第38卷 第18期
Vol.38 No.18

计 算 机 工 程
Computer Engineering

2012年9月
September 2012

• 安全技术 •

文章编号：1000—3428(2012)18—0097—03 文献标识码：A 中图分类号：TP309

最小化扭曲的抗检测隐写算法

刘 华，汤光明

(解放军信息工程大学电子技术学院，郑州 450004)

摘 要：为提高秘密数据传输的安全性，提出一种最小化扭曲的图像隐写算法。根据图像平滑特性及具体隐写嵌入操作对特性的影响为载体像素分配扭曲值，以表征在该像素上进行特定嵌入操作对图像总体统计特性的影响程度，再利用STC码选择使图像整体扭曲函数最小的嵌入位置和嵌入方式进行信息嵌入。仿真实验结果表明，该算法具有良好的抗检测性。

关键词：信息隐藏；隐写术；隐写码；扭曲函数；平滑度；STC码

Undetectable Steganographic Algorithm of Minimized Distortion

LIU Hua, TANG Guang-ming

(Institute of Electronic Technology, PLA Information Engineering University, Zhengzhou 450004, China)

【Abstract】In order to improve the security of secret data transmission, a steganographic algorithm of minimized distortion is proposed. In order to express the influence of the pixel modification on the whole statistic character, scalar values are assigned to every pixel based on smoothness and impact of different embedding mode on it. Embedding is actualized by choosing the proper embedding position and mode utilizing Syndrome-trellis Codes(STC). Experiments show that the proposed algorithm possesses a good undtetability.

【Key words】information hiding; steganography; steganographic code; distortion function; smoothness; Syndrome-trellis Codes(STC)

DOI: 10.3969/j.issn.1000-3428.2012.18.026

1 概述

隐写术作为信息隐藏的重要分支，将秘密信息隐藏于普通公开的信息(如音频、图像或视频等)中传输，保证信息安全传输是隐写算法的目标。抗检测隐写算法因为其良好的安全性成为目前隐写领域的研究热点，它通过定义载体与隐秘体的差异，利用隐写码生成差异较小的隐秘体[1]。F5、文献[2-4]算法都属于此类算法。其中，文献[4]是Filler最新提出的抗检测隐写算法，它基于像素与邻域关系定义差异，相关数据表明其安全性优于前述算法。Filler设计的STC码[5-6]对载体与隐秘体差异定义具有普适性，可利用其生成与载体差异最小的隐秘体。

然而目前的抗检测算法也存在以下不足：(1)差异未反应载体特性；(2)差异定义没有考虑嵌入操作对载体的影响，从而使算法存在缺陷。针对以上不足，本文设计并实现了一种抗检测隐写算法，根据图像平滑特性及具体隐写嵌入操作对特性的影响构造扭曲函数，并分析其有效性。

2 扭曲函数构造

合理定义差异，使之与抗检测性紧密联系是抗检测算法需解决的关键问题，本文通过扭曲函数 D 来衡量载体与隐秘体间的差异。

2.1 扭曲函数

$X=\{x_1,x_2,\cdots,x_n\}\in\chi(\chi=\{I\}^n)$ 表示由 n 个像素构成的图像载体，x_i 表示图像中第 i 个像素；$Y=\{y_1,y_2,\cdots,y_n\}\in\chi$ 表示隐秘体。I 表示像素的取值范围，如8 bit PNG图像的 $I=\{0,1,\cdots,255\}$，$I_i\in I$ 为嵌入信息后像素 x_i 所有可能取值的集合。如在LSB匹配算法中，$I_i=\{x_{i-1},x_i,x_{i+1}\}\cap I$。

定义 1(加性扭曲函数) 为所有 $x_i\in\chi$ 对应于 I_i 上的每个 y_i 分配一个实数(或无穷大)，以表示在 x_i 上进行该嵌入操作带来的失真，称该实数为像素 x_i 对应于嵌入操作 y_i 的扭曲度，记为 $\rho_i(x_i,y_i)$。定义加性扭曲函数[3]为：

$$D(X,Y)=\sum_{i=1}^{n}\rho_i(X,y_i) \tag{1}$$

本文选择LSB匹配嵌入方式，即 $|I_i|=3$，所以像素扭曲度 ρ_i 是一个三元组：$[\rho_i^{-1},\rho_i^0,\rho_i^1]$。3个元素分别表示对像素 x_i 做加1、减1操作和 x_i 不发生变化时的扭曲度。

2.2 图像平滑特性分析

根据像素与其邻域像素差值衡量像素邻域平滑程度，进而将信息嵌在平滑度较差的位置来减少嵌入对图像特性的修改是自适应隐写算法的基本思路。本文借鉴以上思想，利用像素邻域平滑特性构造扭曲函数。

