一种基于湿纸编码和图匹配理论的直方图保持隐写算法

刘九芬* 韩 涛 张卫明 陈嘉勇
(信息工程大学信息工程学院 郑州 450002)

摘 要：该文结合隐写码、湿纸码和图匹配理论提出一种具有高嵌入效率的且可保持载体图像一阶直方图的双层嵌入隐写算法。首先构造出一条新的四进制的隐写信道，然后在该信道的 LSB(Least Significant Bit)层和次 LSB 层分别使用二元隐写码和湿纸码嵌入秘密消息，这样即可确定出需要修改的元素，接着构造出一个图，最后使用图论中匹配算法寻找一种减小失真且保持直方图的修改方式。性能分析和实验结果表明：在嵌入相同长度秘密消息的情况下，新算法的 PSNR、嵌入效率和保持一阶直方图效果均优于隐写软件 Steghide。

关键词：隐写术；隐写码；湿纸码；图匹配理论；嵌入效率
中图分类号：TP309 **文献标识码**： A **文章编号**：1009-5896(2011)03-0592-05
DOI: 10.3724/SP.J.1146.2010.00427

A Histogram-preserving Steganography Based on Wet Paper Coding and Graphic Matching Theory

Liu Jiu-fen Han Tao Zhang Wei-ming Chen Jia-yong
(*Institute of Information Engineering*, I*nformation Engineering University*, *Zhengzhou* 450002, *China*)

Abstract: This paper presents a novel double-layered embedding steganographic algorithm based on steganographic codes, wet paper codes and graphic matching theory, which can achieve high embedding efficiency and preserve the first-order histogram of the cover image. At first, a new 4-ary steganographic channel is constructed. Then the secret message is embedded in the LSB (Least Significant Bit) layer of this channel using binary steganographic codes and in the second LSB layer using wet paper codes, and the elements that need to be changed, are obtained. Afterwards, a graph is constructed. Then a changing manner of the cover image is found to decrease the distortion and preserve the histogram, using the matching algorithm in graph theory. The performance analysis and experimental results show that PSNR, the embedding efficiency and the ability to preserve the first-order histogram of the proposed algorithm are better than the steganographic software Steghide, when the same amount of secret message is embedded.

Key words: Steganography; Steganographic codes; Wet paper codes; Graphic matching theory; Embedding efficiency

1 引言

信息隐藏是信息安全领域的一个新的前沿技术。隐写术是信息隐藏技术的一个重要分支，研究如何把秘密消息嵌入到公开的多媒体数据中以实现隐蔽通信。隐写术有两个关注的核心问题：第一，如何以最小的失真代价在载体中嵌入尽可能多的信息，针对这一问题的编码方法称之为隐写码[1]；第二，如何避开对载体敏感区域的修改，湿纸码[2]可以解决这一问题。目前已构造出很多性质优良的二元隐写码[3,4]。Fridrich等人[5]和Zhang等人[6]等分别给出了一种提高湿纸码的嵌入效率的构造方法。

嵌入消息后能够保持载体的统计特性也是设计隐写算法时需要考虑的一个重要指标。文献[7]提出的SSM(Secure Steganographic Method)算法在JPEG图像的DCT系数上嵌入秘密消息，并保证DCT系数的直方图基本不变。文献[8]也提出了一种可以保持载体图像一阶直方图的隐写算法。文献[9]提出了一种能减小载体失真同时保持载体直方图的隐写算法。文献[10]提出了一种利用图匹配理论来保持载体的一阶直方图的隐写算法，并将其运用到著名隐写软件Steghide[11]中。而Steghide也已因其优良的性能已被一些隐写系统所采用[12]。

