广西科学院学报
Journal of Guangxi Academy of Sciences

2010,26(4):449~451
Vol. 26, No. 4 November 2010

一种基于 LSB 隐写算法的图像盲检测方法*

Blind Detection Technology Based on Image LSB Steganography Algorithm

邱志宏,张爱科
QIU Zhi-hong, ZHANG Ai-ke

(柳州职业技术学院,广西柳州 545006)
(Liuzhou Vocational & Technical College, Liuzhou, Guangxi, 545006, China)

摘要:在隐写技术被动检测模式下,用数学方程对 LSB 图像隐写算法进行抽象和建模,定量分析被检测图像的隐写信息边界情况,根据隐藏信息的比特数推出隐藏信息的检测概率和误检概率的表达式,提出一种基于 LSB 隐写的图像盲检测方法。基于 LSB 隐写的盲检测方法在 LSB 隐写算法嵌入图像的隐藏信息超过一定范围时,可以有效分辨出原始图像和隐藏信息。

关键词:隐写算法 盲检测 LSB 隐写容量

中图法分类号:TP391 **文献标识码**:A **文章编号**:1002-7378(2010)04-0449-03

Abstract: In the steganography and passive tracking-mode, mathematical equations are used to abstract and model LSB steganography algorithm. Quantitative analysis of hidden information on images, which is hidden by detection, are used to make sure the biggest capacity of steganography algorithm. Then the blind detection is proposed based on the steganography image. Based on LSB steganography image and the blind detection method in LSB algorithm, which embeds on image with the steganography algorithm and is over a certain range of information, the original image and hidden information can be effectively distiguished.

Key words: steganography algorithm, blind detection, LSB, steganography capcity

基于图像最低有效位的 LSB 隐写算法是目前非常经典的隐写算法。这类算法的特点是将待隐藏的数据嵌入在图像信息的 LSB 位。由于图像 LSB 的修改对图像视觉效果影响非常小,因此,这种算法的隐写效果明显[1]。目前很多公开的隐写算法都是基于 LSB 位的[2~4]。LSB 隐写算法的这种特点给隐写检测和分析带来了一些困难和挑战,因为图像 LSB 位在改动很小的情况下,将覆盖图像和隐写图像区分出来比较困难。而且在隐写的过程中,如果引入随机化的隐写过程,使得图像在 LSB 位嵌入信息后,呈现出的是一种随机受损的效果,这将更加增大图像隐写分析的难度,这是因为信息以 LSB 算法嵌入覆盖图像,隐写图像的 LSB 平面合成结构将会成为泄密对象。因此在图像隐写时建议将信息嵌入图像之前首先进行加密,以保持一个随机的 LSB 外貌。此时为了增加图像隐写的安全性,可以对隐写的信息加密后再嵌入图像中[5,6],那么一个新问题随之出现,即隐写信息在嵌入时,应该嵌入多少比特的信息才算是安全的。Cachin[7] 证实,如果覆盖对象和隐写对象的概率分布的相对熵小于或者等于某个 ε,那么此隐写算法是 ε-安全的。他也证实确实存在隐写算法是 ε-安全的,但是他所描述的技术只是在理论层面,并未实现。

本文基于图像 LSB 隐写算法,在隐写分析被动检测模式[8,9]下,根据隐藏信息的比特数推出隐藏信息的检测概率和误检概率的表达式,提出一种基于 LSB 隐写的图像盲检测方法。

