

一种基于 LSB 图像信息隐藏的改进算法^①

李桂芸, 邓桂英, 赵逢禹

(上海理工大学 光电信息与计算机工程学院, 上海 200093)

摘 要: 介绍并分析了传统的 LSB 信息隐藏算法原理, 详细阐述了图像置乱技术的原理和一种传统的混沌图像置乱方法。在此基础上, 提出了一种新的图像信息隐藏算法: 基于图像向量索引奇偶性进行信息隐藏的算法。试验结果及分析结果表明, 该算法实现简单, 有很好的视觉掩蔽性和较高的信息隐藏容量, 并提高了信息隐藏的安全性。

关键词: LSB; 信息隐藏; 图像置乱; 视觉掩蔽性; 信息隐藏容量

Improved Algorithm Based on LSB Image Information Hiding

LI Gui-Yun, DENG Gui-Ying, ZHAO Feng-Yu

(School of Optical-Electrical and Computer Engineer, University of ShangHai for Science and Technology, ShangHai 200093, China)

Abstract: The LSB is the traditional information hiding methods, At first, this paper Presented and analyzed its principle. Then elaborated the principles of image scrambling technology . On his basis, we proposed a new image information hiding algorithm, the experiment and analysis results show that the algorithm is simple, having a good visual masking , high information hiding capacity and good security.

Key words: LSB; information hiding; image scrambling; visual masking; capacity of information hiding;

随着 Internet 技术和多媒体技术的飞速发展, 多媒体信息的传输也越来越方便, 人们可以通过 Internet 方便快速地获得其想要的数字化产品。但是, Internet 在带给人们这些便利的同时, 所传输的信息安全性也面临着巨大的挑战, 如何保证信息在传输过程中不受到窃取, 篡改等攻击, 已经成为 Internet 技术向前发展所面临的重要课题^[1]。传统的信息保护机制是对通信内容进行加密处理, 对所要传送的消息先进行加密, 即使遭到窃取也是一堆无意义的乱码。然而随着计算机处理速度的提高, 加密数据的破译时间也不断缩短。另外, 以乱码形式在公共信道中传输的密文更容易引起破译者的兴趣而实施攻击和破坏。在网络传输过程中, 加密后的密文通常无法通过某些网络节点, 因此会造成信息传输的失败。所以, 传统的加密体制面临着巨大的挑战, 寻求更多新的信息保护机制成为研究者们的重要课题。

信息隐藏技术 (Information Hiding) 是 1996 年国外才开始兴起的一门新的学科^[2]。它利用载体信息的冗余性, 将秘密信息隐藏于普通信息之中, 通过普通信息的发布而将秘密信息发布出去, 即将重要的信息隐藏于其他信息里以掩饰它的存在。它隐藏的是信息的“存在性”, 使它们看起来与一般非机密资料没有区别, 可以避免引起其他人注意, 从而具有更大的隐蔽性和安全性, 十分容易逃过拦截者的破解^[3]。信息隐藏技术主要分为频域信息隐藏技术和时域信息隐藏技术。LSB (最不重要位)^[4-6]是时域信息隐藏技术最常见的算法, 它具有嵌入简单, 隐藏容量大, 具有很好的不可感知性等优点。近年来, 也出现了许多 LSB 的改进算法^[7-11]。Chan 等提出了一种基于 LSB 的最优像素调整算法^[7]; Wang 等提出一种基于遗传算法的最优 LSB 替换方法, 搜索出一个最优的灰度值映射, 然后将此信息通过该映射的信息置换, 再嵌入到载体图像

① 收稿时间:2011-07-18;收到修改稿时间:2011-08-31

中^[8]；靳战鹏等通过分析 LSB 以及在此基础上改进的标志位隐藏算法提出一种失真度更低，安全性更高的索引数据链隐藏算法^[11]。

本文基于对图像隐藏技术中空间域信息隐藏技术的研究，首先介绍并分析了传统的 LSB 隐藏算法及图像预处理技术——图像置乱方法，之后提出了一种安全性更高的新的隐藏算法——基于索引奇偶性的隐藏算法。

1 LSB 图像隐藏算法原理

对于计算机来说，一幅图像就是由一些标记像素亮度的值组成的一个矩阵^[11]。LSB 算法是将秘密信息嵌入到载体图像像素值的最低位平面，改变这一位平面的值对载体图像的品质影响最小。

