基于病灶格子图的嵌入编码数字隐写系统*

李学相[1]，张文宁[2]
(1. 郑州大学 软件技术学院，郑州 450002；2. 中原工学院 软件学院，郑州 450003)

摘 要：针对数字图像隐写中常见的 LSB 替换隐写算法的不足，设计并实现一种基于病灶格子图编码(STC)算法的数字隐写系统，该系统对 STC 编码算法进行了改进，给出了隐藏秘密消息比特数的传递方法，优化了其自适应性，解决了秘密消息的长度共享问题，改进了传输过程中 STC 码的抗提取性能，从而提高了隐写系统的安全性。

关键词：LSB 替换隐写算法；病灶格子图编码；数字隐写；自适应性；抗提取性能
中图分类号：TP391.41 **文献标志码**：A **文章编号**：1001-3695(2013)06-1853-03
doi:10.3969/j.issn.1001-3695.2013.06.066

Embedded coding data hiding system based on trellis-coded

LI Xue-xiang[1], ZHANG Wen-ning[2]
(1. *School of Software Technology, Zhengzhou University, Zhengzhou* 450002, *China*; 2. *College of Software, Zhongyuan University of Technology, Zhengzhou* 450003, *China*)

Abstract: Aiming at traditional LSB replacement steganography weakness, this paper designed and implemented a data hiding system based on STC(steganography on trellis-coded) algorithm. The novel STC algorithm defined the bit number transmission method of secret hidden information to optimize its adaptivity. It solves the length sharing of the information hiding and improves the extractable resistance to STC code, hence improves the security of data hiding system.

Key words: LSB replacement steganography algorithm; steganography on trellis-coded; data hiding; adaptivity; extractable resistance

数字隐写是指将秘密信息嵌入到数字多媒体数据中(如数字图像、视频、音频等)，利用多媒体表面意义的掩护达到掩盖秘密消息存在的目的。那些隐藏秘密信息的多媒体可通过公开信道传递给接收方，接收方从多媒体中取出秘密消息，但攻击者往往无法发现秘密信息通信的存在。当前以图像作为载体的隐写软件十分常见，但其使用的嵌入方法多是简单的 LSB 替换算法，这些算法面临着隐写检测的威胁，采用好的嵌入方法提高隐写系统的安全性，是隐写系统设计的一个关键。本文设计并实现了图像数字隐写系统，该系统基于病灶格子图嵌入编码算法(STC)，优化了其自适应性，解决了秘密消息的长度共享问题，改进了传输过程中 STC 码的抗提取性能，给出了隐藏秘密消息比特数的传递方法，提高了隐写系统的安全性。

1 病灶格子图嵌入编码算法

设嵌入仅改动载体数据的最低比特位，可用二进制向量 $\boldsymbol{x}=(x_1,\cdots,x_n)\in\{0,1\}^n$ 来表示载体图像，用 $\boldsymbol{y}=(y_1,\cdots,y_n)\in\{0,1\}^n$ 表示载密图像。设要嵌入 m bit 秘密信息 $\boldsymbol{w}$，即 $\boldsymbol{w}\in\{0,1\}^m$，则嵌入函数可表达为

$$\mathrm{Emb}:\{0,1\}^n\times\{0,1\}^m\rightarrow\{0,1\}^n \tag{1}$$

提取函数为

$$\mathrm{Ext}:\{0,1\}^n\rightarrow\{0,1\}^m \tag{2}$$

上述两个函数满足 $\mathrm{Ext}(\mathrm{Emb}(\boldsymbol{x},\boldsymbol{w}))=\boldsymbol{w}$，$\forall\boldsymbol{x}\in\{0,1\}^n$，$\forall\boldsymbol{w}\in\{0,1\}^m$。

基于 STC 编码进行隐写的基本思想是引入一个 m 行 n 列的矩阵 $\boldsymbol{H}$，载密体 $\boldsymbol{y}$ 应满足

$$\boldsymbol{H}\cdot\boldsymbol{y}^{\mathrm{T}}=\boldsymbol{w} \tag{3}$$

当矩阵 $\boldsymbol{H}$ 的秩小于载体元素个数 n 时，有多个 $\boldsymbol{y}\in\{0,1\}^n$ 满足式(3)，寻找一个一定意义上最佳的 $\boldsymbol{y}$。为此，为每个载体元素指定一个 ρ_i，ρ_i 表示为了嵌入秘密信息而对第 i 个载体元素进行修改所带来的扭曲，这种扭曲也可以形象地理解为付出的代价。ρ_i 通常根据载体图像的内容取定，如根据载体像素 x_i 的邻域或者边缘特性确定。假设嵌入操作相互独立，信息嵌入后的总代价 $D(\boldsymbol{x},\boldsymbol{y})$ 为各个载体元素的代价 ρ_i 的和：

