基于 LSB 及置乱的图像隐藏算法研究

牛振喜

(西北工业大学 科技处，陕西 西安 710072)

摘 要：基于传统 LSB 算法，提出了一种新的图像信息隐藏算法。基本思想为：根据人眼对 R、G、B 三种颜色敏感度不同，在三种颜色分量上分别隐藏不同信息量。在隐藏信息的同时，使用 Baker 算法进行图像置乱，使之具有更好的混沌性和隐藏性。实验证明，该算法具有密钥空间大、隐藏效果好等特点。

关 键 词：图像隐藏，置乱，LSB
中图分类号：TP391 **文献标识码**：A **文章编号**：1000-2758(2013)02-0300-05

随着通信和计算机技术的发展，网络通信已经成为信息传播的主要工具，其中数字图像的传输在网络通讯中起着越来越重要的作用。据美国国家安全局统计，在当前网络通信中，图像信息约占信息总量的 70%，是人们进行信息交换的重要手段[1]。更重要的是，随着互联网技术的普及、开放和共享，具有高保密特点的图像受到越来越多的威胁[2]，特别是涉及国家安全和战略的图像，这些图像信息在传输之前必须经过严格、有效、具有自主知识产权技术的加密处理。

信息隐藏技术又称隐写术，是将秘密信息隐藏于另一公开信息(载体信息)中形成隐蔽载体，然后通过隐蔽载体的传输来传递隐藏信息[3,4]，使潜在的攻击者难以从公开信息中判断秘密信息是否存在，难以截获隐藏信息，从而达到保证信息安全的目的。

虽然信息隐藏技术的研究已经取得了很大进展[5]，但总的来说还未达到可实用的阶段[6]，而且尚未形成完整的理论体系[7]，其隐蔽性和不可测性在一定程度上还可能被分析，又因为隐藏算法比加密算法相对简单，因此存在隐藏图像具有易被还原的缺陷。

在此背景下，本文试图在图像隐藏过程中引入数字图像置乱技术，以规避单纯隐藏技术引起的缺陷，保护数字图像所要表达的真实内容。

1 LSB 隐藏及图像置乱技术

1.1 LSB 技术

LSB(Least Significant Bit)是一种图像隐藏技术，它利用人眼对像素点细微改变的不敏感性，使用 R、G、B 3 种颜色的最低比特位来进行图像隐藏，其嵌入比为 12.5%，是目前公认信息隐藏量大的一种算法，同时还具有算法简单、嵌入速度快等优点。这些优点是一些基于变换域的隐藏算法所无法比拟的，因此 LSB 算法在信息隐藏领域中占有重要地位[8]。

但是，由于 LSB 隐藏算法仅仅将原图通过“填入”方式嵌入到载体图片中，而且使用了图像最低像素位，因此算法的鲁棒性有待提高，容易受到各种非正常攻击。比如攻击者在传输中将最低位置乱，这样接收者就不能接收到完整的信息。再者，LSB 算法仅仅使用了最低位，信息隐藏比也较低。

文献[8]利用在强背景下叠加一个弱信号，只要叠加的信号低于对比度门限，视觉系统就无法感觉到信号存在，根据 HVS(Human Visual System)的对比度特性，该门限值受背景照度、背景纹理复杂性和信号频率的影响。背景越亮，纹理越复杂(或者说边缘越丰富)，门限就越高[9]，这类现象称为亮度

收稿日期：2012-06-12 基金项目：2011 年度创新支撑计划-产学研合作促进计划(CXY1118)资助
作者简介：牛振喜(1969—)，西北工业大学副研究员、博士，主要从事系统工程研究。

掩蔽和纹理掩蔽。对 R、G、B 彩色图像而言,人类视觉系统对 LSB 位是不可感知的,但并不是只有对 LSB 位不可感知,对于较亮的像素点,例如,比 LSB 更高的某些位,同样是不可感知的,这些不可感知位也可用来嵌入信息,从而进一步提高嵌入容量。于是,文献 [8] 根据该原理,提出了一种新型隐藏算法,其嵌入比为 36%,隐藏量已相当可观。