本文在软件Steghide的基础上，利用隐写码和湿纸码改进其嵌入效率，并结合图匹配理论提出了一种具有高嵌入效率的且可保持载体图像一阶统计

2010-04-26收到，2010-11-15改回
国家自然科学基金(60803155)资助课题
*通信作者：刘九芬 jiufenliu@163.com

特性的双层嵌入隐写算法，将其简记为DLE (Double-Layered Embedding)算法。首先将载体图像的像素进行分组，再按照一定的计算规则构造出一条新的四进制的隐写信道；然后利用文献[13,14]中双层嵌入算法在该信道的LSB层和次LSB层上嵌入秘密消息；在新的隐写信道嵌入消息后，即可确定该信道上需要修改的元素，然后根据这些元素的位置构造出一个图，再运用图论中的图匹配理论来寻找图的最大势最小重量匹配；最后根据找到的匹配确定载体图像的修改位置和修改方式，进而可对载体图像进行修改，完成消息嵌入过程。实验结果和理论分析都表明：在嵌入相同长度秘密消息的情况下，相对于Steghide，DLE算法减少了对载体图像像素的修改个数，减小了载体图像的失真，进而提高了嵌入效率；同时DLE算法还能更好保持载体图像的一阶直方图，因而可更好抵抗一阶统计攻击。

2　准备知识

下面给出一些图论中的术语和记号。

本文只考虑无向图的情形。一个无向图 G 是由包含 p 个顶点的非空集合 A 和 A 中不同顶点的 q 个无序对集 E 组成，记作 $G=(A,E)$，其中 A 和 E 分别称为顶点集和边集。E 中的每个顶点对 (x,y) 称为 G 的边，如果用 e 表示这条边，则记 $e=(x,y)$，称 x，y 是 e 的端点，也称 x，y 与 e 关联，且称 x 和 y 是邻接的顶点。若两条不同的边与一个公共的端点关联，则称这两条边是邻接的。定义边 $e\in E$ 的重量为 $c(e)$。

设 M 是图 G 的边集 E 的一个子集，如果 M 中任意两条边在 G 中都不邻接，则称 M 是 G 的一个匹配。M 中的一条边的两个端点叫做在 M 中相配。若匹配 M 的某条边与顶点 x 关联，则称 M 饱和顶点 x，并且称顶点 x 是 M-饱和的，否则称 x 是 M-不饱和的。如果 G 的每个顶点都是 M-饱和的，则称 M 是 G 的一个完美匹配。G 中边数最多的匹配称为 G 的最大势匹配。如果 M 是 G 的一个最大势匹配，同时 M 中所有边的重量之和在 G 的所有最大势匹配中是最小的，则称 M 是 G 的一个最大势最小重量匹配。

本文采用如下关于隐写码的记号：二元隐写码 $\mathrm{SC}(R_a,n,l)$ (Steganographic Codes)可在 n 比特长的二元载体上嵌入 l 比特消息，平均修改 R_a 比特。采用如下关于湿纸码的记号：$\mathrm{WPC}(\alpha,c)$ (Wet Paper Codes)表示以嵌入率 α 和修改率 c 嵌入消息的湿纸码。

3　双层嵌入算法

3.1　消息嵌入过程

3.1.1　嵌入框架　本文选择灰度图像作为载体图像。假设载体图像含有 N 个像素，发送者首先根据共享密钥 K 置乱载体图像，用 $\boldsymbol{x}=(x_1,x_2,\cdots,x_N)$ 表示置乱后载体图像的像素值，其中 $x_i\in S=[0,255]$，$1\le i\le N$。定义嵌入值函数 $v:S\to\{0,1,2,3\}$，$v(x_i)=x_i(\mathrm{mod}\,4)$，将 $v(x_i)$ 称为 x_i 的嵌入值。将载体图像的像素进行分组，连续 k 个像素一组，定义第 i 个像素分组的嵌入值为 $V_i=\left(\sum_{j=1}^{k}v(x_{k(i-1)+j})\right)(\mathrm{mod}\,4)$，$1\le i\le\widehat{N}=\lfloor N/k\rfloor$。

设 $\boldsymbol{V}=(V_1,V_2,\cdots,V_{\widehat{N}})$，将每个四进制的 V_i 转化为二进制表示形式：$V_i=V_{i,1}\times2+V_{i,2}$，$1\le i\le\widehat{N}$，即可得到 V_i 的 LSB 位 $V_{i,2}$ 和次 LSB 位 $V_{i,1}$，从而获得了两条二进制的载体序列，将其分别记为 $\boldsymbol{V}^1=(V_{1,1},V_{2,1},\cdots,V_{\widehat{N},1})$ 和 $\boldsymbol{V}^2=(V_{1,2},V_{2,2},\cdots,V_{\widehat{N},2})$。