像素间相关性随像素间距离的增大而较弱[7]，所以本

基金项目：河南省信息安全重点实验室基金资助项目(09ISLB001)

作者简介：刘 华(1985－)，女，硕士研究生，主研方向：信息隐藏；汤光明，教授、博士生导师

收稿日期：2011-09-30 **修回日期：**2011-11-21 **E-mail：**liuhua_yw@163.com

文在像素 24 邻域上分析区域平滑特性和定义扭曲度，即 $\rho_i(X,y_i)=\Theta(x_{\sigma(i)},y_i)$，$x_{\sigma(i)}$ 表示像素 x_i 邻域内的像素。

在 24 邻域内，分别计算像素在水平、垂直、主对角线和幅对角线 4 个方向的差值对。水平方向 3 组差值对由下式表示：

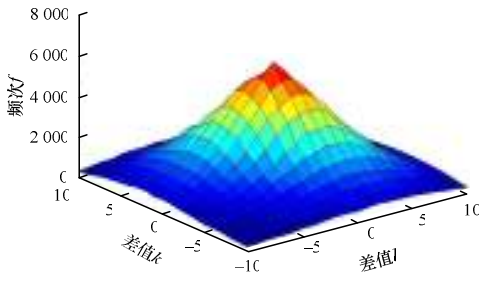
$$D^{\text{hor}}(x_{i,j})=\{(x_{i,j-2}-x_{i,j-1},x_{i,j-1}-x_{i,j}),(x_{i,j-1}-x_{i,j},x_{i,j}-x_{i,j+1}),(x_{i,j}-x_{i,j+1},x_{i,j+1}-x_{i,j+2})\} \tag{2}$$

同理可得其他方向的差值对，分别记为 D^{ver}、D^{dia} 和 D^{off}，令 $D(x_{i,j})=D^{\text{hor}}\cup D^{\text{ver}}\cup D^{\text{dia}}\cup D^{\text{off}}$。

若 $D(x_{i,j})$ 中元素都在 (0,0) 附近，则说明 $x_{i,j}$ 邻域平滑度较好。为量化像素邻域平滑程度，便于扭曲度定义，引入参数集 $\theta\in R^{(2\Delta+1)^2+1}$：阈值 $\Delta>0$，对于 $\forall(k,l)$，当 $-\Delta\leqslant k$，$l\leqslant\Delta$ 时，其对应参数为 $\theta_{k,l}\geqslant 0$；当差值对中任意差值超出 $[-\Delta,\Delta]$ 时，对应参数为 θ_{out}。

自然图像可看作局部平稳信源、局部区域内像素灰度取值之间相关性较强，将图像像素与其邻域像素的差 TD(包括各个方向的邻域像素)看作随机变量，则 TD 近似服从广义拉普拉斯分布，其统计概率在 0 处达到最大且关于 0 点偶对称。将其扩展至二维差值对，实验说明上述结论仍然成立：统计图像差值对 (k,l) 出现的频次 $f_{k,l}$，其在 (0,0) 处取得最大值，且关于 (0,0) 点近似偶对称。图 1(a) 是 NRCS 图像库中 512×512 像素的 Lena 图像[8]，图 1(b) 是其 (k,l) 分布($\Delta=10$)。

(a)Lena 图



(b)Lena 图的(k,l)分布

图 1 Lena 图及其 (k,l) 分布

$m\times n$ 的载体图像 X，其参数集 θ 构造方法如下：

$$T=m(n-2)+n(m-2)+2(m-2)(n-2)$$

$$\theta_{k,l}=f_{k,l}/T$$

$$\theta_{\text{out}}=\min(\theta_{k,l})\times\left(T-\sum_{i=-\Delta}^{\Delta}\sum_{j=-\Delta}^{\Delta}f_{k,l}\right)/T \tag{3}$$

由式(3)易得，$\theta_{k,l}$ 是频次 $f_{k,l}$ 的单调函数，因此 $\max(\theta)=\theta_{0,0}$；随着 (k,l) 距 (0,0) 的距离增大，$\theta_{k,l}$ 的值减小；$\min(\theta)=\theta_{\text{out}}$。