LSB 算法主要过程如下：将原始载体图像的时域像素值用二进制表示，用二进制秘密信息中的每一比特信息替换与之相对应的载体数据的最低位平面，假设待嵌入的秘密信息流为[0 1 1 0 0 0 1 0 0]，载体图像矩阵如下图左边文本框所示，则替换过程可如图 1 表示：

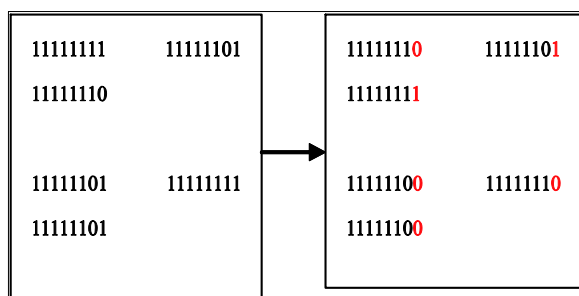


图 1 算法替换过程

对于 LSB 算法，其算法复杂度较低，实现简单；由于通常替换的是图像像素值的最低位平面，故对图像品质影响较小，不可感知性好；每一个像素最少可隐藏一位秘密信息，其隐藏容量较大。但对像素值的改变使像素的统计特性也随之改变，且存在“值对”现象，安全性不高。

2 图像预处理——图像置乱

“置乱”，顾名思义就是把待处理的信息次序打乱。数字图像可以表示为一个矩阵，矩阵的维度即代表图像的宽度和高度，故图像置乱，就是对矩阵进行特殊的行列变换，改变元素在矩阵中的位置，使图像没有

任何可统计的特征如形状，纹理等，可将图像抽象成一些随机的信息。

对于任意一幅图像 I，设其大小 $n=M \times N$ ，M 和 N 分别是图像 I 的高度和宽度，且 I 中共包含 k 种颜色，其中具有颜色 c_i 的像素个数为 n_i ， $n_1 + n_2 + \dots + n_k = n$ ，则 I 的直方图可以看作是一个具有 k 种元素的多重集 $S = \{n_1 * c_1, n_2 * c_2, \dots, n_k * c_k\}$ ，其基数为 n。显然，S 上的一个全排列 P 均可定义为一幅或多幅像素总数为 n、高度和宽度分别为 M、N 的图像，但其中有且仅有一幅图像像素的排列与 I 的像素排列相同，其他不同的排列，我们可以称之为图像 I 经过置乱后的图像。对图像的置乱操作，实际上也就是经过一个转换，把图像 I 转变到这些图像中的任意一个。S 的全排列和图像大小为 n，高度和宽度分别为 M、N 的图像之间是一一对应的关系。也 s 就是说，具有相同大小和直方图的每幅图像与相应的全排列之间存在着一一对应的映射关系，如图 2 所示^[1]：

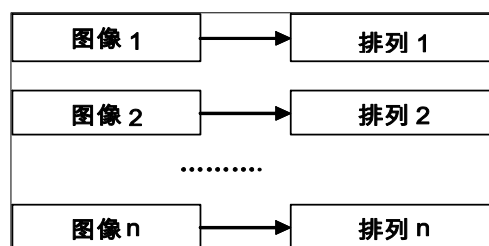


图 2 图像与排列的对应关系

图像置乱可分为基于密码学的图像置乱（如维基利亚（Vignere）密码、DES 等）和基于混沌的图像置乱两大类^[1]。本文主要介绍以 Logistic 方程作为模型的混沌序列发生器。

1975 年《美国数学月报》上发表了一篇短文《周期 3 蕴涵着混沌》，第一次引入了“混沌”的概念^[12]。Logistic 映射，即虫口模型是最基本的混沌模型。Logistic 映射如下式(1)所示，它最初用来描述昆虫数目的时代的变化规律：

$$x_{n+1} = \mu x_n (1 - x_n) \quad n = 0, 1, 2, \dots, x_n \in (-1, 1) \quad (1)$$

相应的概率密度函数为：

$$\rho(x) = \begin{cases} \frac{1}{\pi \sqrt{1-x^2}}, & x \in (-1, 1) \\ 0, & \text{其他} \end{cases} \quad (2)$$