基于文献[19,20]中双层嵌入的思想，在 $\boldsymbol{V}^1$ 和 $\boldsymbol{V}^2$ 上分别使用湿纸码 $\mathrm{WPC}(\alpha,c)$ 和二元隐写码 $\mathrm{SC}(R_a,n,l)$ 嵌入秘密消息：

第 1 层嵌入：使用二元隐写码 $\mathrm{SC}(R_a,n,l)$ 在 $\boldsymbol{V}^2$ 上嵌入消息。在 $\boldsymbol{V}^2$ 上平均可嵌入 $\widehat{N}\cdot l/n$ 比特消息，平均需要修改 $\widehat{N}\cdot R_a/n$ 个 $\boldsymbol{V}$ 的元素。为了描述方便且不失一般性，假设 $\widehat{N}\cdot l/n$ 和 $\widehat{N}\cdot R_a/n$ 都是整数，而且恰好可以通过修改 $\widehat{N}\cdot R_a/n$ 个 $\boldsymbol{V}$ 的元素嵌入 $\widehat{N}\cdot l/n$ 比特消息。

对于 $\boldsymbol{V}$ 的一个元素 V_i，V_i+1 或 V_i-1 都会使其 LSB 位 $V_{i,2}$ 翻转为 $V_{i,2}\oplus1$，但是次 LSB 位 $V_{i,1}$ 的取值在两种修改模式下会不同。如果 V_i 是偶数，则加 1 时 $V_{i,1}$ 保持不变，减 1 时 $V_{i,1}$ 翻转；V_i 是奇数的情况刚好相反，减 1 时 $V_{i,1}$ 保持不变，加 1 时 $V_{i,1}$ 翻转。利用这个性质，在第1层嵌入过程中 $\boldsymbol{V}$ 中有 $\widehat{N}\cdot R_a/n$ 个元素的 LSB 位需要修改，可以通过选择加 1 或减 1 来同时自由控制这 $\widehat{N}\cdot R_a/n$ 个元素的次 LSB 位，从而可进行第二层信息嵌入。

第 2 层嵌入：使用湿纸码 $\mathrm{WPC}(\alpha,c)$ 在 $\boldsymbol{V}^1$ 上嵌入消息。在第 2 层嵌入中，有 $\widehat{N}\cdot R_a/n$ 个 $\boldsymbol{V}$ 的元素的次 LSB 位可以自由变动，其他 $\widehat{N}\cdot(1-R_a/n)$ 个元素的次 LSB 位不可变动，即在 $\boldsymbol{V}^1$ 上有 $\widehat{N}\cdot R_a/n$ 个“干的”位置和 $\widehat{N}\cdot(1-R_a/n)$ 个“湿的”位置，用湿纸码 $\mathrm{WPC}(\alpha,c)$ 平均可在 $\boldsymbol{V}^1$ 上嵌入另外 $\alpha\cdot\widehat{N}\cdot R_a/n$ 比特消息。

上述嵌入过程中若遇到 $V_i=0$ 需要减 1 或 $V_i=3$ 需要加 1 的情况，需要特殊处理：

(1)若 $V_i=0$ 需要进行减 1 修改，由于 $0-1=3(\mathrm{mod}\,4)$，所以设定修改 V_i 的结果为 3；

(2)若 $V_i=3$ 需要进行加 1 修改，由于 $3+1=0(\mathrm{mod}\,4)$，所以设定修改 V_i 的结果为 0。

这样即可得到两条二进制的载密序列，将其分别记为 $\boldsymbol{V}^{1'}=(V_{1,1}^{'},V_{2,1}^{'},\cdots,V_{\widehat{N},1}^{'})$ 和 $\boldsymbol{V}^{2'}=(V_{1,2}^{'},V_{2,2}^{'},\cdots,V_{\widehat{N},2}^{'})$。将 $\boldsymbol{V}^{1'}$ 和 $\boldsymbol{V}^{2'}$ 的元素按如下规则合并为一个四进制数：$V_i^{'}=V_{i1}^{'}\times 2+V_{i2}^{'}$，$1\le i\le\widehat{N}$，从而可得到一条四进制的载密序列，将其记为 $\boldsymbol{V}'=(V_1^{'},V_2^{'},\cdots,V_{\widehat{N}}^{'})$。

