基于 Canny 边缘检测的自适应空域隐写术

韩 涛* 祝跃飞
(信息工程大学 郑州 450001)
(数学工程与先进计算国家重点实验室 郑州 450001)

摘 要：针对自适应空域隐写术设计的关键问题，该文结合 Canny 边缘检测和校验格编码(STC)提出一种不需要同步边信息的自适应空域隐写方法。首先，根据秘密消息长度、载体图像等因素确定 Canny 边缘检测算法中的参数取值，进而根据相应的参数取值使用 Canny 边缘检测算法来选择载体图像的边缘区域。然后，分别定义边缘区域像素和非边缘区域像素的嵌入失真；最后，在载体像素的多个最低有效位平面(LSB)使用 STC 嵌入秘密消息。实验结果表明：该隐写方法在 4 种嵌入率情况下抵抗常见通用隐写分析的性能优于 3 种已有的隐写方法，且在较小嵌入率情况下与空域通用小波相对失真方法(S-UNIWARD)相当。

关键词：信息安全；隐写术；自适应隐写；边缘检测；校验格编码
中图分类号：TP309 **文献标识码**：A **文章编号**：1009-5896(2015)05-1266-05
DOI: 10.11999/JEIT141121

Adaptive Spatial Steganography Based on Canny's Edge Detection

Han Tao Zhu Yue-fei
(*Information Engineering University*, *Zhengzhou* 450001, *China*)
(*State Key Laboratory of Mathematical Engineering and Advanced Computing*, *Zhengzhou* 450001, *China*)

Abstract: Aiming at the essential problems of the design of adaptive spatial steganography, this paper proposes an adaptive spatial steganographic algorithm without synchronizing the side information, combining with Canny's edge detection algorithm and the Syndrome Trellis Code (STC). Firstly, the parameters of Canny's algorithm are obtained on the basis of the factors, including the length of the secret message, the cover image, and so on; then Canny's algorithm is used to select the edge region of the cover image. Moreover, the embedding distortions of the edge and non-edge pixels are defined respectively. Finally, the STC is used to embed the secret message in multiple Least Significant Bit (LSB) planes of the pixels. The experimental results illustrate that, under the condition of four kinds of embedding rates, when resisting common universal steganalysis, the proposed method performs better than other three existing methods, and is comparable to the Spatial-UNIversal WAvelet Relative Distortion (S-UNIWARD) under the condition of small embedding rates.

Key words: Information security; Steganography; Adaptive steganography; Edge detection; Syndrome Trellis Code (STC)

1 前言

随着计算机网络技术和信息技术的不断发展，人们在享受新技术带来便利的同时，个人隐私等方面也遭受着各种可能的安全威胁。人们不仅要求通信内容能保密，而且通信行为能隐蔽地进行，这种新的通信模式称为隐蔽的保密通信。这种模式可以通过信息隐藏技术来实现。作为信息隐藏的一个重要分支，隐写术主要研究如何在公开的多媒体数据隐藏秘密消息以实现隐蔽通信。按照秘密消息嵌入是否自适应地进行，隐写术可分为非自适应隐写和自适应隐写。自适应隐写是指根据载体特性自适应地将秘密消息嵌入到最不容易引起怀疑的区域，从而提高隐写术抵抗隐写分析的能力，目前是隐写术的一个研究热点。而本文主要关注空域图像上的自适应隐写，所以下面主要介绍自适应空域隐写术的研究现状。根据接收者是否需要边信息以重构承载秘密消息的像素（也称边信息同步），自适应空域隐写术主要可分为两类：

第 1 类是不需要同步边信息，即最小化嵌入失真的隐写方法。该类隐写方法是目前隐写术设计最

2014-08-29 收到，2014-12-01 改回
国家科技支撑计划(2012BAH47B01)，国家自然科学基金(61170234, 61309007)，郑州科技创新团队项目(10CXTD150)和信息工程大学博士研究生学位论文创新基金(BSLWCX201309)资助课题
*通信作者：韩涛 lhstslhsts@163.com

