

## 基于混沌加密的彩色图像自适应密写算法

岳 乐, 彭 波

(中国农业大学信息与电气工程学院, 北京 100083)

(bobbyv@gmail.com)

**摘 要:**提出了一种新的利用混沌信号作为密钥流对密写信息进行加密,进而根据载体图像特性进行分块,自适应调节嵌入深度的最低比特位(LSB)密写算法。实验结果表明,该密写算法具有较好的隐蔽性,以及较大的隐藏容量。通过对彩色图片的密写来进行文本信息传输,较好地解决了在互联网上信息传输的通信安全问题。

**关键词:**密写;彩色图像;混沌系统;恰可察觉失真阈值;最低比特位

**中图分类号:**TP309;TP391 **文献标志码:**A

## Adaptive color image steganography algorithm based on chaos encryption

YUE Le, PENG Bo

(College of Information and Electrical Engineering, China Agriculture University, Beijing 100083, China)

**Abstract:** A new kind of design and implementation of a steganography algorithm based on Least Significant Bit (LSB) was proposed, which used chaos system as key to encrypt the steganography information, then according to the image characteristic, adaptively regulated embedding depth. The results suggest: good invisibility can be achieved, and the hiding capacity of information is large. The new steganography algorithm, based on the color image, solves the communication security problem of the information at Internet well.

**Key words:** steganography; color image; chaos system; JND threshold value; Least Significant Bit (LSB)

### 0 引言

密写是信息隐藏的一个重要分支,其目的是将信息秘密地、安全地传递给接收方,而不引起第三方的怀疑。相对于传统将信息加密为密文的信息加密,密写是将有用信息隐藏到另一个公开的信息媒体中,是对信息存在本身或信息存在位置的保密。鉴于密写比信息加密更安全以及网络与信息安全问题变得越来越重要,密写已经成为当前国际上的研究热点。

密写信息能够隐藏在彩色图像中,其依据:

1) 彩色图像本身存在大量冗余。从信息论的角度看,彩色图像信息的编码效率不是很高。所以在其中嵌入一定量的密写信息是完全可行的,并不影响图像本身的传送和使用。

2) 人眼具有一定的掩蔽效应,比如对灰度的可分辨率只有几十个灰度级;对边沿附近的信息不敏感。利用人眼的这些特点,可以很好地将信息隐藏在多媒体载体中而不易被察觉。

到目前为止,还无法建立密写技术的完整理论;密写的重要特性——隐蔽性、嵌入数据量、稳健性三者如何达到最优,是密写研究的难点。利用人类视觉系统的视觉掩蔽性,是解决这一矛盾的有效方法之一。

本文提出了一种利用混沌信号作为密钥流对信息进行加密,进而根据载体图像特性进行分块,自适应地调节嵌入深度的密写算法。并用 Matlab 进行了仿真实验,实验结果表明,用该算法进行密写具有较好的隐蔽性,且具有较大的隐藏容量。

### 1 传统的 LSB 算法

密写算法基本上分为两大类:空域法和频域法。空域法

是直接改变图像元素的值;频域法是利用某种数学变换,将图像用频域表示,通过改变图像的某些频域系数加入密写消息,再利用反变换来生成隐藏有其他信息的图像。其中,最低比特位(Least Significant Bit, LSB)密写<sup>[1]</sup>即用秘密信息位来替换最不重要位,是空域法中的常见算法。这种算法实现比较容易,而且隐藏量大。如一幅  $256 \times 256$  的彩色图像,传统 LSB 算法的最大隐藏容量是  $3 \times 256 \times 256$  bit。传统 LSB 算法虽然隐藏容量较大,但隐蔽性不够佳。

### 2 混沌加密

英国数学家 Matthews 于 80 年代末,首先明确地提出了用混沌系统来产生序列密码的思想。他分析了用 Logistic 混沌映射作为密码序列产生器的实际问题,其后相关的研究又有了一定的进展。目前,随着非线性和混沌理论的成熟,研究者纷纷探索混沌在多媒体数据加密中的可能应用。

本文提出的算法为了提高密写信息的安全性,利用混沌信号作为密钥流对密写信息进行加密。首先采用 Logistic 映射法生成混沌序列,然后再将混沌序列与密写信息生成的二进制编码进行异或运算,得到经加密处理的二进制数字序列。具体实现步骤如下:

1) 生成混沌序列。

选择 Logistic 方程作为模型,方程的形式为:

$$X_{n+1} = \mu X_n (1 - X_n), X_n \in (0, 1), \mu \in (3.5699), n = 0, 1, 2, \dots \quad (1)$$

