基于最低有效位和最高有效位替换法的熵理论模型*

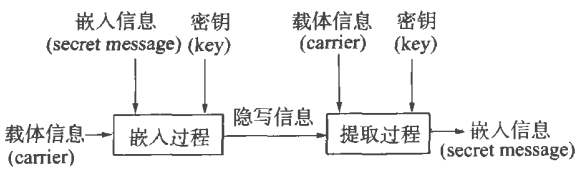
肖洪华, 黄永峰, 朱明方
(清华大学电子工程系 //网络与人机语音通信研究所网络实验室, 北京 100084)

摘 要: 信息隐藏是一个新兴的技术领域, 从现在的研究结果来看, 熵的概念对于信息隐藏技术的理解是很有好处的, 因此, 从信息论理论的角度出发, 用熵和互信息的原理分析最低有效位 (LSB) 替换法和基于位图调色板的最高有效位 (MSB) 替换法的具体实现。从信息论理论角度解释 LSB 替换法和 MSB 方法, 建立了一种用信息熵分析隐写术的理论模型。

关键词: 信息隐藏; 最低有效位 (LSB); 最高有效位 (MSB); 熵
中图分类号: TP274 文献标识码: A 文章编号: 0529-6579 (2004) S2-0042-04

信息隐藏是集多学科理论与技术于一身的新兴技术领域, 它应用于通信安全领域的一个重要分支就是隐写术 (steganography)。隐写术这个词语本身的意思是“隐蔽的写”, 而密码学的意思是“秘密的写”。与密码术保护消息内容的目的不同, 隐写术是为了隐蔽消息存在的事实或消息存在的位置, 将重要信息隐藏在其他信息之中, 使攻击者察觉不到它的存在, 或者即使知道它的存在, 但未经授权就无法确定它的位置。这就较之单纯的密码加密算法多了一层保护。

信息隐藏的一般模型如图:



嵌入过程用于将待隐信息通过密钥使用某种算法嵌入到载体信息中去, 形成外部特征与载体信息相同的隐写信息; 写信息通过公开信道传输到接收一方, 通过相对应的提取过程, 利用密钥将秘密信息从隐写信息中提取出来。

LSB 替换法是最典型的空域隐藏方法, 而 MSB 替换法能提供较高的安全性; 本文就这两种信息隐藏方法, 建立了一种熵分析的理论模型。

信息论的创始人香农在其发表的信息论奠基性论文“通信的数学理论”中提出了熵和互信息这两个重要的概念。

熵可以用来度量随机变量的不确定性, 设有一个离散随机变量 X, 它有 K 个可能的取值, 分布矩阵为:

$$\begin{bmatrix} X \\ P(x) \end{bmatrix} = \begin{bmatrix} a_1 & a_2 & \cdots & a_K \\ p_1 & p_2 & \cdots & p_K \end{bmatrix}$$

熵 $H(X)$ 定义为: $H(X) = -\sum_{i=1}^{K} p_i \log p_i$。

设随机变量 Y 的分布为:

$$\begin{bmatrix} Y \\ P(y) \end{bmatrix} = \begin{bmatrix} b_1 & b_2 & \cdots & b_J \\ p_1 & p_2 & \cdots & p_J \end{bmatrix}$$

条件熵:

$$H(X \mid Y) = -\sum_{k=1}^{K}\sum_{j=1}^{J} p(a_k, b_j) \log p(a_k \mid b_j)$$

条件熵可以用来表示当已知变量 Y 的取值的情况下, 随机变量 X 的不确定性的大小。

定义离散随机变量 X 和 Y 之间的互信息为:

$$I(X; Y) = H(X) - H(X \mid Y)$$

它表示在已知 Y 后所提供的有关 X 的信息量。

某些关于信息隐藏的理论文章从熵的角度进行分析已经得到了一些很有用的结论[1]。文献 [1] 中提出了一种基于熵的信息隐藏模型: 在信息隐藏系统中, 用 C 表示载体文件, E 表示隐藏数据 (嵌入信息), S 表示隐藏信息。则有

$$H(S) = H(C) + H(E) \quad (1)$$

为保证嵌入隐藏数据以后的载体文件和没有嵌入隐藏数据以前的载体文件对攻击者来说不可区分, 应该尽量使 $H(E)$ 的值尽量小于 $H(C)$ 的值。本文将延续这一思路并进一步的用熵的观点分析信息隐藏技术。