定义 2(平滑度) 设 $x_{i,j}$ 为图像 X 上第 i 行、第 j 列的像素，令 $s(x_{i,j})$ 为集合 $D(x_{i,j})$ 上所有差值对对应参数 θ 的平方和，称 $s(x_{i,j})$ 为 $x_{i,j}$ 邻域的平滑度：

$$s(x_{i,j})=\sum_{(k,l)\in D(x_{i,j})}\theta_{(k,l)}^2 \tag{4}$$

由定义得，若 $D(x_{i,j})$ 中元素都在 (0,0) 附近，则对应的 θ 参数值较大，从而 s 值较大，表示像素邻域平滑度较好。

2.3 扭曲度定义及分析

像素 $x_{i,j}$ 的扭曲度 $\rho_{i,j}$ 定义如下：

$$\rho_{i,j}=\begin{cases}0 & \text{if } y_{i,j}=x_{i,j}\\ s(x_{i,j})+|s(y_{i,j})-s(x_{i,j})| & \text{otherwise}\end{cases} \tag{5}$$

分析扭曲度定义，当 $x_{i,j}$ 平滑度较好时，其 s 值较大，从而 $\rho_{i,j}(x,y)$ 较大。扭曲度确定后即可利用 STC 生成隐秘体。

STC 由一个长度为 n，维数为 $n-m$ 的线性码 ς 实现，其嵌入和提取模型如下：

$$Emb(X,M)=\arg\min_{Y\in\varsigma(M)}D(X,Y) \tag{6}$$

$$Ext(Y)=\boldsymbol{H}Y \tag{7}$$

其中，$\boldsymbol{H}\in\{0,1\}^{m\times n}$ 是码 ς 的奇偶校验矩阵，$\varsigma(M)=\{z\in\{0,1\}^n\mid \boldsymbol{H}z=M\}$ 是秘密消息 M 的陪集。由式(6)知，隐秘体的 D 值最小；由式(7)得，接收方无需知道 $\{\rho_i\}$，只需 $\boldsymbol{H}$ 即可从接收到的隐秘体中提取 M，STC 编码过程详见文献[5-6]。

根据 STC 原理，信息将嵌入在扭曲度较小的位置，而由式(5)知邻域平滑度较好的像素 ρ 值较大，所以被改变概率较小。密文消息将被嵌在邻域平滑度较差的位置，这与自适应隐写思想一致，从而使载体特征改变较小，达到抗检测目的。

嵌入像素位置一定，则其 s 值一定，对像素邻域平滑度改变较大的嵌入方式对应的扭曲度较大。根据 STC 原理，信息将以扭曲度较小的嵌入方式嵌入，即选择对像素邻域平滑度改变较小的嵌入方式。

综上，利用本文构造的扭曲函数结合 STC，可选择对载体统计特性改变小的嵌入位置和嵌入方式实现信息嵌入，即可有效抵抗检测算法的攻击。

3 隐写算法设计

3.1 嵌入算法

基于第 2 节构造的扭曲函数和 STC，本节实现扭曲最小化的隐写算法，图 2 为嵌入框图。

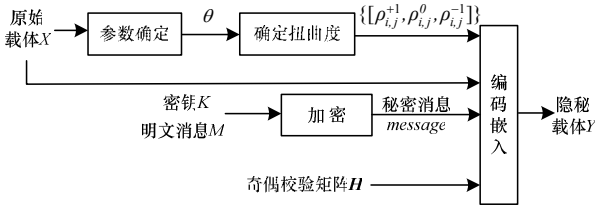


图 2 嵌入框图

嵌入过程包括确定参数、计算扭曲度、明文加密及编码嵌入 4 个部分，具体步骤如下：

Step1 输入载体图像 X、明文消息 M。

Step2 判断 M 长度 L_M 是否小于图像容量 $m\times n$，若是则继续，否则跳出。

Step3 输入阈值 Δ(本文取 10)、密钥 K 及奇偶校验矩阵 $\boldsymbol{H}$。

Step4 确定图像的参数集 θ；为图像像素确定扭曲度 $\{\rho_{i,j}\}$。

Step5 使用密钥 K 加密明文消息 M。

Step6 利用 STC 将已加密消息嵌入原始载体中，输出扭曲函数值最小的隐秘体 Y。

3.2　提取算法

提取算法如图 3 所示，其中，实线表示公开信道，虚线表示秘密信道。

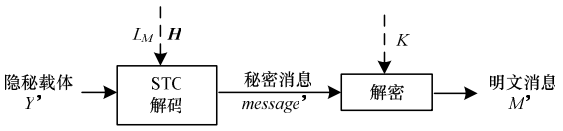


图 3　提取框图

提取算法包括 STC 解码及解密 2 个模块，具体步骤如下：

Step1 从公开信道获取隐秘体 Y'。

Step2 从秘密信道获取 L_M 和密钥 K。

Step3 进行 STC 解码运算，得到秘密消息 $message'$。

Step4 利用密钥 K 对 $message'$ 解密，得到明文消息 M'。

4　仿真实验及性能分析

实验环境为 MatlabR2008a 平台；硬件为 Pentium® 4 3.0 GHz。选取图像库 NRCS[8]中的 1 000 幅图像，将其全部转化为 512×512 像素大小的 PNG 图像。明文消息为随机 01 序列，分类器为 Fisher 线性分类器(简称 FLD)。