本算法选定  $X_0 = 0.5$ ,  $\mu = 3.9$ , 得到实数序列:

$$X = \{X_i | 0 < X_i < 1; i = 1, 2, 3, \dots\} \quad (2)$$

收稿日期:2007-04-09;修回日期:2007-06-22。

作者简介:岳乐(1982-),女,内蒙古包头人,硕士研究生,主要研究方向:信息隐藏;彭波(1960-),女,北京人,教授,博士研究生,主要研究方向:信息隐藏。

图 1 为混沌序列的轨迹点形成的点线图。从图 1 可以看出,混沌序列变化没有规律,类似随机现象,要对系统进行长期预测是不可能的。将其应用到密写信息中,可以提高密写信息的随机性,增大攻击难度。

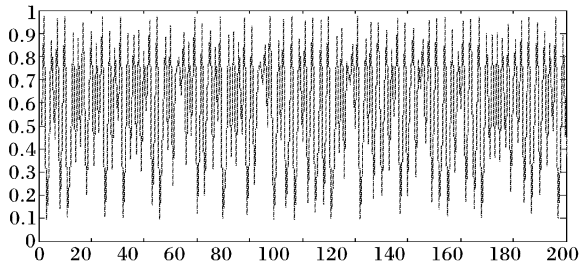


图 1 混沌序列轨迹点生成的点线图

2) 根据生成的混沌序列,对信息进行加密。

首先,将式(2)产生的混沌序列依据式(3)进行归一化处理,得到混沌二值序列  $S$ ,如式(4)。

$$T(x) = \begin{cases} 0, & \text{if } 0 < X \leq 0.5 \\ 1, & \text{if } 0.5 < X < 1 \end{cases} \quad (3)$$

$$S = \{S_i \mid S_i = T(X_i); i = 1, 2, 3, \dots\} \quad (4)$$

其次,将密写信息转化为二进制数字序列:

$$M = \{m_0, m_1, m_2, \dots\} \quad (5)$$

最后,将式(4)混沌二值序列与式(5)密写数字序列进行异或运算,得到加密的密写信息。

### 3 载体图像的分块

#### 3.1 理论依据

保证秘密信息的不可见性和提高密写容量的有效途径,是充分利用人眼的视觉特性。心理视觉的研究表明<sup>[2-4]</sup>,人眼对图像平滑区的噪声较敏感,而对较复杂纹理区的噪声不敏感。因此,有必要根据视觉掩蔽效应将图像划分成不同的类别,以便在不同的噪声敏感区域分别嵌入不同的信息量,自适应地对密写深度进行调节。图 2 为本算法对载体图像的分块流程:

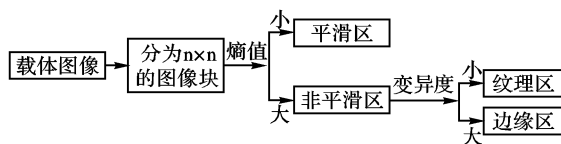


图 2 载体图像的分块流程

#### 3.2 具体实现

对图像进行子块划分(如  $8 \times 8, 4 \times 4$  等),计算每一块的熵值和变异度。根据熵值和变异度将图像子块归为三类:平滑块、边缘块和纹理块。只要选取合适的熵和变异度阈值,即可将图像划分为以上三种不同属性的块。

1) 选取熵的最佳阈值

熵在信息论中是描述信源的平均信息量<sup>[6]</sup>。在图像分类中,可以应用熵这个概念来衡量一幅图像的复杂程度,熵值越小,包含信息量越少,对应的图像部分变化越少,也就是说这部分图像较为平滑;反之,包含信息量多,对应的图像部分变化复杂,也就是说这部分图像包含纹理和边缘部分,因此利用熵值的大小可以划分平滑区和非平滑区。图像子块熵值的计算方法:设图像有  $S_1, S_2, \dots, S_q, q$  种幅值,并且出现的概率为  $P_1, P_2, \dots, P_q$ ,那么每一幅值信息量为  $\log_2 P_i$ ,则其熵值为:

$$H = - \sum_{i=1}^q P_i \times \log_2 P_i \quad (6)$$

据此,计算出一个  $8 \times 8$  图像块的最大熵值为 6,而通过对多幅标准图像进行平滑区与非平滑区的划分测试,4.5 为最佳阈值。即图像最大熵值的 75% 作为划分平滑与非平滑区的阈值。

2) 选取变异度的最佳阈值

方差用于表示数据分布和离散程度的一维统计特性。方差越大,说明该数据集与平均值的差异越大,数据离散程度越大;反之,则说明该数据集与平均值的差异越小,数据离散程度越小。但方差随像素灰度值的变化起伏较大。因此利用方差进行多组数据的比较就显得不太合理,而利用变异度(Coefficient of Variance, CV)则更为合适,它在数量上度量了一个总体的变异性相对于其总体均值的大小,标准方差为:

$$s = \frac{1}{n-1} \sum_{x,y \in B_{i,j}} [f(x,y) - \bar{f}]^2 \quad (7)$$

式中,  $n$  为图像块  $B_{i,j}$  中元素的个数;  $f(x,y)$  为图像块  $B_{i,j}$  中像素点的灰度值;  $\bar{f}$  图像块  $B_{i,j}$  的平均灰度。变异度为:  $c = s/\bar{F}$ 。其中  $\bar{F}$  为图像的平均灰度值。通过 canny 算子对多幅标准图像进行边缘检测,实验结果表明,最大变异度的 25% 是划分边缘区与纹理区的最佳阈值。