1 LSB 图像隐写算法的模型分析

使用数学方程对 LSB 隐写算法进行抽象和建模。LSB 隐写算法既可以对图像中的像素做出±1的改动,也可以不做任何改动,这依赖于待隐藏信息

收稿日期:2010-08-05

作者简介:邱志宏(1963-),男,副教授,主要从事信息安全研究。

*广西教育厅科研基金项目(200911LX490)资助。

的特性和相应像素的LSB值。在这里设 $I=\{x_i, i\in\Omega\}$，Ω 是一个索引集，表示覆盖图像。集合 Ω 划分为3个子集和 Λ_1、Λ_2、Λ_3，$\Omega=\bigcup_{i=1}^{3}\Lambda_i$ 且 $\Lambda_i\cap\Lambda_j=\Phi(i\neq j)$。LSB隐写图像的像素值集合是 $I_s=\{y_i, i\in\Omega\}$，其表达式为

$$y_i=\begin{cases}x_i+1, & \text{if } i\in\Lambda_1,\\ x_i-1, & \text{if } i\in\Lambda_2,\\ x_i, & \text{if } i\in\Lambda_3。\end{cases}\tag{1}$$

隐写分析的目标是估计 I 是否含有隐藏信息，即判断 Λ_1 和 Λ_2 是否非空，如果非空，这两个集合又包含哪些元素。在达成目标之后，就可能检测出覆盖图像中是否含有隐藏数据 I。当然，在此过程中，由于统计的不完整性和不确定性，预先不知道数据隐藏键值，隐写分析者会产生错误。错误的数量取决于 Λ_i 的集势。这又会引出另外一个问题：在给定不可检测概率的情况下，多少比特的信息可以隐写在 I 中（I 的隐写容量）。

用以下符合实际的假设来计算隐写容量。x_i 服从 $x_i\sim N(0,\sigma^2)$ 的高斯分布。对每个 $i(i\in\Omega)$，隐写分析过程可以归结为一个多重假设检验问题。

$$H_j: y_i=x_i+d_i, i=1,2,3,\tag{2}$$

$d_i=-1,0,1$ 时可以表示为 $H_1: y_i\sim N(1,\sigma^2)$，$H_2: y_i\sim N(-1,\sigma^2)$，$H_3: y_i\sim N(0,\sigma^2)$。

研究发现 H_3 的隐写图像和覆盖图像在统计上没有任何区别，因此只需检测 H_1 和 H_2 即可。如果 H_1 和 H_2 之一检验成功，就说明图像含有隐藏信息。如果覆盖图像中的像素比特和LSB中相应的像素比特相等，就可以肯定此图像没有包含任何隐藏信息。

再假设一个数据比特位值是1的概率是 p_d，$0<p_d<1$；LSB比特位值是1的概率是 p_l，$0<p_l<1$；隐藏数据的比特位和LSB比特位的取值是相互独立的，那么他们的联合概率为

$$P(d_1=1,l_1=1,\cdots,d\mid\Omega\mid,l\mid\Omega\mid)=(p_dp_l)^{\mid\Omega\mid},\tag{3}$$

$\mid\mid$ 表示集的势。当 $\mid\Omega\mid$ 无穷大时，联合概率趋近于0。对每一个像素进行上述3种假设检验判断，并使用最小错误概率准则作为价值函数。最小错误概率检测也表现为最大后验概率（MAP）检测。真验概率表示为

$$H=\arg\max_j P(H_j)P(y_i\mid H_j)。\tag{4}$$

因为 y_i 服从高斯分布，所以真验概率表达式

$$H=\arg\max_j P(H_j)\exp\frac{-(y_i-d_j)^2}{2\sigma^2}。\tag{5}$$

与 H_1，H_2，H_3 相对应的 d_j 分别是1、−1和0。这样就能够估计出含有隐藏信息的像素位置，也可以说像素位置是由 H_1 和 H_2 检测到的。当然，在此过程中也会产生错误，错误概率为 $p_{kj}=P(\text{decide } H_j\mid H_k\text{true}), j,k=1,2,3$。$p_{kj}$ 的值与图像的差异和分析方法有关。

2 LSB图像隐写盲检测方法

设 u_i 是像素 i 的模型分析结果。$M=\mid\Omega\mid$，$u_i=H_j, j=1,2,3$。以最小错误概率准则作为检测准则，如果符合以下条件就断定图像中包含隐藏数据。

$$P(H_1)\prod_{i=1}^{M}P(u_i\mid H_1)\cdot\begin{cases}>P(H_2)\prod_{i=1}^{M}P(u_i\mid H_2),\\ >P(H_3)\prod_{i=1}^{M}P(u_i\mid H_3),\end{cases}\tag{6}$$