本节拟利用分类器的最小错误率 P_e 来衡量算法的抗检测性：

$$P_e = \min(P_{Fp} + P_{Fn})/2$$

其中，虚警率 P_{Fp} 为分类器将载体判定为隐秘体的概率；漏警率 P_{Fn} 为分类器将隐秘体判定为载体的概率。P_e 值越大，表示分类器的错误率越高，即算法的抗检测性越好。

实验步骤如下：(1)利用本文算法、文献[4]算法和 LSB 匹配算法分别生成嵌入率 α(实际嵌入比特数与图像像素数之比，单位为 bbp)为 10%,20%,…,100%的隐写图像；(2)将不同隐写率的隐写图像及对应载体分成等大的训练和测试集；(3)在各训练集的图像中提取 2 阶 SPAM 特征，进行分类器训练(分类器门限为训练集中载体和隐写图像样本均值向量的平均)；(4)利用训练所得分类器对对应的测试集进行检测，统计 P_{Fp}、P_{Fn} 和 P_e。

图 4 中曲线、带圆圈曲线和带星号曲线分别是分类器对 LSB 匹配、文献[4]算法和本文算法的 α-P_e 曲线。分析实验结果可知：(1)分类器对本文与文献[4]算法的平均最小错误率明显高于对 LSB 匹配算法的检测错误，即抗检测隐写算法安全性高于 LSB 匹配算法；(2)本文算法在定义扭曲度时考虑了图像平滑特性及嵌入操作的影响，使扭曲函数与抗检测性联系紧密，所以抗检测性能高于文献[4]算法；(3)随着 α 增大，为保证信息完全嵌入，信息被嵌在扭曲度大的位置导致算法抗检测性能降低，接近于 LSB 匹配算法的抗检测性。

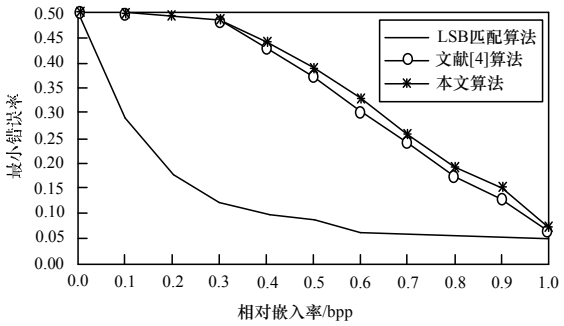


图 4　3 种算法抗检测性对比

5　结束语

本文提出了根据像素邻域平滑特性及不同嵌入操作对特性的影响定义扭曲函数，为信息嵌入提供有效指导，并通过 STC 生成扭曲函数值最小的隐秘体的图像隐写算法。对比实验验证了本文算法抵抗检测攻击的有效性。但是本文的隐写算法只能以图像为载体，基于音频等其他类型载体的抗检测隐写算法是今后研究的方向。

参考文献

[1] Fridrich J, Filler T. Practical Methods for Minimizing Embedding Impact in Steganography[C]//Proc. of SPIE'07. Orlando, USA: [s. n.], 2007.

[2] 朱雪秀, 刘九芬, 张卫明. 一种基于汉明码和湿纸码的隐写算法[J]. 电子与信息学报, 2010, 32(1): 162-165.

[3] Pevny T, Filler R, Bas P. Using High Dimensional Image Models to Perform Highly Undetectable Steganography[C]//Proc. of the 12th International Conference on Information Hiding. Albetta, Canada: [s. n.], 2010.

[4] Filler T, Fridrich J. Design of Adaptive Steganographic Schemes for Digital Images[C]//Proc. of SPIE'11. San Francisco, USA: [s. n.], 2011.

[5] Filler T, Judas J, Fridrich J. Minimizing Embedding Impact in Steganography Using Trellis-coded Quantization[C]//Proc. of SPIE'10. San Jose, USA: [s. n.], 2010.

[6] Filler T, Fridrich J. Minimizing Additive Distortion Functions with Non-binary Embedding Operation in Steganography[C]//Proc. of the 2nd IEEE Workshop on Information Forensics and Security. New York, USA: [s. n.], 2010.

[7] 耿广志, 张汗灵, 熊彩琼. 自适应的无损像素差分隐写算法[J]. 计算机工程, 2009, 35(23): 136-137, 140.

[8] Bas P, Furon T. USDA NRCS Photo Gallery[EB/OL]. (2010-03-12). http://photo gallery.nrcs.usda.gov.

编辑　任吉慧