* 收稿日期: 2004-09-11
作者简介: 肖洪华 (1980 年生), 男, 硕士研究生; E-mail: xiaohh03@mails.tsinghua.edu.cn

1　最低有效位替换法熵分析模型

在参考文献 [2] 中有对最低有效位 (LSB) 方法的详细介绍，这里简要的叙述 LSB 方法的主要思想，以方便对它进行熵的分析。

设 C 为最初的 8×8 的 8 bit 灰度级载体图像，表示为：

$$C=\left\{\begin{array}{l} x_{ij} \mid 0\leqslant i<M_C, 0\leqslant j<N_C, \\ x_{ij}\in\{0,1,\cdots,255\} \\ E \text{ 表示待隐藏的秘密信息：} \\ E=e_i \mid 0\leqslant i<n, e_i\in\{0,1\} \end{array}\right\}$$

假设 n bit 的秘密信息要隐藏到载体 C 的像素的最右边 k bit 中，首先，将 n bit 秘密信息重新排列成 k 位信息 E'：

$$E'=\left\{e'_i \mid 0\leqslant i<n', e'_i\in\{0,1,\cdots,2^k-1\}\right\}$$

要想将 E 嵌入到 C 中，要求：$n'\leqslant M_C * N_C$。E 与 E' 映射关系可以表示为：

$$e'_i=\sum_{j=0}^{k-1} e_{i*k+j} *2^{k-1-j}$$

然后，从载体 C 中抽取出 n' 个像素作为隐藏消息的位置。于是，嵌入过程将这 n' 个像素的最右边 k bit 替换成 S' 中的秘密信息。即将 X_{l_i} 的最右边 k 位替换为 e'_i。

从直观的意义上观察，k 的值越大则对原始载体图像的改变就越大，因此，隐藏信息的不可见性就越差。

如果把一幅图像看成是由所有像素点组成的一个随机序列，当只分析图像中的单个像素时，假设每个像素点之间是独立的，把每一个像素点看成一个随机事件 X，这个事件的取值有 256 种可能，$X\in\{0,1,\cdots,255\}$。假设随机事件 X 即取等概分布，那么 X 的最大平均不确定性是：

$$H(X)=\log 256=8(\text{bit})$$

将秘密消息隐藏到这个像素最右边的 k bit 中，待隐消息位的最大平均不确定性为：

$$H(E)=\log 2^k=k(\text{bit})$$

设 C 和 E 是相互独立的，根据 LSB 替换方法，将秘密消息 E 隐藏到 X 的最右边 k 个比特，设

$$X=(x_1,x_2,\cdots,x_8),$$
$$E=(e_1,e_2,\cdots,e_k)$$

则隐藏信息：

$$S=(s_1,s_2,\cdots,s_{8-k},S_{8-k+1},\cdots,s_8)=$$
$$(x_1,x_2,\cdots,x_{8-k},e_1,\cdots,e_k)$$

引入中间变量

$$Y=(x_1,x_2,\cdots,x_{8-k},0,\cdots 0)$$

则 $S=Y+E$，Y 和 E 是统计独立的。可以看到，Y 的取值完全由 X 确定，Y 有 2^{8-k} 种可能的取值。而且由于 Y 的最后 k 位全都为 0，E 是 k 位 bit 的随机数，因此，当确定 S 的值时能惟一的确定 Y 的取值，即能由 S 的取值唯一的确定 E 的取值，故 S 的概率：

$$P(S=a)=P(Y+E=a)=$$
$$P(Y=a_1,E=a_2)=$$
$$P(Y=a_1)P(E=a_2)$$

其中，a_1 的前 $8-k$ 位和 a 的前 $8-k$ 位相同，a_1 的后 k 位全为 0；a_2 有 k bit，且与 a 的最右边 k 位相等。

因此，S 的平均不确定性

$$H(S)=\sum P(s)\log P(s)=$$
$$\sum P(y)\log P(y)+\sum P(e)\log P(e)=$$
$$H(Y)+H(E)$$