或

$$P(H_2)\prod_{i=1}^{M}P(u_i\mid H_2)\cdot\begin{cases}>P(H_1)\prod_{i=1}^{M}P(u_i\mid H_1),\\ >P(H_3)\prod_{i=1}^{M}P(u_i\mid H_3)。\end{cases}\tag{7}$$

由对称性知，(6)式和(7)式会产生相同的结果，因此考虑(6)式做简化，即仅考虑 H_1 和 H_3，因为在统计上它们的接近度优于 H_1 和 H_2。因此多元假设检验问题就简化为二元假设检验，(6)式简化为(8)式。S_1，S_2 和 S_3 分别是像素值为1，−1和0的像素集合。

$$\frac{\prod_{i=1}^{M}P(u_i\mid H_1)}{\prod_{i=1}^{M}P(u_i\mid H_3)}\begin{cases}>\dfrac{P(H_3)}{P(H_1)}, & \text{包含隐藏数据},\\ \text{else}, & \text{不含隐藏数据}。\end{cases}\tag{8}$$

再转化为

$$\prod_{S_1}\frac{P(u_i=1\mid H_1)}{P(u_i=1\mid H_3)}\prod_{S_2}\frac{P(u_i=-1\mid H_1)}{P(u_i=-1\mid H_3)}\prod_{S_3}\frac{P(u_i=0\mid H_1)}{P(u_i=0\mid H_3)}\begin{cases}>\dfrac{P(H_3)}{P(H_1)}, & \text{包含隐藏数据},\\ \text{else}, & \text{不含隐藏数据}。\end{cases}\tag{9}$$

最后简化为

$$\prod_{S_1}\frac{P_{11}}{P_{31}}\prod_{S_2}\frac{P_{12}}{P_{32}}\prod_{S_3}\frac{P_{13}}{P_{33}}\begin{cases}>\dfrac{P(H_3)}{P(H_1)}, & \text{包含隐藏数据},\\ \text{else}, & \text{不含隐藏数据}。\end{cases}\tag{10}$$

假设 $P_d=P(\text{decide}H_1 \mid H_1\text{true})$ 是正确检测概率，$P_f=P(\text{decide}H_1 \mid H_3\text{true})$ 是假警概率，从(10)式得出 P_d 和 P_f 的值是 $|S_1|$ 和 $|S_2|$ 的函数，$|S_1|$ 和 $|S_2|$ 是含有隐藏信息的比特位数。检测总共有 2^{3^M} 种可能的检测规则，其中包括优化的检测规则。计算全部的检测参数需要很大的计算量，基于此，假设检测使用 C_M^J 种检测规则，那么可以得到

$$P_d=\sum_{k=J}^{M}\sum_{r=0}^{M-k}\cdot \frac{M!}{k!\ r!\ (n-k-r)!}p_{11}^{k}p_{12}^{r}p_{13}^{M-k-r}, \tag{11}$$

$$P_f=\sum_{k=J}^{M}\sum_{r=0}^{M-k}\cdot \frac{M!}{k!\ r!\ (n-k-r)!}p_{31}^{k}p_{32}^{r}p_{33}^{M-k-r}。 \tag{12}$$

因此，在给定 P_d 和 P_f 的情况下，通过(12)式可以计算得到隐写的比特数，也就得到了隐写图像的容量 J，即在 M 比特的图像中，在误检概率给定的情况下，不可能隐藏多于 J 比特的数据而不被检测到。