### 4 密写的实现

#### 4.1 密写信息的嵌入过程

密写的本质是用某种方式改变图像像素点的值而不引起观察者视觉上的改变。图像每个像素值的改变有一定的限度而且应该是不可察觉的,这种限度称作恰可察觉失真(Just Noticeable Distortion, JND)<sup>[6]</sup>。在对载体图像进行密写时,当嵌入的信息量低于 JND 阈值,原图的变化将不会被察觉。在密写中利用 JND 阈值,不仅保证密写信息的不可见性,也增强了密写信息的鲁棒性。

大量统计结果表明,平滑区、边缘区和纹理区对应的 JND 阈值分别为 2、4、10<sup>[7]</sup>。据此,本算法分别在平滑区、边缘区和纹理区自适应的选取末位、末 2 位、末 3 位嵌入密写信息;像素值依次最多变化 1、3、7,均低于 JND 阈值。因此,该密写算法中,信息嵌入位不再是一个固定的值,载体图像的纹理复杂程度不同的区域,嵌入深度是不同的,这样就可以在视觉允许的范围,更充分地利用载体图像的信息冗余,使载体图像的信息隐藏能力得到充分发挥。攻击者也很难知道密写者究竟利用了哪些低比特位进行信息隐藏。因此,这种 LSB 密写算法既保证了隐秘性,又能够最大限度地嵌入密写信息以及具有较好的鲁棒性。

将彩色图像分为 R、G、B 三层,分别进行如下操作:

1) 按照混沌加密的步骤,对信息进行加密;

2) 按照图像的划分规则,区分每个块属于平滑区、边缘区还是纹理区,并作相应标记;

3) 依次扫描每个图像块,进行自适应地信息嵌入。即分别在平滑区、边缘区、纹理区自适应地选取末位、末 2 位、末 3 位嵌入密写信息;

4) 将 R、G、B 层组合为含密写信息的图像。

#### 4.2 密写信息的提取过程

提取过程为嵌入过程的逆过程。提取内容转化为 txt 文件,与原信息一字不差。

### 5 实验

目前对于隐蔽图像和载体图像,多采用考虑人眼视觉系

统掩蔽特性的加权均方根误差 (weighted RMSE, wRMSE) 和加权峰值信噪比 (weighted PSNR, wPSNR) 来反映误差和客观保真度。

隐蔽图像  $P$  和载体图像  $Q$  的加权均方根误差为:

$$wRMSE = \left\{ \frac{1}{M \times N} \sum_{i=1}^n \sum_{j=1}^n w(i, j) \times [P(i, j) - Q(i, j)]^2 \right\}^{-1/2} \quad (8)$$

其中,  $w(i, j)$  表示图像在  $(i, j)$  处的像素所属的平滑区、边缘区和纹理区的加权系数。针对人类视觉系统特性,  $w(i, j)$  分别设置为 1.9、1.0、0.1<sup>[7]</sup>。

隐蔽图像  $P$  和载体图像  $Q$  的加权峰值信噪比为:

$$wPSNR = 10 \log_{10} (255^2 / wRMSE^2) \quad (9)$$

加权峰值信噪比  $wPSNR$  作为图像客观保真度准则, 它的值越大, 说明隐蔽图像的保真度越好, 这两幅图像越相似。

利用传统 LSB 算法和本算法对  $256 \times 256$  的彩色图像做了大量 Matlab 仿真实验, 并对密写前后的图像进行性能分析。本文仅给出 Lena 标准图像的测试结果, 所采用的秘密信息是包含字母、数字、汉字的 txt 文件, 测试结果见表 1、2。

表 1 传统 LSB 末 2 位嵌入的测试结果

层	嵌入量 (bit)	隐藏率	wRMSE	wPSNR
R	123 072	2	0.892 08	49.123
G	141 952	2	0.825 12	49.801
B	129 600	2	0.857 58	49.465

表 2 本文提出算法的测试结果

层	嵌入量 (bit)	隐藏率	wRMSE	wPSNR
R	123 072	1.877 93	0.609 83	52.427
G	141 952	2.166 02	0.789 56	50.183
B	129 600	1.977 54	0.776 98	50.323