热门的研究方向，主要有两个关键问题：一是失真函数的定义；二是自适应隐写编码的设计，文献[1]提出的校验格编码(Syndrome Trellis Code, STC)可较好地解决自适应隐写编码的设计问题。利用邻域像素差分矩阵(Subtractive Pixel Adjacency Matrix, SPAM)[2]隐写分析特征集合来指导嵌入失真函数的设计，文献[3]提出了高度不可检测隐写方法(Highly Undetectable steGO, HUGO)。文献[4]利用小波分析领域的方向滤波来定义空域图像的嵌入失真，提出了权重获得小波方法(Wavelet Obtained Weights, WOW)。文献[5]使用小波分析中方向滤波的分解系数来定义嵌入失真，提出了可应用于任意域的通用小波相对失真方法(UNIversal WAvelet Relative Distortion, UNIWARD)，其中应用于空域的方法称为空域 UNIWARD (Spatial-UNIWARD, S-UNIWARD)，目前 S-UNIWARD 抵抗通用隐写分析的性能最优。

第 2 类是需要同步边信息，其目的是使得接收者能够重构出消息嵌入区域，该类方法称为基于边信息同步的隐写方法。基于改进的最低有效位匹配(LSB Matching Revisited, LMR)[6]，文献[7]提出了边信息同步的边缘自适应 LMR(Edge Adaptive LMR, EALMR)，使用相邻两个像素的差分值作为边缘像素的度量标准。文献[8]提出了只在噪声区域嵌入消息的噪声区域嵌入方法(Noisy Region Embedding, NRE)。在 NRE 的基础上，通过使用双层嵌入构造[9]，文献[10]提出了一种在扩展的噪声区域嵌入消息且边信息同步的扩展 NRE(Extended NRE, ENRE)。基于图像边缘检测和 LSB 替换，文献[11]提出了一种边信息同步的基于边缘的图像隐写方法(Edge-Based Image Steganography, EBIS)。然而，为了实现边信息同步，EBIS 只使用 2 层 LSB 替换，其嵌入效率并不高。

本文在 EBIS 的基础上，结合图像处理领域中的 Canny 边缘检测方法和 STC，提出了一种边缘自适应且不需要同步边信息的隐写方法。本文首先根据嵌入率、载体图像等来确定合适的 Canny 边缘检测算法的参数取值，并使用 Canny 边缘检测算法来选择图像的边缘区域，然后根据非边缘区域内的像素为不可修改像素、边缘区域内的像素为可修改像素的原则，定义像素的嵌入失真，最后使用多层 STC 嵌入秘密消息。抵抗通用隐写分析实验的结果表明：本文方法的性能优于 3 种已有的隐写方法，在较小嵌入率时与 S-UNIWARD 性能相当。

2　预备知识

2.1 Canny 边缘检测算法

Canny 边缘检测算法是文献[12]于 1986 年提出的一个多级边缘检测算法。其目标是寻找一个最优的边缘检测算法，主要包括以下 3 个方面：(1)最优检测；(2)最优定位准则；(3)检测点与边缘点一一对应。Canny 边缘检测算法很好地结合了最优边缘检测的 3 个准则。首先使用高斯滤波器平滑图像，其次使用一阶偏导的有限差分来计算梯度的幅值和方向，再次通过寻找图像梯度的局部极大值对梯度幅值进行非极大值抑制，最后通过双阈值法来检测强边缘和弱边缘，当弱边缘与强边缘连接成轮廓边缘才输出。因此，Canny 边缘检测算法不易受噪声影响，能在噪声和边缘检测间取得较好的平衡，具有很好的边缘检测性能。

Canny 边缘检测算法包含许多可调整的参数，参数的取值会影响到算法的性能。根据本文方法的需求，本文主要考虑的参数包括：(1)高斯滤波器的宽度 w，w 的取值会直接影响 Canny 边缘检测算法的结果；(2)高阈值 th 和低阈值 tl，tl 用于控制边缘连接，th 用于控制强边缘的初始分割，通常情况下，取 $\mathrm{tl}=0.4\times\mathrm{th}$。