3 实例验证

通过一个具体的实例验证基于 LSB 图像隐写算法的最大隐写容量的计算。

设 $M=64$，$p_{12}=0.05$，$p_{13}=1-(p_{11}+p_{12})$，$p_{13}=p_{31}$，$p_{13}=p_{32}$，$p_{33}=1-(p_{31}+p_{32})$。注意 $M=64$ 不是一个限制性的假设，因为隐写分析以块为基本单元进行分析，检测能力达到 64 个块(block)。隐写分析技术的性能如图 1 所示。从图 1 可以看出，隐写分析提升了本地检测能力(p_{11} 增大)，说明我们能以很高的概率检测到 LSB 数据的存在，这就意味着隐写图像的容量小于 64bits(当 1bit/pixel 和 $M=64$ 时)。实际上，在此例中，当 $p_{11}=0.45$ 时，$p_d=0.5$，这意味着在 $p_{11}=0.45$ 的条件下，隐写分析者只有一半的正确率判断隐藏信息是否存在。因此，如果 $p_{11}=0.45$，44bits 的信息能够被可靠的隐藏(假定一半的隐藏数据不需要替换 LSB)。说明一点，p_{jk} 的值取决于图像的属性，例如图像像素的标准方差 σ。因此图像的属性和隐写分析策略在一定程度上决定了 LSB 的数据隐藏容量。我们所得到的隐藏容量只是一个上边界，因为可能还存在其它的检测方法来检测隐藏信息的存在。例如，基于图像质量度量值的分类技术能够十分精确的区分水印图像和非水印图像。

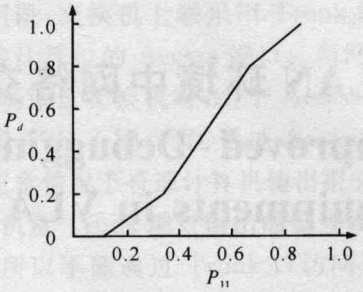

图 1 在 $J=\lceil (M+1)/2 \rceil$ 条件下隐写分析性能

4 结束语

许多研究者对图像隐写算法的盲检测主要是在信息论或者图像相关理论的基础上开展研究，已取得了不少的研究成果。本文从图像的统计特性的角度，分析基于图像 LSB 隐写算法的信息隐藏模型，提出隐写容量的计算方法。依据盲检测能力而定义的信息隐藏容量，实际上也确定了图像隐写的边界信息量，即能够正确可靠的区分覆盖对象和隐写对象的情况下，多少比特的信息可以嵌入。我们所得到的隐写容量公式是被动模式，下一步将研究包含有噪声注入覆盖对象的情况下图像盲检测的规则和技术。

参考文献:

[1] 陈国明，印鉴，周端宁，等. 一种新的隐写分析方法：IKLDA[J]. 电子学报，2009，37(8)：1762-1767.

[2] Niu Shaozhang，Zhou Qi，Cui Baojiang，et al. Detecting LSB steganography based on noise function[J]. 电子学报：英文版，2009，18(2)：343-346.

[3] 廖鑫，温巧燕. 基于拉普拉斯算子统计量的 LSB 替换隐写分析方法[J]. 电子与信息学报，2009(5)：1054-1058.

[4] 袁占亭，张秋余，刘洪国，等. 一种改进的 LSB 数字图像隐藏算法[J]. 计算机应用研究，2009，26(1)：372-374，377.

[5] 毛家发，林家骏，戴蒙. 基于图像攻击的隐藏信息盲检测技术[J]. 计算机学报，2009(2)：318-327.

[6] 张红娟，朱晨鸣. 抗统计分析的新型 LSB 隐写算法[J]. 计算机工程，2008，34(23)：144-146.

[7] Cachin，C. An information-theoretic model for steganography[J]. Proc 2nd Information Hiding Workshop，1998，1525：306-318.

[8] 秦姣华，孙星明，程小艳. 基于相邻像素统计特性的 LSB 隐写分析技术[J]. 系统仿真学报，2007，19(24)：5856-5860.

[9] 周治平，康辉. 基于特征的彩色位图隐写分析[J]. 计算机工程与应用，2007，43(7)：87-89.

(责任编辑：尹 闯)