其中 x 为控制参量, 式(1)可以看作是一个动力学系统。

值确定后, 由任意初值 $x_0 \in [0,1]$, 可迭代出一个确定的序列 $x_1, x_2, x_3, \dots$, 对应不同的 μ 值, 将得到不同的序列。以 μ 为横坐标, $x \in [0,1]$ 为纵坐标得到式(1)的函数图像如图 3 所示。

2.1 的函数图像如图 3 所示:

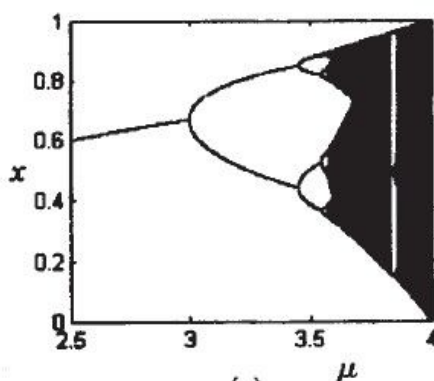


图 3 Logistic 序列的周期分叉

由图 3 可知, 当 $1 \leq \mu < 3.0$ 时, 方程 2.1 的解为稳态解, 即周期为 1 解; 当 $\mu = 3.0$ 时, 方程的解由 1 个变为 2 个, 为一个一分为二的分叉过程; 当 $\mu = 3.449489$ 时, 解由 2 个变 4 个; 当 $\mu = 3.544090$ 时, 解由 4 个变 8 个; ... 当 $\mu = 3.569945$ 时, 解为无数个, 系统进入混沌状态。当 $\mu = 4$ 时, 产生混沌序列。

由上述可知, 当 $\mu = 4$ 时, Logistic 映射在有限区间 $[0,1]$ 内部运动, 表现出随机性; x_0 的微小变化会导致序列 $\{x_n\}$ 的巨大差异, 当 x_0 未知时, x_n 的值也不可预测, 则 $\{x_n\}$ 对初值具有的极度敏感性。因此我们可以利用 Logistic 映射产生很好的随机数。

3 提出的算法

假设 $M \times N$ 的载体图像 X , $X = \{X(i, j) | 0 \leq i < M, 0 \leq j < N\}$, M 和 N 分别为图像的高度和宽度, $m = \{m_i\}$ (为要嵌入的秘密信息) 为二进制比特流, 长度 $l \leq M \times N$ 。设嵌入秘密信息后的载体图像为含密图像 Y , $Y = \{Y(i, j) | 0 \leq i < M, 0 \leq j < N\}$ 。

嵌入算法的具体步骤如下:

① 首先对载体图像降维: 按照行扫描的方式对载体图像 X 进行扫描, 使载体图像 C 变成一个图像向量 $x = \{x_i | 0 \leq i < (M \times N - 1)\}$, 它的标记按照顺序的方式进行, 即 0 到 $M \times N - 1$ 。

② 采用 Logistic 方程作为模型的混沌序列发生器生成随机混沌序列 z_n 对图像向量 x 置乱: 首先对混沌序列 z_n 从大到小或者从小到大排序, 将图像向量 x 的各个像素与排序后的混沌序列顺序相对应, 然后按照生成的混沌序列顺序, 来改变图像向量像素的顺序, 完成对图像的置乱, 置乱后的图像向量设为 x' , $x' = \{x'_i | 0 \leq i < (M \times N - 1)\}$ 。

③ 对置乱后的图像向量 x' , 按照其像素索引的奇偶性分成两大部分: 偶序列 x'_{even} , 奇序列 x'_{odd} 。

④ 遍历要嵌入的秘密信息 m , $m_i = 0$ 时嵌入偶序列 x'_{even} , $m_i = 1$ 时嵌入奇序列 x'_{odd} , $m_{i+1} \neq m_i$ 时, 则改变 m_i 所对应的像素 x'_i 的 LSB 位 ($x'_{(i,0)}$), 使其满足与次不重要位 $x'_{(i,1)}$ 相异或的结果为 1, 即:

```
even=0;
odd=1;
if ( $m_0 == 0$ )
     $x'_{even,0} = x'_{even,1}$ ; //秘密信息第一位为 0 时
else
     $x'_{even,0} = x'_{even,1} - 1$ ; //秘密信息第一位为 1 时
even=even+2;
for i=0:(l-1)
    //秘密信息位为 0 时, 隐藏于偶序列
    if ( $m_i == 0$ )
        if ( $m_{i+1} == m_i$ )
             $x'_{even,0} = x'_{even,1}$ ;
        elseif ( $m_{i+1} != m_i$ )
             $x'_{even,0} = x'_{even,1} - 1$ ;
        even=even+2;
    //秘密信息位为 1 时隐藏于奇序列
    elseif ( $m_i == 1$ )
        if ( $m_{i+1} == m_i$ )
             $x'_{odd,0} = x'_{odd,1}$ ;
        elseif ( $m_{i+1} != m_i$ )
             $x'_{odd,0} = x'_{odd,1} - 1$ ;
        odd=odd+2;
```