$$D(\boldsymbol{x},\boldsymbol{y})=\sum_{i=1}^{n}\rho_i|x_i-y_i| \tag{4}$$

隐写期望 $D(\boldsymbol{x},\boldsymbol{y})$ 应尽可能地小，即寻找一个既满足 $\boldsymbol{H}\cdot\boldsymbol{y}^{\mathrm{T}}=\boldsymbol{w}$ 又使 $D(\boldsymbol{x},\boldsymbol{y})$ 最小的 $\boldsymbol{y}$，上述嵌入方法就可表达为

$$\mathrm{Emb}(\boldsymbol{x},\boldsymbol{w})=\arg\min_{\boldsymbol{y}\in C(\boldsymbol{w})}D(\boldsymbol{x},\boldsymbol{y})$$
$$C(\boldsymbol{w})=\{z\in\{0,1\}^n|\boldsymbol{H}z=\boldsymbol{w}\} \tag{5}$$

对应提取方法为

$$\mathrm{Ext}(\boldsymbol{y})=\boldsymbol{H}\boldsymbol{y} \tag{6}$$

当前，已有隐写算法[1,2]采用$(n,n-m)$的二进制线性码 C 的奇偶校验阵作为 $\boldsymbol{H}$ 矩阵，此时相当于设 $\rho_i=1$，$i\in\{1,2,\cdots,n\}$，$D(\boldsymbol{x},\boldsymbol{y})$最小对应于载体元素修改的个数最少。但是，对于实际的图片来说，在每个载体元素修改的代价是不一样的，仅仅简单地变为载体元素修改的个数最小，并不能达到最佳的 D($\boldsymbol{x}$, $\boldsymbol{y}$)。因此，如何找到最佳的 $D(\boldsymbol{x},\boldsymbol{y})$ 是解决自适应隐写的关键。

在 STC 嵌入编码中，目标是找到一个最佳矢量 $\boldsymbol{y}$，使 $\boldsymbol{H}\cdot\boldsymbol{y}^{\mathrm{T}}=\boldsymbol{w}$($\boldsymbol{w}$ 为秘密消息，秘密消息的长度为 m)，并且使嵌入代

收稿日期：2012-10-08；**修回日期**：2012-11-26 **基金项目**：国家自然科学基金资助项目(10771028)

作者简介：李学相(1965-)，男，河南淮阳人，副教授，博士，主要研究方向为计算机软件与理论(lxx@zzu.edu.cn)；张文宁(1982-)，女，讲师，硕士，主要研究方向为软件工程.

价 $\Sigma\rho_i|x_i-y_i|$ 最小。根据 H,可以把所有满足 $H\cdot y^{\mathrm{T}}=w$ 的 y 在格子上用一条路径表示,最佳的 y 可以通过 Viterbi 算法[3]找到。

1.1 确定代价

设定一个嵌入代价 ρ_i(ρ_i 为改变每个像素的代价),ρ_i 可以限制为一个有很小支集的实数函数,即 $\rho_i(x,y_i)=\Theta(x_{\sigma(i)},y_i)$,$x_{\sigma(i)}$ 指像素 i 的相邻像素。

根据实践,像素在不平滑的区域比平滑的区域被嵌入的概率大。另一方面,像素在"湿纸区"是不能改变的[4]。本文在 Θ 引入参数 θ,因此找到最佳 ρ_i 的问题可以转换为求参数 θ 的问题,参数 θ 以实际经验值的形式给出,取 $\theta=1$。下面对参数 θ 与嵌入代价的关系进行说明。

定义单个像素代价 $\rho_i(x,y_i)$ 为

$$\rho_i(x,y_i)=\Theta(N_i,y_i)=$$

$$\begin{cases}0 & \text{当 } y_i=x_i\\ \infty & \text{当 } y_i\notin I_i\\ \Sigma_{z\in N_i}(1+\theta|z-x_i|)^{-1}+(1+\theta|z-y_i|)^{-1} & \text{其他}\end{cases}\tag{7}$$