3.1.2 顶点的定义和顶点集的构造 一个顶点 $\boldsymbol{w}$ 是由一个位置向量 $\boldsymbol{P}$ 和一个目标值向量 $\boldsymbol{T}$ 组成，其中位置向量 $\boldsymbol{P}=(p_1,p_2,\cdots,p_k)\in\{1,\cdots,N\}^k$，目标值向量 $\boldsymbol{T}=(t_1,t_2,\cdots,t_k)\in\{0,1,2,3\}^k$，记作顶点 $\boldsymbol{w}=\{\boldsymbol{P},\boldsymbol{T}\}$。如果第 j 个像素分组的嵌入值 V_j 与相应的载密值 $V_j^{'}$ 不相等，即差值 $d_j=V_j^{'}-V_j\neq 0$，也即 $d_j\in\{-1,+1,-3,+3\}$，那么在这个像素分组上需要构造一个顶点，目标值向量为 $(t_{k(j-1)+1},\cdots,t_{k(j-1)+k})$，其中 $t_{k(j-1)+i}=(v(x_{k(j-1)+i})+d_j)(\mathrm{mod}\,4)$，$i=1,2,\cdots,k$，位置向量为 $(k(j-1)+1,\cdots,k(j-1)+k)$。只需用目标值向量中的一个目标值替换对应像素的嵌入值就可以使 $V_j=V_j^{'}$ 成立，将这个操作称为嵌入一个顶点。接下来给出顶点集的构造过程：按照顶点的定义，在 $\boldsymbol{V}$ 与 $\boldsymbol{V}'$ 不相等的位置对应的像素分组上构造出一个顶点，这样就可以构造出整个顶点集。

图 1 给出了像素分组的长度 $k=3$ 时顶点集的构造过程。第 1 行表示载体图像的像素 $\boldsymbol{x}$，第 2 行表示像素值，第 3 行表示像素的嵌入值 $v(\boldsymbol{x})$，第 4 行表示像素分组的嵌入值 $\boldsymbol{V}$，其中：$V_i=(v(x_{3i-2})+v(x_{3i-1})+v(x_{3i}))(\mathrm{mod}\,4)$，$i=1,2,3,\cdots$。第 5 行表示在 $\boldsymbol{V}$ 上嵌入秘密消息后得到的四进制的载密序列 $\boldsymbol{V}'$，最后一行表示构造出的顶点。从图 1 可以看出，$V_1\neq V_1^{'}$，$V_2=V_2^{'}$，$V_3\neq V_3^{'}$，则在第 1 和 3 个像素分组上分别构造出一个顶点，顶点 $\boldsymbol{w}_1$ 和 $\boldsymbol{w}_3$ 的位置向量和目标值向量如图 1 的最后一行所示。在第 1 个像素分组上，只需用 $t_i(i=1,2,3)$ 中的一个替换对应的 $v(x_i)$ 就可以使 $V_1=V_1^{'}$ 成立，即嵌入了顶点 $\boldsymbol{w}_1$。