⑤ 对按照上述过程嵌入信息后的图像向量, 设其为 y' , 按照混沌序列的大小顺序与载体图像像素的对应关系, 将 y' 的像素顺序恢复为原始载体图像的像素顺序, 得到含密图像向量 y 。

⑥ 将含密图像向量 y 按照高度为 M , 宽度为 N 重新还原为 $M \times N$ 的图像矩阵, 即得到含密图像 Y , 如

此, 嵌入过程完成。

提取过程为嵌入过程的逆过程: 首先对含密图像按照行扫描的方式对其降维, 得到含密图像向量 y' 然后按照与嵌入过程同样的混沌序列对 y' 置乱, 得到 y' , 按照其索引的奇偶性将其分为两大类, 一次对这两大类像素的最低两位进行异或, 即若 $y'_{(0.0)} \oplus y'_{(0.1)} = 1$, 则 $m_0 = 1$, 下一个再考虑 $y'_{(1.0)} \oplus y'_{(1.1)}$, 否则若 $y'_{(0.0)} \oplus y'_{(0.1)} = 0$, 则 $m_0 = 0$, 下一个再考虑 $y'_{(2.0)} \oplus y'_{(2.1)}$, 如此依次下去, 得到秘密信息 m 。

例如, 我们将信息流 11010... 嵌入到一个图像中, 假设置乱后的图像向量像素为 $(x_{11}, x_{00}, x_{01}, x_{00}, x_{01}, x_{10}, x_{00}, x_{11}, \dots)$ (由于在嵌入过程中队图像像素的高六位不做修改, 则为书写方便, 高六位用 x 表示), 则嵌入过程如图 4 (提取过程为嵌入过程的逆过程):

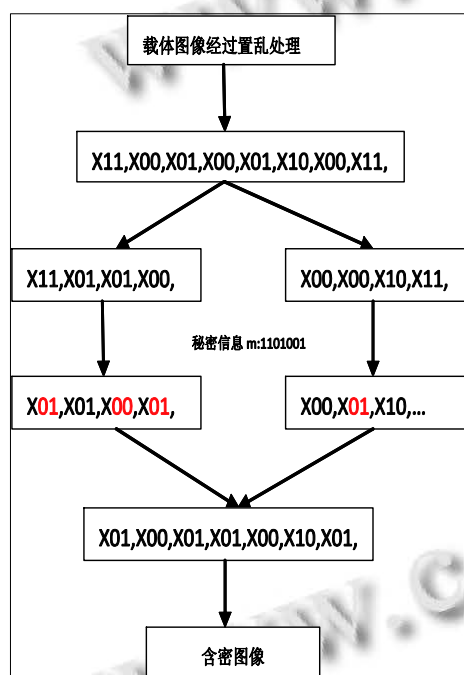


图 4 秘密信息的嵌入过程

4 试验及算法性能分析

4.1 试验

编写实现上述嵌入算法和提取算法的代码。取 256 级灰度图像 Lena (256×256) 为载体图像, 二值图像 xiaohui (128×128) 为秘密信息, 试验结果如下:

对比图 (a) 和图 (c), 从直觉上, 无法判断两者差异, 对比图 (b) 和图 (d), 两者在信息上面没有差异, 信息被完整的提取了出来。



图 5 (a)载体图像 (b)秘密图像 (c)嵌入秘密信息后的载体图像(含密图像) (d)提取的秘密图像

4.2 算法性能分析

① 视觉隐蔽性: 为评价提出算法的隐蔽性, 我们采用峰值信噪比 PSNR 衡量含密图像 S 与原始载体图像 C 的差别, 可以看到, 含密图像可以很好的满足隐蔽性的要求 ($PSNR \geq 28$):

$$PSNR = 10 \log \frac{M \times N \times 255^2}{\sigma_{i=0}^{M-1} \sigma_{j=0}^{N-1} (s-1)^2 - (1)^2} \geq 10 * \log 255^2 \geq 48.1647 \quad (3)$$