2.2 STC

文献[1]提出的 STC 是目前编码性能最优的二元隐写编码方法。STC 是一种特殊的矩阵编码，其奇偶校验矩阵 $\boldsymbol{H}$ 由大小为 $h\times w$ 的子矩阵 $\widehat{\boldsymbol{H}}$ 以一种级联的方式拼接而成，$\widehat{\boldsymbol{H}}$ 是根据共享密钥随机生成的，其中参数 h 的取值主要影响 STC 的速度和效率，w 的取值由嵌入率决定。其目的是发送者通过将二元载体 $\boldsymbol{x}$ 修改为载密 $\boldsymbol{y}$ 来嵌入消息 $\boldsymbol{m}$，即 $\boldsymbol{H}\boldsymbol{y}^{\mathrm{T}}=\boldsymbol{m}^{\mathrm{T}}$，同时使总嵌入失真尽可能小，从而接收者通过计算 $\boldsymbol{H}\boldsymbol{y}^{\mathrm{T}}$ 即可提取消息 $\boldsymbol{m}^{\mathrm{T}}$。STC 将最小化总嵌入失真问题转化为寻找最短路径问题，而后者可以由维特比译码的方式快速得到。注意到嵌入失真 $\rho(\boldsymbol{x},\boldsymbol{y})$ 可以由消息嵌入者根据任意的原则来定义。

另外，受双层嵌入构造[9]的启发，文献[1]提出了 STC 的多层嵌入构造。在 2 层 STC 中，载体元素的最大修改幅度为 1，修改方式为 $\{-1,0,+1\}$，最大理论嵌入率为 $\log_2 3$，由于 2 层 STC 是一个概率算法，即对于给定的嵌入率，LSB 平面的湿点数量并不一定等于 0，可能会发生嵌入失败的情况，所以实际最大嵌入率 α_{DSTC} 达不到 $\log_2 3$，其范围一般为 $[1,\log_2 3)$；在 3 层 STC 中载体元素的最大修改幅度为 2，修改方式为 $\{-2,-1,0,+1,+2\}$，最大理论嵌入率为 $\log_2 5$，同理由于 3 层 STC 也是一个概率算法，所以实际最大嵌入率 α_{TSTC} 达不到 $\log_2 5$，其范围一般为 $[\log_2 3,\log_2 5)$。

3 基于 Canny 边缘检测的自适应空域隐写方法

本文方法的嵌入过程主要包含 4 步：(1)根据 Canny 边缘检测算法选择嵌入区域；(2)定义载体像素的嵌入失真，然后使用多层 STC 嵌入秘密消息；(3)使用 LSB 匹配嵌入头信息；(4)生成载密图像。提取过程主要包括两步：(1)提取头信息；(2)使用 STC 提取秘密消息。

3.1 嵌入过程

下面详细描述本文方法的嵌入过程。

步骤 1 选择嵌入区域。使用 Canny 边缘检测算法来选择图像边缘作为嵌入区域 E，嵌入区域的大小依赖于嵌入消息长度、载体图像和所使用的自适应隐写编码方法。注意到此处本文使用 Canny 边缘检测，是因为新的边缘检测方法可能会更加准确地定位边缘区域，同时也会带来时间复杂度上的代价，而隐写方法的时间复杂度也是需要考虑的重要因素，为了实现时间复杂度和性能两方面的折中，本文使用可快速实现且成熟的 Canny 边缘检测来定位边缘区域。注意到，已有的相关研究表明，在设计隐写方法时，使用 LSB 嵌入的方式能获得更高的安全性，因此，本文方法使用 2 层和 3 层 STC 来嵌入秘密消息。为了将秘密消息集中嵌入到边缘区域，引入调整因子 q 用于嵌入区域的选择：当使用 2 层 STC 嵌入秘密消息时，q 的取值范围为 $[1,\alpha_{\mathrm{DSTC}}]$；当使用 3 层 STC 嵌入秘密消息时，$q$ 的取值范围为 $[1,\alpha_{\mathrm{TSTC}}]$。

使用二分搜索法寻找合适的高阈值 th，需要满足两个条件：一是根据 th 得到的边缘像素数量足以承载待嵌入的秘密消息；二是尽可能将秘密消息集中于边缘像素，即根据 th 选取的边缘像素数量不能过多地超过所需数量。获得高阈值 th 的算法如表 1 所示。