3.1.3 边的定义和边集的构造 设顶点 $\boldsymbol{y}=\{(p_1,\cdots,p_k),(t_1,\cdots,t_k)\}$，$\boldsymbol{z}=\{(q_1,\cdots,q_k),(u_1,\cdots,u_k)\}$，如果 $v(x_{p_i})=u_j$，$v(x_{q_j})=t_i$，$i,j\in\{1,\cdots,k\}$，且 $|x_{p_i}-x_{q_j}|\le r$，其中 r 为某个邻域半径，则称 $\boldsymbol{y}$ 的第 i 个像素与 $\boldsymbol{z}$ 的第 j 个像素有边连接，将这条边记为 $(\boldsymbol{y},\boldsymbol{z})_{i,j}$，这条边的重量记为 $c((\boldsymbol{y},\boldsymbol{z})_{i,j})=|x_{p_i}-x_{q_j}|$。边的作用是连接两个可能会交换的像素，通过交换两个像素可以实现同时嵌入两个顶点。例如，在图 1 中，若设邻域半径 $r=1$，由于 $v(x_3)=t_9$，$v(x_9)=t_3$，且 $|x_3-x_9|=1\le r$，所以 $\boldsymbol{w}_1$ 的第 3 个像素与 $\boldsymbol{w}_3$ 的第 3 个像素有边连接，这条边即为 $(\boldsymbol{w}_1,\boldsymbol{w}_3)_{3,3}$，这条边的重量即为 $c((\boldsymbol{w}_1,\boldsymbol{w}_3)_{3,3})=1$，交换 x_3 和 x_9 可以使 $V_1=V_1^{'}$ 和 $V_3=V_3^{'}$ 同时成立，即实现了同时嵌入了顶点 $\boldsymbol{w}_1$ 和 $\boldsymbol{w}_3$。按照边的定义构造出所有边，也就构造出了整个边集 E。这样就构造出一个图 $G=(A,E)$。

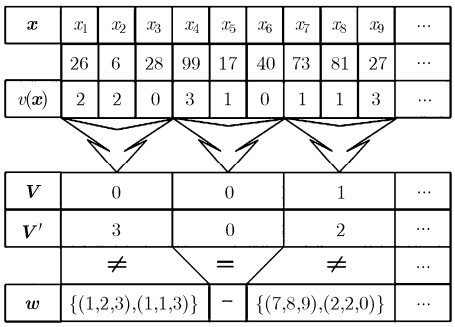

图 1 像素分组的长度 $k=3$ 时顶点集的构造过程

3.1.4 嵌入过程 图 G 的每个匹配都对应着一种对载体图像的修改方式。嵌入过程的目标就是要寻找一种对载体图像的修改方式使得能够嵌入顶点集 A 中所有的顶点，这样就需要尽力寻找到图 G 的一个完美匹配。但是并不一定每个载体图像都能找到一个完美匹配。并且还希望嵌入秘密消息后引起的视觉影响最小。所以本文使用文献[15]中一种启发式的贪心算法——DMD(Dynamic Minimum Degree)算法来寻找图 G 的最大势最小重量匹配 M。从 4.1 节的实验结果中将会发现，自然的载体图像都能够找到足够好的匹配。在寻找到最大势最小重量匹配 M 后，就可以对载体图像进行修改：对于 M-饱和的顶点对应的像素分组，交换在 M 中相配的端点对应的有边连接的两个像素；对于 M-不饱和的顶点对应的像素分组，就不能使用交换像素的修改方式，使用如下的方式进行修改：如果这个像素分组对应的差值的绝对值为 1，则随机选择这个像素分组中的一个像素加上这个差值；如果这个像素分组对应的差值为 -3，则随机选择这个像素分组中的一个像素加 1；如果这个像素分组对应的差值为 $+3$，则随机选择这个像素分组中的一个像素减 1。设 $\boldsymbol{x}=(x_1,x_2,\cdots,x_N)$ 在嵌入秘密消息后修改为 $\boldsymbol{x}'=(x_1^{'},x_2^{'},\cdots,x_N^{'})$，发送者根据共享密钥 K 将 $\boldsymbol{x}'$ 恢复为原来的像素顺序就可获得载密图像。