1.2　置乱技术

置乱技术是对数字图像的空间域进行置换,或者修改数字图像的变换域参数使生成的图像变为完全看不懂的杂乱图像的过程,该过程是一个非线性变换过程,因而可以在二维矩阵内进行可逆的二维变换就可以实现图像置乱。在置乱技术发展史上,学者们提出了基于数学变换技巧的几种算法,包括 Arnold 变换、FASS 曲线、幻方变换、Gray 代码、生命模型等,被有效地应用于数字图像信息安全处理过程的预处理和后处理,更大程度地保证了数字图像的信息安全。在所有可逆二维混沌映射中,baker 映射的性能是最好的,所以在图像置乱隐藏中引入 baker 映射可以起到很好的隐藏效果。本文利用文献 [8] 中新型隐藏技术和 baker 映射结合,提出新型图像置乱隐藏算法。

2　基于 Baker 映射的图像置乱隐藏算法

2.1　Baker 映射

图像置乱的特点在于图像像素可以任意组合,像素可以插入到相邻像素之间。这样的排列和插入实质上就是拉伸和折叠的过程。Baker 映射是最典型的二维混沌映射之一。它把图像在宽度方向上拉伸,而在长度方向上进行压缩。把一个水平方向排列的图像变换成了一个垂直方向上排列的图像。

一个连续的 Baker 映射 $B(x,y)$ 可描述为

$$B(x,y) = \begin{cases} (2x, y/2), & 0 \leqslant x < 1/2 \\ (2x-1, y/2+1/2), & 1/2 \leqslant x < 1 \end{cases} \tag{1}$$

2.2　算法介绍

从文献 [8] 可知,分别在 R,G, B 位上最多隐藏 3,5,4 位信息位时,人眼无法分辨。假设待隐藏图像为 8 位灰度值图像,载体图片为 R、G、B 图像,可以将待隐藏图片的 8 位灰度值信息隐藏到载体图片的一个点中,为了实现方便,在 R,G,B 位上分别隐藏 2,4,2 位,这样,实际的隐藏将 8 位原图像先使用 baker 映射进行置乱,然后隐藏到载体图片中,这样虽然损失了一定的隐藏量,但是算法简单,且便于以后对隐藏置乱算法进行优化。

设原图像为 $G = \{g(i,j); (1 \leqslant i \leqslant n, 1 \leqslant j \leqslant n)\}$,为 8 位灰度值图像,大小为 $n * n$,其中 n 为能被 8 整除的数。

设原图像置乱后图像为 $B = \{b(i,j); (1 \leqslant i \leqslant n, 1 \leqslant j \leqslant n)\}$,大小为 $n * n$。

设载体图像记为 $M = \{m(i,j); (1 \leqslant i \leqslant n, 1 \leqslant j \leqslant n)\}$,为 24 位 R、G、B 彩色图像,大小为 $n * n$。

设隐藏后图像为 $L = \{l(i,j); (1 \leqslant i \leqslant n, 1 \leqslant j \leqslant n)\}$,为 24 位 R、G、B 彩色图像,大小为 $n * n$。

本文使用 Logistic 映射生成序列作为自己的密码: 一方面密码保存方便,只需要保存 Logistic 初始参数,就可生成长度无限制的密码序列; 另一方面,这样处理的算法具有更高的安全性,可防止密码被获取后图像被破解。下面介绍对原图像进行隐藏的过程:

1) 首先由初始条件生成 m 个序列,其中 m 值不定; m 个序列中,当序列值小于 0.5 时,Baker 映射序列选取 4,当 m 大于或等于 0.5 时,Baker 序列选取 2; 如此循环直到序列相加大于等于 n,当序列之和大于 n 时,最后一位改为 2,当相加序列等于 n 时,序列不变。

2) 通过步骤 1) 生成的序列对源图像 G 进行 Baker 置乱,得到图像 B。

3) 将得到的图像 B 隐藏到载体图片 M 中。根据上述结论,将 B 的每一个像素点根据 R、G、B 3 个像素点分别隐藏 2,4,2 位藏入载体图片 M 中,根据一一对应原则得到隐藏后的图片 L。

流程如图 1 所示:

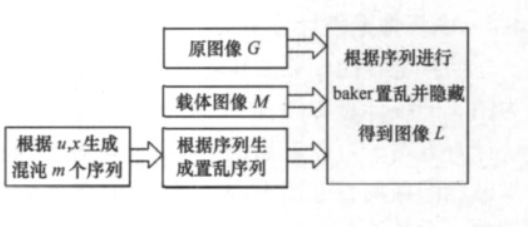

图 1　图像隐藏过程示意图

由于 Baker 映射式为单一映射,隐藏图片信息也为一一对应的像素点隐藏,在程序中,可以将映射

和隐藏设计成多进程，并行执行。

3 试验与分析

3.1 图像置乱算法密钥空间分析

论文中加密图片格式为 $8n * 8n$，在每一列上有(2,4)2 种选择，组合序列有(2,2,2,2)，(2,2,4)，(2,4,2)，(4,2,2)，(4,4)5 种选择，所以其密钥空间为 5^n，由于 n 的不确定性，密钥空间随着加密图片大小而改变；虽然密钥空间不是很大，不过由于其隐藏性较好，可以起到很好的信息保密效果。本文主要利用其隐藏性。

3.2 置乱方法实验结果与分析

载体图像为24位JPEG格式的Lena图像，秘密信息图像是8位BMP格式“1944年6月6日诺曼底登陆”信息图像。图2为Lena原图像，即载体图像，图3为BMP格式的待隐藏图像，图4为对待隐藏图像进行4轮置乱后的图像，图5为隐藏信息后的Lena图像。

图2 Lena原图像

图3 待隐藏图像

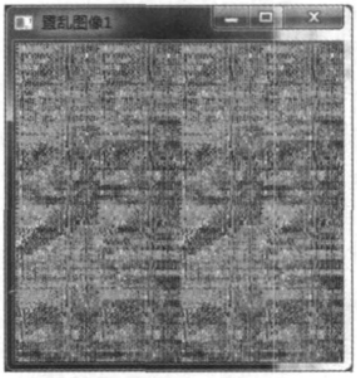

图4 待隐藏图像置乱4轮后的效果图像

图5 隐藏信息后的Lena图像

图6 待隐藏图像统计直方图

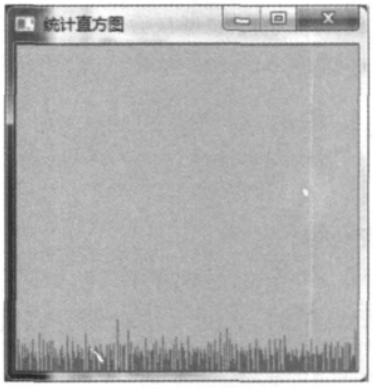

图7 隐藏信息后图像的统计直方图

3.3 图像像素统计分析

同样笔者比较原图和隐藏图像的直方图。图6为图3的统计直方图，图7为隐藏信息后图像5的统计直方图。可以看出，置乱并隐藏后图像直方图与原始图像的直方图有很大的不同，各像素值分布均匀。有效掩盖了原图像的分布规律，增加了破译难度。

3.4 PSNR和PMSE对保真度和失真分析

为了对图像隐藏的效果进行衡量，笔者利用该

领域通用的峰值信噪比(PSNR) 和均方根误差(PMSE) 来衡量载体图像和混合图像之间的客观保真度,给出载体图像 G 和混合图像 F,其基本运算方法如公式(2) 、(3) 所示。

$$PMSE = \left[\frac{1}{M \times N}\sum_{i=1}^{M}\sum_{j=1}^{N}(G(i,j) - F(i,j))^2\right]^{\frac{1}{2}} \quad (2)$$

$$PSNR = 10 \times \lg\left[\frac{M \times N \times 255^2}{\sum_{i=1}^{M}\sum_{j=1}^{N}(G(i,j) - F(i,j))}\right] \quad (3)$$

笔者针对上述实验数据利用 PSNR 和 PMSE 的计算公式得到数值结果展示在表 1 中。

表 1　PSNR 和 PMSE 计算结果

	PSNR	PMSE
图 3 和图 5	1. 721 58	163. 396

由以上实验和计算结果可知,原图像和隐藏图像,PMSE 值大于 160。从肉眼上无法分辨其差异,仅仅能从数据角度看出两者之间存在的变化,

通过对不同格式载体图像和秘密图像做实验,都得到了相同的结论,从而验证了算法的正确性和可行性。

与传统 LSB 算法比较可知,本文算法具有以下优点:

1) 隐蔽性强。经过 Baker 置乱,增加了秘密信息隐藏位置的随意性. 也增加了攻击的难度,由于秘密信息都是隐蔽在载体图像中每个字节的低 2 ~ 4 位,载体图像在隐藏秘密图像之前和隐藏之后难以区分。

