出一个假的密信

第二类错误：漏检了一个真的密信前

本文选用参考文献[4]中提供的门限确定方法。就是使得犯第一类错误和第二类错误的概率相等，即满足方程

$$P(\mathrm{I}) = P(\mathrm{II})$$

$$P(\mathrm{I}) = \int_{-\infty}^{Th} \frac{1}{\sqrt{2\pi\sigma^2}} e^{\frac{(x-\mu)^2}{2\sigma^2}} dx = \int_{Th}^{\infty} \frac{1}{\sqrt{2\pi\sigma(s)^2}} e^{-\frac{(x-\mu(s))^2}{2\sigma(s)^2}} dx = P(\prod)$$

方程两边分别用 $w=(x-\mu)/\sigma$ 及 $w'=(x-\mu(s))/\sigma(s)$ 做一个代换，不难得到下面的等式

$$\frac{Th-\mu(s)}{\sigma(s)} = \frac{\mu-Th}{\sigma}$$

由上式可以导出一个可以确定门限 Th 的表达式

$$Th=(\mu\sigma(s)+\mu(s)\sigma)/(\sigma+\sigma(s))$$

4 实验结果及结论

我们以质量因子 90 压缩了 1000 幅位图为 JPEG 图片。然后分别嵌入不同大小的隐秘信息。表 1 列出了平均相邻色统计监测器在嵌入不同大小隐密信息的情况下的门限选择情况以及错误率。

可以看出对于 jpg 格式的隐秘图片，本文提供的加权平均检测器的效果是很不错的。尤其是在嵌入的信息量很小的情况下，仍然可以有很高的检出率。

表 1

隐藏信息嵌入率	门限	错误率
5%	3.446	25.47%
10%	3.887	16.53%
20%	3.994	8.36%
50%	4.145	5.03%
100%	4.258	2.12%

但是本文的检测器对于 bmp 图片的 LSB 隐写算法的检测效果就不可靠了，原因是 bmp 图片的相邻色彩数不满足前文所说的条件。

图 3 中蓝色直方图表示的是载体图片的相邻色彩数的统计情况，红色直方图表示的是嵌入了 5KB（相当于总容量的 70%）的信息之后的隐秘图片的相邻色彩数的统计情况。可以看到载体图片和隐秘图片的相邻色彩数的变化并不明显。

据此我们可以得到两个结论：

（1）加权平均相邻检测对 jpg 图片的 LSB 匹配隐写可以进行可靠的检测。在不同需求下，可以通过调整门限来满足虚警率和漏警率的要求。

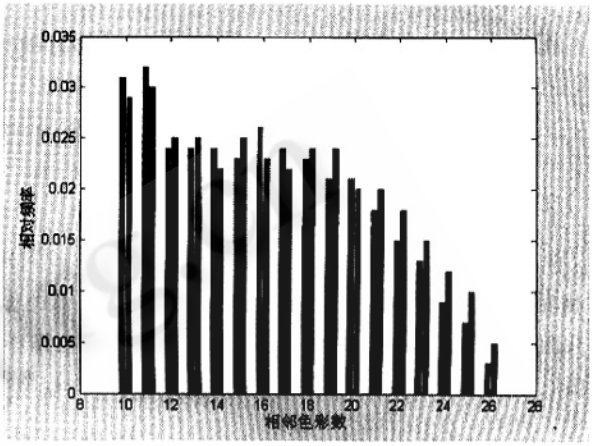

图 3

（2）本文提出的检测算法只适用于 jpg 彩色图片，载体为 bmp 图片的时候，就不能提供可靠的检测了。这是由于 bmp 图片的色彩特性决定的。

参考文献

1 J. Fridrich, M. Goljan, and R. Du, "Reliable detection of LSB steganography in color and grayscale images," Proc. ACM Workshop on Multimedia and Security, pp. 27 - 30, 2001.

2 S. Dumitrescu, X. Wu, and Z. Wang, "Detection of LSB steganography via sample pair analysis," in Proc. Information Hiding Workshop, Springer LNCS 2578, pp. 355 - 372, 2002.

3 A. Ker, "Improved detection of LSB steganography in grayscale images," in Proc. Information Hiding Workshop, Springer LNCS 3200, pp. 97 - 115, 2004.

4 A. Westfeld, "Detecting low embedding rates," in Proc. Information Hiding Workshop, Springer LNCS 2578, pp. 324 - 339, 2002.

5 Andrew D. Ker "Resampling and the Detection of LSB Matching in Colour Bitmaps" in Proc. of SPIE - IS&T Electronic Imaging, SPIE Vol. 5681 2005.