3.2 消息提取过程 接收者在接收载密图像后根据共享密钥 K 置乱载密图像，即可得到 $\boldsymbol{x}'=(x_1^{'},x_2^{'},\cdots,x_N^{'})$。接收者再按照与消息嵌入过程相同的分组方式对 $\boldsymbol{x}'$ 进行分组，并计算每个像素分组的嵌入值，从而可以获得四进制的载密信道 $\boldsymbol{V}'=(V_1^{'},V_2^{'},\cdots,V_{\widehat{N}}^{'})$，并将 $\boldsymbol{V}'$ 分解为次 LSB 层 $V^{1'}$ 和 LSB 层 $V^{2'}$，分别在 $V^{1'}$ 和 $V^{2'}$ 上分别使用湿纸码 WPC(α,c) 和 SC(R_a,n,l) 对应的提取方法即可提取出秘密消息。

4　实验和性能分析

4.1 实验结果

在 Steghide 中像素分组的长度$k=3$，邻域半径$r=10$。在 DLE 算法的实验中取像素分组的长度$k=3$，邻域半径$r=1$，匹配率的实验结果将会说明$r=1$时也能寻找到足够好的匹配，在$\boldsymbol{V}$的次 LSB 层$\boldsymbol{V}^1$和 LSB 层$\boldsymbol{V}^2$上分别使用湿纸码 WPC(1,1/2) 和基于二元汉明码的隐写码 SC($7/2^3$,7,3) 嵌入二元随机消息。在实验中使用 10 幅常用的 512×512 的灰度图像作为载体图像。

本文采用峰值信噪比(PSNR)来度量载密图像的视觉效果。PSNR 值越大表明载密图像与载体图像的相似性越大。表 1 给出了使用 Steghide 和 DLE 算法在 10 幅载体图像中嵌入 5 kB 秘密消息后的 PSNR。从表 1 可以看出，由两者得到的载密图像的视觉效果都比较好，人眼都很难区分；但 DLE 算法的 PSNR 大于 Steghide，所以使用 DLE 算法得到的载密图像的视觉效果更好。

下面采用嵌入效率来度量隐写算法的性能，嵌入效率表示单位失真代价所能嵌入的消息比特数，因而嵌入效率越大表明隐写算法的性能越好。表 2 给出了 Steghide 和 DLE 算法在嵌入 5 kB 秘密消息时的嵌入效率。从表 2 可以看出，在嵌入相同长度的秘密消息的情况下，DLE 算法的嵌入效率高于 Steghide。

匹配率度量隐写算法保持载体图像一阶直方图的能力。匹配率越高表明隐写算法对载体图像一阶直方图的修改越少，即保持载体图像一阶直方图的能力越强。图 2 给出了两种算法在 5 种嵌入消息长度情况下的匹配率。从图 2 可以看出，DLE 算法的匹配率高于 Steghide，从而能够更好的保持载体图像的一阶直方图。

4.2 性能分析与讨论

由于 Steghide 中像素分组长度为 3，所以其最大嵌入率为$\alpha_1=2/3$。经计算可得，DLE 算法的最大嵌入率为$\alpha_2=(l+R_a\cdot\alpha)/(n\cdot k)$，其中 k 是像素分组长度。因而采用 DLE 算法时，发送者可根据要嵌入的消息长度，选择合适的隐写码和湿纸码使得失真尽可能小，即嵌入效率尽可能大。

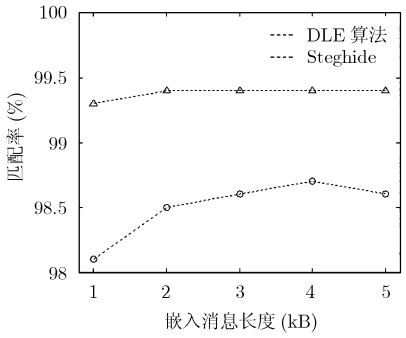

图 2 Steghide 和 DLE 算法在 5 种嵌入消息长度情况下的匹配率

下面分别讨论 Steghide 和 DLE 算法对四进制隐写信道$\boldsymbol{V}$和载体图像像素的修改情况：

(1)在 Steghide 中，$\boldsymbol{V}$中每个元素需要修改的概率为$P_1=1-(1-1/2)(1-1/2)=3/4$，则载体图像每个像素需要修改的概率为$P_1'=P_1/3=1/4$；