2) 容量明显提高。若载体图像的大小为 N 字节. 则可以隐藏的秘密信息图像的大小约为 $N/3$;

3) 实用性好。本算法中的秘密信息可以是任何格式的文件,从而增加了隐藏的质量和性能。

4) 秘密信息的提取容易。只需提供跟加密相同的初始参数,即可从隐藏了秘密图像的载体像中提取秘密信息。

4　结　论

本文在基于传统 LSB 算法的基础上,根据人眼对 R、G、B 3 种颜色敏感度不同,在 3 种颜色分量上分别隐藏不同信息量。即在 R,G,B 3 种颜色分量上分别隐藏 2,4,2 位信息位,这样每一个 8 位色深的灰度值图像就可以隐藏到 24 位 R、G、B 彩色图像中,且具有一一对应的关系,因此,可以利用 Baker 映射进行图像置乱,置乱的次数与使用者对安全性要求相关。

参考文献:

[1] 李　鹏,田东平,张　楠. 基于混沌序列的数字图像隐藏技术. 信息安全与通信保密, 2007, 6: 22-225
Li Peng, Tian Dongping, Zhang Nan. Digital Image Hiding Method Based on Chaotic Sequence. Information Security and Communications Privacy, 2007, 6: 22-225 (in Chinese)

[2] 汤光明,王亚弟. 信息隐藏安全性研究. 计算机工程, 2008, 34(16) : 183-185
Tang Guangming, Wang Yadi. Research on Security of Information Hiding. Computer Engineer, 2008, 34(16) : 183-185 (in Chinese)

[3] Osamu Matoba, Bahram Javidi. Optically Encrypted Data Storage Using Multi-Dimensional Keys. IEEE Lasers and Electro-Optics Society 12th Annual Meeting, San Francisco, CA, USA, 1999, 8: 66-67

[4] Elaine Shi John Bethencourt T H. Hubert Chan Dawn Song Adrian Perrig. Multi-Dimensional Range Query over Encrypted Data. 2007 IEEE Symposium on Security and Privacy, Berkeley, CA, United states, 2007, 20: 350-364

[5] 戴　蒙,林家骏,毛家发. 一种基于粗糙集属性约简的图像隐藏信息检测方法. 华东理工大学学报(自然科学版) , 2008, 34(1) : 122-125
Dai Meng, Lin Jiajun, Mao Jiafa. Steganalysis Based on the Rough Set Attribute Reduction. Journal of East China University of Science and Technology (Natural Science Edition) , 2008, 34(1) : 122-125 (in Chinese)

[6] 邱应强,张育钊,杜吉祥,郭荣新. 一种用于矢量量化压缩图像的信息隐藏新方法. 电子与信息学报, 2008, 30(7) : 1695-1699
Qiu Yingqiang, Zhang Yuzhao, Du Jixiang, Guo Rongxin. A Novel Information Hiding Method for VQ Compressed Images.

Journal of Electronics & Information Technology, 2008, 30(7): 1695-1699 (in Chinese)

[7] 刘一均. 图像掩密分析及伪造认证算法研究. 重庆大学, 2007
Liu Yijun. Image Steganalysis and Study on Algorithm of Images Steganography. University of Chongqing, 2007 (in Chinese)

[8] 谢建全,阳春华. 大容量的信息隐藏算法. 计算机工程, 2008, 34(8): 167-169
Xie Jianquan, Yang Chunhua. High Capacity Information Hiding Algorithm. Computer Engineer, 2008, 34(8): 167-169 (in Chinese)

[9] Jayant N, Johnston J, Safranek R. Signal Compression Based on Models of Human Perception. Proceedings of the IEEE, 1993, 81(10): 385-1422

An Effective Hiding Algorithm Based on LSB(Least Significant Bit) and Scrambling

Niu Zhenxi

(Office of University Research, Northwestern Polytechnical University, Xi'an 710072, China)

Abstract: Starting from the traditional LSB algorithm, I developed a new hiding algorithm. Sections 1 though 3 of the full paper explain the new hiding algorithm and its evaluation. Baker algorithm and image scrambling are used to make security of data better. Experimental results and their analysis prove preliminarily that the algorithm has ample key space and good hiding effect.

Key words: algorithms, efficiency, security of data; image scrambling, least significant bit (LSB)