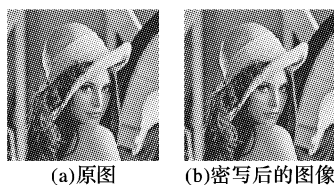


图 3 实验结果

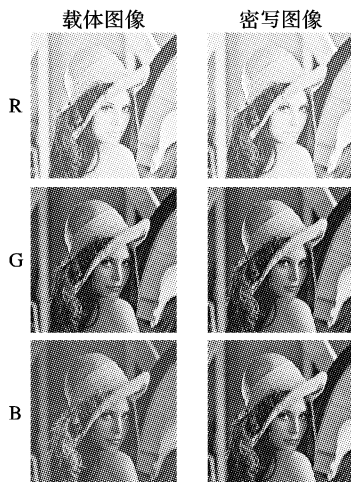


图 4 隐藏前后的图像对比

对比表 1 和表 2, 总的隐藏率相当, 但本文提出算法的保真度更好。传统 LSB 算法本身的安全性不够, 容易被别人提取。表 2 对应的算法说明了本算法不仅具有较高的隐藏率,

隐藏容量一般为载体图像的 20%, 而且 wPSNR 也相当高。同时密写信息经混沌加密以及根据载体图像特性进行分块, 自适应地调节嵌入深度进行密写, 安全性好, 即使别人知道该载体含有秘密信息, 也无法正确提取。

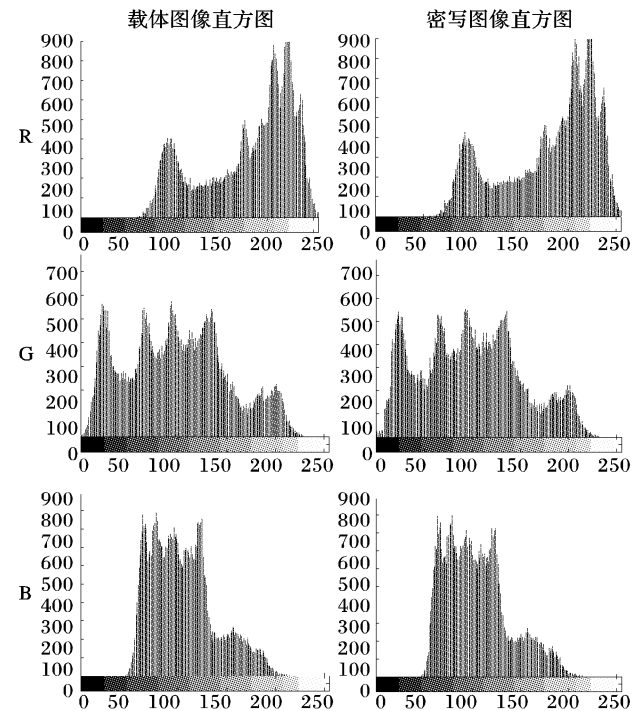


图 5 隐藏前后的直方图对比

密写前后图像对比如图 3 示, 密写前后 R、G、B 层的直方图以及图像对比如图 4、5 所示。从图 5 可以看出, 原图和密写图像在直方图统计上变化不大, 说明该算法具有良好的隐蔽性。

## 6 结语

本文提出的利用混沌信号作为密钥流对密写信息进行加密, 进而根据载体图像特性进行分块, 自适应地调节嵌入深度的数字密写算法, 经实验表明, 具有较好的隐蔽性以及较大的隐藏容量。通过对彩色图像的数字密写来进行文本信息传输, 较好地解决了在互联网上信息传输的通信安全问题。

## 参考文献:

- [1] BENDER W, GRUHL D, MORIMTO N, *et al.* Techniques for data hiding [J]. IBM System Journal, 1996, 35(3&4): 313-335.
- [2] KANKANHALLI M S, RAMAKRISHNAN K R. Content Based Watermarking of Images [C]// Proceedings of the 6th ACM International Conference on Multimedia, New York: ACM Press, 1998: 61-70.
- [3] 尹康康, 石教英, 潘志庚. 一种鲁棒性好的图像水印算法[J]. 软件学报, 2001, 12(5): 668-676.
- [4] 黄继武, SHI Y Q, 姚若河. 基于块分类的自适应图像水印算法[J]. 中国图象图形学报, 1999, 4A(8): 640-643.
- [5] 姜玉宪. 信息技术导论[M]. 北京: 北京航空航天大学出版社, 1991: 35-37.
- [6] YANG X K, LIN W S, LU Z K, *et al.* Just-noticeable-distortion profile with nonlinear additivity model for perceptual masking in color images [C]// Proceedings of IEEE Conference on Acoustics, Speech & Signal Processing (ICASSP2003). Hongkong: IEEE Press, 2003: 609-612.
- [7] 胡彦. 人类视觉系统及其在信息隐藏中的应用研究[D]. 福州: 福州大学, 2002.