(2)在 DLE 算法中，$\boldsymbol{V}$中每个元素需要修改的概率为$P_2=R_a/n$，则载体图像每个像素需要修改的概率为$P_2'=P_2/k=R_a/(n\cdot k)$；

对于给定的像素分组长度k，所需要的嵌入率小于2/3时，总有$P_2'\le P_1'$。因此，相对于 Steghide，DLE 算法减少了载体图像像素的修改个数。另外，$\boldsymbol{V}$中元素的修改个数还直接决定着图G的规模，修改个数越少，图G的顶点数就越少，从而占用的存储空间就越小。

接下来讨论 Steghide 和 DLE 算法的嵌入效率。

(1)由于在 Steghide 中邻域半径$r=10$，所以只能用实验数据给出 Steghide 的嵌入效率。

(2)在 DLE 算法中，$\boldsymbol{V}$可能出现的修改幅度值的集合为$\{0,-1,+1,-3,+3\}$，各个修改幅度值出现的

表 1 使用 Steghide 和 DLE 算法嵌入 5 kB 消息时载密图像的 PSNR(dB)

图像名称	Airplane	Baboon	Barb	Boat	Goldhill	Lake	Lena	Man	Peppers	Portofino
Steghide	57.44	57.30	57.30	57.36	57.37	57.40	57.35	57.13	57.34	57.39
DLE 算法	62.70	62.68	62.65	63.65	62.65	62.69	62.67	62.66	62.68	62.64

表 2 使用 Steghide 和 DLE 算法嵌入 5 kB 消息时的嵌入效率

图像名称	Airplane	Baboon	Barb	Boat	Goldhill	Lake	Lena	Man	Peppers	Portofino
Steghide	1.33	1.29	1.29	1.31	1.31	1.32	1.31	1.24	1.30	1.32
DLE 算法	4.48	4.45	4.42	4.46	4.42	4.41	4.44	4.43	4.45	4.41

概率为 $p_0=1-R_a/n$， $p_1=p_{-1}=(R_a/n-R_a\cdot c/(2\cdot n))/2$， $p_3=p_{-3}=R_a\cdot c/(4\cdot n)$。

取邻域半径 $r=1$，由于 $-3=+1(\mathrm{mod}\,4)$ 和 $+3=-1(\mathrm{mod}\,4)$，所以载体图像像素可能出现的修改幅度值的集合为 $\{0,-1,+1\}$，各个修改幅度值出现的概率为 $p_0^{'}=p_0/k=(1-R_a/n)/k$， $p_1^{'}=(p_1+p_{-3})/k=R_a/(2\cdot k\cdot n)$， $p_{-1}^{'}=(p_{-1}+p_3)/k=R_a/(2\cdot k\cdot n)$。

这样可以计算出平均失真 $D=p_0^{'}\cdot 0^2+p_1^{'}\cdot 1^2+p_{-1}^{'}\cdot(-1)^2$，从而可以得到 DLE 算法的嵌入效率为 $e=\alpha_2/D=l/R_a+\alpha$。例如，实验中隐写码 $\mathrm{SC}(R_a,n,l)$ 取为 $\mathrm{SC}(7/2^3,7,3)$，湿纸码 $\mathrm{WPC}(\alpha,c)$ 取为 $\mathrm{WPC}(1,1/2)$，可以计算出 $e=31/7\approx 4.43$，这说明理论推导结果与实验结果相符合。

最后考察一下 Steghide 和 DLE 算法抵抗一阶统计攻击的能力。M-不饱和的顶点的数量就是一阶统计改变量的上界。从 4.1 节中匹配率的实验结果可以看出，对于自然的灰度图像， DLE 算法的 M-不饱和的顶点所占比例<1%，所以可以获得足够好的最大势最小重量匹配。另外，因为 DLE 算法的 M-饱和的顶点所占比例>99%，高于 Steghide，所以 DLE 算法能够更好保持载体图像的一阶直方图，从而更好抵抗一阶统计攻击。