在图像的边界处,像素点的相邻像素 N_i 相应地减小(即边界点的相邻像素点为 5 个,顶点的相邻像素点为 3 个)。

由于只进行加减 1 运算,ρ_i 只在 I_i 区间内有效,即当 $y_i=x_i$ 时,不改变图像的像素,即代价为零;当 $y_i\notin I_i$ 时,不在允许范围内的操作,即代价为无穷大;当 $y_i=\{x_i-1,x_i+1\}$ 时,ρ_i 和原始像素点与嵌入后像素点都有关,所以不仅需要考虑原始像素点和八邻域的关系,还需要考虑嵌入后像素点与八邻域的关系,因此得出的代价是自适应的[5,6]。由此可见对于原始图像,像素点和八邻域的差异越大,图像越不平滑,像素点的代价越小;反之,像素点的代价越大。所以 ρ_i 与 $|z-x_i|$ 成反比。对于嵌入后图像,嵌入后的像素点与八邻域的差异越大,嵌入后的图像越不平滑,则是不易被检测的,即嵌入代价越小;反之,嵌入代价越大。所以 ρ_i 与 $|z-y_i|$ 也成反比。式中引入一个相关参量 θ,θ 的大小直接影响到图像像素点代价随图像平滑程度大小而变化的快慢。

1.2 奇偶校验矩阵 H 的构造

引入 m 行 n 列的矩阵 H,H 与最终的载密矢量 y 满足式(3),$H\cdot y^{\mathrm{T}}=w$,其中 $w=(w_1,w_2,\cdots,w_m)$ 代表了 m bit 嵌入信息。定义一个相对载荷,记为 α,$\alpha=\frac{m}{n}$。其中,m 表示嵌入信息的比特数,n 表示图像像素总数。

奇偶校验矩阵 H 通过一个 $h\times\omega$ 子矩阵 $\hat{H}$ 拼凑得出,子矩阵 $\hat{H}$ 的行高 h 是自由设定的参数,h 的大小影响算法的速度和效率,子矩阵的列宽 ω 决定于相对载荷 α,如果 $\alpha=1/k$ ($k\in N$),则 $\omega=k$,一般情况下的 α 满足 $1/(k+1)<\alpha<1/k$。子矩阵 $\hat{H}$ 作为一个特定的矩阵,接收方和发送方是共享的。

H 的构造方法:子矩阵 $\hat{H}$ 沿对角线依次排列,并且每次错开一列,最后构成一个稀疏的奇偶校验矩阵 H。奇偶校验矩阵 H 需要由两个子矩阵构成,一个子矩阵为 $\hat{H}$,列宽为 k,另一个子矩阵的列宽为 $k+1$,只有这样才能使最后奇偶校验矩阵 H 的大小为 $[\alpha n]\times n(\alpha=\frac{m}{n}$,即 $[\alpha n]\times n=m\times n)$。由此,对于任意合理的 $\alpha\leqslant 1/2$ 都能得到一个奇偶校验矩阵 H。

$$\hat{H}=\begin{pmatrix}1&0\\1&1\end{pmatrix}$$

$$H=\begin{pmatrix}1&0&&&&&&&&&\\1&1&1&0&&&&&&&\\&&1&1&1&0&&&&&\\&&&&1&1&&&&&\\&&&&&&\ddots&&&&\\&&&&&&&\ddots&&&\\&&&&&&&&\ddots&&\\&&&&&&&&&1&0\\&&&&&&&&&1&1&1&0\end{pmatrix}$$

y 的前 ω bit 能够影响消息 w 的第一比特,因此 $(y_1,y_2,\cdots,y_\omega)$ 以满足 $(H_{11},H_{12},\cdots,H_{1\omega})\cdot(y_1,y_2,\cdots,y_\omega)^{\mathrm{T}}=w_1$。同理,$y$ 的前 2ω bit 影响消息 w 的第二个比特,依此类推。