而 Y 的取值完全取决于 X，因此，Y 的平均不确定性肯定要小于 X 的平均不确定性，即：$H(Y)\leqslant H(X)$。在假设 X 是等概分布的情况下，可知 Y 的分布也是等概的，且 Y 有 2^{8-k} 种取值可能，Y 的最大平均不确定性为 $H(Y)=8-k$。而 E 的最大平均不确定性为 $H(E)=k$，则

$$H(S)=H(Y)+H(E)=8-k+k=8(\text{bits})$$

即隐藏前后图像的最大熵不变，而只有在都满足等概分布的情况下，熵才能取最大。然而需要指出的是，一般情况下的分布都不是等概的。

根据前面所说的，Y 的最左边 k 位和 X 的最左边 k 位一样，最右边 k 位为 0。以最简单的 $k=1$ 为例来分析不等概的情况，对于 8 位灰度级图像，X 取值有 256 种可能，当 $k=1$ 时，Y 取值有 128 种可能。举如下一个特殊的例子：

$$P(Y=11111110)=$$
$$P(X=11111110)+P(X=11111111)$$

同样，这个式子也可推广到 k 取其他值和不同的 Y 的取值的情况。

设 X 和 Y 的概率分布为：

$$\begin{bmatrix} X \\ P(x) \end{bmatrix}=\begin{bmatrix} 0 & 1 & \cdots & 255 \\ p_1 & p_2 & \cdots & p_{256} \end{bmatrix},$$
$$\begin{bmatrix} Y \\ Q(y) \end{bmatrix}=\begin{bmatrix} 0 & 2 & \cdots & 254 \\ q_1 & q_2 & \cdots & q_{128} \end{bmatrix}$$

熵函数与随机变量的具体取值无关，只与概率分布有关，利用熵函数的可加性有：

$$H(X)=H(p_1,p_2,\cdots,p_{256})=$$
$$H((p_1+p_2),(p_3+p_4),\cdots,(p_{255}+p_{256}))+$$
$$\sum_{n=1}^{128}(p_{2n-1}+p_{2n})H(p_{2n-1},p_{2n})=$$

$$H(q_1, q_2, \cdots, q_{128}) + \sum_{n=1}^{128}(p_{2n-1}+p_{2n})H(p_{2n-1}, p_{2n}) = H(Y) + \sum_{n=1}^{128}(p_{2n-1}+p_{2n})H(p_{2n-1}, p_{2n})$$

即

$$H(Y) = H(X) - \sum_{n=1}^{128}(p_{2n-1}+p_{2n})H(p_{2n-1}, p_{2n})$$

计算 $H(S)$

$$H(S) = H(Y) + H(E) = H(X) - \sum_{n=1}^{128}(p_{2n-1}+p_{2n})H(p_{2n-1}, p_{2n}) + H(E)$$

故，只要

$$H(E) - \sum_{n=1}^{128}(p_{2n-1}+p_{2n})H(p_{2n-1}, p_{2n})$$

的值尽量小，隐藏前后图像的熵相差就越小。

如果把整幅图像当成一个由所有像素点组成的随机变量序列来看的时候，考虑各个像素点之间的相关性，为简单起见把图像看成是一个 1 阶的马尔可夫序列 $(x_1, x_2, \cdots, x_N)$，由马尔可夫性可得：

$$H(x_1, x_2, \cdots, x_N) = H(x_1) + H(x_2 \mid x_1) + \cdots + H(x_N \mid x_{N-1})$$

与将单个像素点作为一个随机变量考虑时一样：

$$H(s_1, s_2, \cdots, s_N) = H(y_1, y_2, \cdots, y_N) + H(e_1, e_2, \cdots, e_N) = H(y_1, y_2, \cdots, y_N) + H(E)$$

因为

$$H(y_1, y_2, \cdots, y_N \mid x_1, x_2, \cdots, x_N) = 0$$

故

$$H(s_1, s_2, \cdots, s_N) = H(y_1, y_2, \cdots, y_N) + H(E) = H(x_1, x_2, \cdots, x_N) + H(E) - H(x_1, x_2, \cdots, x_N \mid y_1, y_2, \cdots, y_N)$$

故，当

$$H(E) - H(x_1, x_2, \cdots, x_N \mid y_1, y_2, \cdots, y_N)$$

的值尽量小的时候，隐藏前后熵值的变化可以尽量的小。

2 基于图像的最高有效位替换法熵分析模型

如前面所述，当改变图像像素的 LSB 时，对像素值的影响比较小，因此不易引起攻击者的察觉。当改变像素点最高比特位时，像素值的改变就十分的大。如果有一种方法可以让最高比特位变为无关的比特位的话，那么将秘密信息隐藏到最高比特位不仅不会引起图像的改变，而且能获得较高的安全性。基于图像的最高有效位（MSB）替换法就是这么一种方法。