5 结束语

本文结合二元隐写码、湿纸码和图匹配理论提出了一种可保持载体图像一阶直方图的双层嵌入隐写算法。实验结果和理论分析都表明：相对于 Steghide，在嵌入相同消息长度的情况下，DLE 算法减小了载体图像的失真，从而提高了嵌入效率；而且 DLE 算法能更好的保持载体图像的一阶统计特性，进而能抵抗常见的一阶统计攻击。设计能保持高阶统计特性的隐写算法将是下一步要研究的问题。

参 考 文 献

[1] Zhang Wei-ming and Li Shi-qu. A coding problem in steganography[J]. *Designs, Codes and Cryptography*, 2008, 46(1): 67–81.

[2] Fridrich J, Goljan M, and Lisonek P, *et al*.. Writing on wet paper[J]. *IEEE Transactions on Signal Processing*, 2005, 53(10): 3923–3935.

[3] Filler T, Judas J, and Fridrich J. Minimizing embedding impact in steganography using trellis-coded quantization[C]. Proceedings of SPIE, Electronic Imaging, Media Forensics and Security XII, San Jose, CA, USA, Jan. 18–22, 2009, 5: 1–14.

[4] Zhang Wei-ming, Zhang Xin-peng, and Wang Shuo-zhong. Near-optimal codes for information embedding in gray-scale signals[J]. *IEEE Transactions on Information Theory*, 2010, 56(3): 1262–1270.

[5] Filler T and Fridrich J. Wet ZZW construction for steganography[C]. IEEE Workshop on Information Forensic and Security (WIFS), London, UK, December 7–9, 2009: 131–135.

[6] Zhang Wei-ming and Zhu Xue-xiu. Improving the embedding efficiency of wet paper codes by paper folding[J]. *IEEE Signal Processing Letters*, 2009, 16(9): 794–797.

[7] Amiruzzaman M and Hyoung J K. Secure steganographic method[C]. Proceedings of 5th International Conference on Visual Information Engineering, Xi'an, China, July 29– Aug 1, 2008: 141–145.

[8] Lee Y, Bell G, and Huang S, *et al*.. An advanced least-significant-bit embedding scheme for steganographic encoding[C]. Proceedings of the 3rd Pacific Rim Symposium on Advances in Image and Video Technology, Tokyo, Japan, on January 13–16, 2009: 349–360.

[9] Zhang Xin-peng, Wang Shuo-zhong, and Zhang Wei-ming. Steganography with histogram-preserving and distortion-constraining properties[C]. 2009 International Conference on Multimedia Information Networking and Security, Wuhan, China, Nov.18–20, 2009, 1: 30–34.

[10] Hetzl S and Mutzel P. A graph-theoretic approach to steganography[C]. Proceedings of 9th IFIP TC-6 TC-11 International Conference on Communications and Multimedia Security, Salzburg, Austria, September 19–21, 2005: 119–128.

[11] Hetzl S. Steghide. http://steghide.sourceforge.net/. 2010.04.

[12] Hioki H. Web behind web — a steganographic web framework[C]. Proceedings of the 5th International Conference on Intelligent Information Hiding and Multimedia Signal Processing, Kyoto, Japan, September 12–14, 2009: 60–63.

[13] Zhang Xin-peng, Zhang Wei-ming, and Wang Shuo-zhong. Efficient double-layered steganographic embedding[J]. *IET Electronics Letters*, 2007, 43(8): 482–483.

[14] Zhang Wei-ming, Zhang Xin-peng, and Wang Shuo-zhong. A double layered "plus-minus one" data embedding scheme[J]. *IEEE Signal Processing Letters*, 2007, 14(11): 848–851.

[15] Mohring R and Muller-Hannemann M. Cardinality matching: heuristic search for augmenting paths[R]. Technical Report 439 of Fachbereich Mathematik, Technische Universit Berlin, 1995.

刘九芬： 女，1963 年生，副教授，研究方向为小波理论及其应用和信息隐藏.

韩 涛： 男，1986 年生，硕士生，研究方向为信息隐藏.

张卫明： 男，1976 年生，讲师，研究方向为密码学和信息隐藏.