1.3 病灶格子图嵌入编码算法

a)通过图像扫描,将图像中所有的像素以载体 $x=(x_1,\cdots,x_n)\in\{0,1\}^n$ 的形式给出。

b)构造病灶格子图。病灶格子图是由 m 个模块组成的一个图形,每一个模块由一个 $\omega+1$ 列和 2^h 行,即 $2^h(\omega+1)$ 个节点组成。每一模块的第一列依次标记 p_l,$l\in\{1,2,\cdots,n\}$,所有的边只连接相邻两列之间的节点,且相邻两列相连构成无向图。每一列有 2^h 个状态,对应表示 h bit 秘密消息的所有可能情况。

c)构造奇偶校验矩阵 H,连接病灶格子图中的节点。列中每个节点的状态都有两条边对应,其中 y_i 可能的取值为 0 和 1。格子图中水平边代表 y_i 为 0,斜边代表 y_i 为 1。水平边还是斜边的选择取决于秘密消息。

d)给每一条网格上的边都赋上一个权重 ρ_i。具体方法为:比较 x_i 和 y_i,若 x_i 和 y_i 取值相同,那么这条边的权重 ρ_i 定义为 0,即该点的像素没有发生变化;若 x_i 和 y_i 取值不同,那么定义这条边的权重为 ρ_i(ρ_i 不为 0),此时 ρ_i 是按照确定代价部分得到的一个确定值。

e)利用 Viterbi 算法寻找网格里一条代价最小的边。算法由两个部分组成;

(a)算法前向部分。由 $(n+m)$ 个步骤组成,即每个解对应路径的 $(n+m)$ 条边,第 i 步求出从最左边第一个全零状态到第 i 列各状态的最短路径(每一列有 2^h 个状态),第 $n+m$ 步,找到了贯穿于整个网格的一条最短边,如果一些状态是不可达的(也就是说没有路径到达这些点),那么把权重赋为 ∞。

(b)算法后向部分。沿着最短路径向前查找能够根据边的标记找到 y。

2 算法实现

基于病灶格子图嵌入编码(STC)算法开发了一个自适应数字隐写系统,系统结构分为嵌入部分和提取部分两大模块。

2.1 嵌入部分

嵌入模块可分为代价确定子模块、密钥子模块、STC 码处理子模块。

2.1.1 代价确定子模块

图像导入后,根据单个像素代价确定算法,对图像的嵌入所产生的代价进行逐一计算。

2.1.2 密钥子模块

密钥方案是随机选取 36 个像素位置嵌入 36 bit 消息长度,具体嵌入的位置选择是由一个密钥控制的伪随机数生成方法确定的。

a)对载体图像进行扫描,确定其总像素个数值 n。

b)通过对初始密钥赋值,生成一个随机数 X。

c)将 X 作模 n 运算,生成像素编号。

d)判断 s 所指编号的像素是否已经被选中作为嵌入信息的载体像素。若已经嵌入信息则该比特被舍弃,返回操作 b);若没有嵌入信息则将像素从载体图中去除,并用 K_i 数组记录该图像位置,剩余像素用于嵌入秘密消息。

e)重复操作 b) ~ d),共取出 36 个有效像素。

f)逐一将 1 bit 的长度消息嵌入到每个像素的最低位比特中,直至 36 bit 信息全部嵌入图像中。

g)秘密消息嵌入在图像中后,将去除的 64 bit 像素按照 K_i 的记录放回图像中。

2.1.3　STC 处理子模块

该模块使用 STC 算法在像素中进行秘密消息的嵌入。

a)根据嵌入的秘密消息长度,使用奇偶校验矩阵 H 的构造算法,构造出嵌入的奇偶校验矩阵 H。

b)将载体图像进行处理。图像的像素排列由二维向量转换为一维数组存储,分别为按行扫描产生和按列扫描产生的一维向量。

c)根据 STC 嵌入过程分别找到代价最小的嵌入位置 y,将需嵌入的秘密消息分为 w_1 和 w_2 两部分,嵌入时 w_1 中每一位嵌入 y 分量像素的最低位比特,w_2 中每一位嵌入在 y 分量像素的次低位。

d)将秘密消息嵌入,并得出相应的总代价:行 $D_0(x,y)$、列 $D_1(x,y)$。

e)进行 LSB 嵌入。将秘密消息每一位按顺序逐一嵌入在载体图像中每个像素的最低位比特上,并根据每个载体图像的代价值,得出 LSB 嵌入所产生的代价 $D_2(x,y)$。

f)比较 $D_0(x,y)$ 和 $D_1(x,y)$,得到一个最小总代价即为 $D(x,y)$。

g)记录取得总代价的扫描方式,在密钥子模块将 64 个像素放回图像后,将其方式隐写在图像第一个像素的倒数第三位比特上(避免后两位比特已嵌入秘密消息),0 代表按行扫描,1 代表按列扫描。