要想把信息隐藏在载体文件中，就必须在载体文件中创造冗余空间，参考文献 [3] 中叙述了一种利用颜色量化来创造冗余空间的方法。颜色量化过程实际上是一个颜色分类的过程，即用一种颜色代替和它比较接近的那些颜色。在选择了合适的颜色量化算法后，把图像量化到颜色数少于 256 色（这里以将颜色数降到 128 色为例），然后把图像按 256 色的格式存储。

在 256 色存储格式中，有一个 256 色的调色板，每个像素都用一个 8 位的索引号来表示（$2^8=256$），这对于 128 色的图像来说则是多余的，因为 128 色只用 7 位（$2^7=128$）来表示就足够了，所以剩余的那位就可以作为冗余空间来存储隐藏信息。需要特殊说明的是，图像的调色板要以 128 为周期循环排列，即调色板索引值为 p 的像素点和索引值为 $128+p$ 的点表示的是同一颜色，可见图像像素值的最高位的值的变化不会影响该点的颜色值，因此图像每个像素值的最高位可以用于信息隐藏。

从熵的角度来看，原来用 256 色格式存储图像时，每个像点 X 有 256 种可能的取值，把每个像素点的取值看成一个随机事件的话，它的最大平均不确定性，即最大熵为：

$$H(X) = \log 256 = 8(\text{bit})$$

当用 128 色图像表示时，单个像素点的最大熵为：

$$H(X) = \log 128 = 7(\text{bit})$$

为了讨论的方便，简单地将图像量化过程看成是一个多到一的映射过程，映射前的像素点为 X，用 Y 表示将 X 进行映射后的像素点。则 Y 由 X 确定，即 $H(Y \mid X) = 0$。

根据互信息函数：

$$I(X;Y) = H(X) - H(X \mid Y) = H(Y) - H(Y \mid X)$$

将 $H(Y \mid X) = 0$ 代入上式，得：

$$H(Y) = H(X) - H(X \mid Y)$$

Y 是由 X 确定的，而由于是多到一的映射，当已知 Y 的时候并不能惟一的确定 X，只是能知道 X 的取值范围，即 Y 能提供关于 X 的一部分信息，而不是全部，故 $H(X \mid Y) \geqslant 0$。则

$$H(Y) = H(X) - H(X \mid Y) \leqslant H(X)$$

因此，当用适当的图像量化方法将颜色数降到 128 的时候，图像熵将变小。这将有利于秘密消息的嵌入。

MSB 替换法与 LSB 替换法不同。在 LSB 方法中，利用的是改变每一个像素点最右边的 k 个比特，这样对原来像素的值的改变不大，因此可以进

行秘密信息的隐藏；而在 MSB 方法中，由于先对图像进行了颜色量化处理，每个像素的最高一位变成是对图像的索引值没有影响的冗余位了，因此，改变这个最高位对于图像的索引值没有任何的影响。故在将秘密信息嵌入到经颜色量化处理后的图像的这一过程中，图像的熵没有改变；可以认为图像的熵是在颜色量化的过程中改变了，并不是在秘密信息嵌入过程中改变了。

3　总　结

本文尝试从信息熵的角度建立信息隐藏空域法中最典型的 LSB 替换法和基于 8 位图像的 MSB 方法的信息熵研究模型。因为不能将所有的不确定因素一一列举出来，所以上面分析的熵值是不准确的。尽管如此，文章中做出的分析依然能使我们对秘密信息嵌入前后图像的熵值改变从数量上有一个直观的概念。

参考文献：

[1] 郑炜, 胡正国, 汤小春, 等. 基于熵的信息隐藏算法研究[J]. 西北工业大学学报, 2003, 21(1).

[2] CHAN C K, CHENG L M. Hiding data in images by simple LSB substitution[J]. Elsevier Computer Science, 2003.

[3] 任智斌, 隋永新, 杨英慧, 等. 以图像为载体的最大意义位(MSB)信息隐藏技术的研究[J]. 光学 精密工程, 2002, 10(2).

An Entropy Model Based on LSB Substitution and MSB Substitution

XIAO Hong hua, *HUANG Yong feng*, *ZHU Ming fang*

(Network Laboratory //Department of Electronic Engineering, Tsinghua University, Beijing 100084, China)

Abstract: Information hiding is a rising research area, the introduction of the concept of entropy is very helpful for comprehending the information hiding technology. This paper analyzes two typical information hiding methods, simple LSB substitution and MSB substitution, in the approach of information entropy theory. This paper also present a theoretical model for analyzing the information hiding technology.

Key words: information hiding; LSB; MSB; entropy