从嵌入修改的像素个数和对单个像素灰度值的修改幅度上来看, LSB 算法对像素个数的修改数接近于待嵌入的秘密信息位数, 显然大于本文提出的算法对像素的修改数。故提出的算法较 LSB 算法具有更好的视觉隐蔽性。

② 隐藏容量: 提出的算法的信息隐藏容量可达到 1bpp, 和 LSB 算法相近, 保持了 LSB 算法隐藏容量大的特性。

③ 抗统计分析特性: 图像信息隐藏改变了图像数据流的冗余部分, 经常会改变原始图像数据的统计特

性。LSB 算法是将像素值的最低有效信息用秘密信息取代,即如果秘密信息为与隐藏该位的像素灰度值的最低位相同,则不改变原始载体的最低位的值;反之,则修改原始载体的最低有效位,即将 $2i$ 改为 $2i+1$ 或将 $2i+1$ 改为 $2i$,而不会将 $2i$ 改为 $2i-1$ 或将 $2i+1$ 改为 $2i+2$ 。秘密信息在嵌入前一般经过加密,0 和 1 出现的概率近似为 $1/2$ 。可见,如果秘密信息完全取代载体的最低位平面,则像素值的奇偶个数比较相近,但如果是原始图像,这奇偶个数相差甚远。基于这种情况的隐写分析方法如分析法^[12]、RS 分析法^[13]很容易检测到载体的异常。提出的算法首先对载体图像置乱,后根据索引的奇偶性来隐藏信息流,不直接根据信息位的值来改变载体像素的 LSB 位,改变之后的 LSB 位仍是随机的,故不会出现上述的奇偶个数相近的情况,即对载体统计特性影响不大。

5 结论

针对以数字图像为载体的信息隐藏技术为当前研究热点,基于传统的 LSB 算法,本文提出了一种新的算法。试验结果和分析结果表明,该算法保持了 LSB 算法良好的视觉隐蔽性和较大的信息隐藏容量,并提高了抗统计攻击性。该算法简洁,实现简单,不损坏原秘密信息,具有一定的应用价值。

参考文献

- 1 曹卫兵.基于数字图像的信息隐藏技术研究[博士学位论文].西安:西北工业大学,2003.
- 2 Biham E, Shamir A. Differential cryptanalysis of DES-like cryptosystems. *Journal of Cryptography*, 1991,4(1):3-72.
- 3 闵连权.把信息隐藏在各个角落.计算机世界网(01) B10-B11.
- 4 McNally JG. Computer optical-sectioning microscopy for 3D quantitation of cell motion: results and challenges. *SPIE*, 1994,(2302):342-351.
- 5 Westfield A, Pfitzmann A. Attacks on teganographic systems. In: Pfitzmann A, ed. *Proc. of the 3rd Int'l Workshop on Information Hiding*. LNCS 1768, Berlin: Springer-Verlag, 1999:61-76.
- 6 Chang CC, Linm H, Hu YC. A fast and secure image hiding scheme based on LSB substitution. *International Journal of Pattern Recognition and Artificial Intelligence*, 2002, 16(4): 399-416.
- 7 陈铭.基于置乱变换与改进 LSB 嵌入的信息伪装算法研究.解放军信息工程大学,2005.
- 8 Wang RZ, Liu CF, Lin JC. Image hiding by optimal LSB substitution and gere ticalgorithm. *Pattern Recognition*, 2001, 34(3):671-483.
- 9 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.电子与信息学报,2009,31(5):1054-1058.
- 10 刘红翼,王继军.一种基于 LSB 的数字图像信息隐藏算法.计算机科学,2008,35(1):100-125.
- 11 靳战鹏,沈绪榜.基于位平面的 LSB 图像隐藏算法分析及改进.2005,20(5):2541-2543.
- 12 张新鹏,王朔中,张开文.基于统计特 fl 的 LSB 渐写分析.应用科学学报,2004,22(1):16.19.
- 13 Fridrieh J, Goljan M. Detecting LSB Steganography in Color and Gray, tale Images Magazine of IEEE Multimedia, Special Issue on Secudty, 2001:22-28.