2.2　提取部分

2.2.1　嵌入方式分析子模块

处理载密图像的第一步必须先确定载密采用了何种嵌入扫描方式,因此在嵌入方式分析子模块中,要完成对图像的初步分析。步骤如下:检测载密图像第一个像素的倒数第三位比特,确定嵌入扫描方式是按行扫描还是按列扫描;将载密图像按照扫描方式进行处理,若为行则直接转换为一维数组存储,若为列则应将图像的所有行列图像对换,然后转换为一维数组存储。

2.2.2　密钥提取子模块

接收方根据共享的密钥提取出秘密消息长度 m,用于奇偶校验矩阵 H 的构造,提取过程如下:

a)对载体图像进行扫描,确定其总像素个数值 n,并且输入正确密钥。

b)由密钥循环生成随机数 X,通过模 n 运算得到 64 个有效像素序号。

c)将对应的 64 个像素从载密图像中提取出,将剩余像素用于秘密消息提取。

d)逐一提取出前 36 个像素的最低位比特信息,还原秘密消息的长度 m。

2.2.3　秘密消息提取子模块

从载密图像中提取出秘密消息,需先还原发送方的奇偶校验矩阵 H,流程如下:

a)将提取 64 个像素后的载密图像进行处理,用 $n \times 1$ 向量 y 表示。

b)由共享的 $\hat{H}$ 构造方法,构造 $[\alpha n] \times n$ 的稀疏矩阵 H。

c)通过 $H \cdot y^{\mathrm{T}} = w$ 运算,得出秘密消息 w,还原秘密消息。

3　实验结果及分析

为了验证本文给出的病灶格子图嵌入编码算法性能,选取不同类型的二值图像作为载体图像,所选取的图像大小均为 256 × 256,分别采用数字图像隐写中常见的 LSB 替换隐写算法和 STC 算法嵌入信息。从载密图像质量、隐藏容量、隐写检测、自适应性、抗提取性、安全性等方面进行比较。

载密图像质量越好,信息隐藏的安全性越高。STC 算法具有良好的视觉不可感知性,即人眼无法区分载密图像与载体图像之间的差异。隐藏容量主要取决于图像中可用子块的数量。密钥的使用亦是决定安全性的重要因素之一,STC 算法通过使用共享密钥进一步增强了安全性。

表 1 中列出了 LSB 算法和 STC 算法的比较结果。可以看出 LSB 替换隐写算法有很多不足,如算法简单,容易进行隐写检测进而降低隐写系统的安全性等。而 STC 算法由于采用引入基于行列总代价减小的嵌入方案和密钥控制方案,并给出了奇偶校验矩阵 H 的构造方法以及隐藏秘密消息比特数的传递方法,进而优化了其自适应性,解决了秘密消息的长度共享问题,改进了传输过程中 STC 码的抗提取性能,最终提高了隐写系统的安全性。

表 1　LSB 算法与 STC 算法对比

算法	载密图像质量	隐写检测	自适应性	抗提取性	安全性
LSB	一般	容易检测	一般	较弱	一般
STC	较好	不易检测	较好	较强	较好

4　结束语

本系统以 STC 算法为基础,引入基于行列的总代价减小嵌入方案和密钥控制方案,设计并实现了在抗检测和抗提取方面性能均提升的数字隐写软件,能够避过大多数隐写检测软件的检测,进而保护了隐藏信息的安全。

参考文献:

[1] TSENG Y C, CHEN Yu-yuan, PAN H K. A secure data hiding scheme for binary images[J]. IEEE Trans on Communications, 2002, 50(8): 1227-1231.

[2] WU Ming, LIU B. Data hiding in binary image for authentication and annotation[J]. IEEE Trans on Multimedia, 2004, 6(4): 528-538.

[3] 刘春庆,戴跃伟,王执铨. 一种新的二值图像信息隐藏方法[J]. 东南大学学报:自然科学版, 2003, 33(S1): 98-101.

[4] LIN Yi-xun. Graph extensions and some optimization problems in sparse matrix computations[J]. Advances in Mathematics, 2001, 30(1): 1-21.

[5] YIN Ping. Study on reusable test case[J]. Journal of Computer Applications, 2010, 30(5): 1309-1311.

[6] ZHANG Wen-ning, LI Xi-yan, ZHOU Qing-lei. Model research of testing process based on comparison[J]. Computer Engineering and Design, 2010, 31(4): 696-699.