表 1 获得高阈值 th 的算法

输入：载体图像 C，调整因子 q，限制因子 l，秘密消息长度 L，高斯滤波器的宽度 w。

输出：高阈值 th。

(1) 设 $\mathrm{th}_1=1$，$\mathrm{th}_2=0$，实际所需的边缘像素个数为 L/q；

(2) 令 $\mathrm{th}=(\mathrm{th}_1+\mathrm{th}_2)/2$，使用 Canny 边缘检测算法获得 C 的边缘，参数为 $\mathrm{tl}=0.4\times\mathrm{th}$，th 和 w，则可通过计算得到边缘像素数量，设为 k_{E}；

(3) 若 $k_{\mathrm{E}}>(1+l)\times L/q$，则令 $\mathrm{th}_1=\mathrm{th}$；若 $k_{\mathrm{E}}<L/q$，则令 $\mathrm{th}_2=\mathrm{th}$。若 k_{E} 的取值出现上述两种情况，则重复(2)，即重新计算边缘像素数量 k_{E}，直到 k_{E} 满足 $L/q\le k_{\mathrm{E}}\le(1+l)\times L/q$，此时返回高阈值 th。

在获得高阈值 th 之后，根据参数 tl，th 和 w 的取值，使用 Canny 边缘检测算法获得载体图像 C 的边缘像素的位置，即为嵌入区域 E。由于经 Canny 边缘检测得到的边缘像素数量并不一定刚好等于实际所需的像素数量，所以使用一个限制因子 l 来控制选出的边缘像素数量，在本文实验中，限制因子取 $l=0.01$。

步骤 2 在嵌入区域 E 上嵌入秘密消息。使用发送者和接收者之间共享的密钥 K 置乱大小为 $h_{\mathrm{C}}\times w_{\mathrm{C}}$ 的载体图像 C，假设载体图像置乱后得到的载体像素为 $\boldsymbol{c}=(c_1,c_2,\cdots,c_N)$，载密像素为 $\boldsymbol{s}=(s_1,s_2,\cdots,s_N)$。若使用 2 层 STC，则载密像素 s_i 的取值范围为 $I_i=\{c_i-1,c_i,c_i+1\}$，嵌入失真定义为

$$\rho_2(c_i,s_i)=\begin{cases}0, & s_i=c_i\\ 1, & s_i=c_i-1,\ c_i\in\mathrm{E},\ c_i\neq 0\\ 1, & s_i=c_i+1,\ c_i\in\mathrm{E},\ c_i\neq 255\\ \infty, & \text{其它}\end{cases}\tag{1}$$

若使用 3 层 STC，则载密像素 s_i 的取值范围为 $I_i=\{c_i-2,c_i-1,c_i,c_i+1,c_i+2\}$，嵌入失真定义为

$$\rho_3(c_i,s_i)=\begin{cases}0, & s_i=c_i\\ 1, & s_i=c_i-1,\ c_i\in\mathrm{E},c_i\neq 0\\ 1, & s_i=c_i+1,\ c_i\in\mathrm{E},c_i\neq 255\\ 2^2, & s_i=c_i+2,\ c_i\in\mathrm{E},\ c_i\neq 255\,\text{or}\,254\\ 2^2, & s_i=c_i-2,\ c_i\in\mathrm{E},\ c_i\neq 0\,\text{or}\,1\\ \infty, & \text{其它}\end{cases}\tag{2}$$

注意到以上只是给出一种简单的嵌入失真定义用于本文方法的描述，消息嵌入者可根据一定的原则任意的定义嵌入失真。使用 f 作为标志位来表示所使用的 STC 层数：若 $f=0$，则表示使用 2 层 STC；若 $f=1$，则表示使用 3 层 STC。在嵌入失真定义结束后，根据 f 的取值，调用 STC 分别在载体图像的 2 或 3 个 LSB 平面上嵌入秘密消息。

步骤 3 同步头信息。为了保证接收者能够正确提取秘密消息，需要将标志位 f 和各层 LSB 承载的秘密消息长度通信给接收者，其中，标志位 f 占用 1 bit，每层 LSB 承载的秘密消息长度占用 24 bit。若 $f=0$，则头信息 h 总共占用 $1+24+24=49$ bit，使用 LSB 匹配将 49 bit 的头信息 h 嵌入到图像置乱后的载体像素 $(c_1,c_2,\cdots,c_{49})$；同理，若 $f=1$，则头信息总共占用 $1+24+24+24=73$ bit，使用 LSB 匹配将 73 bit 的头信息 h 嵌入到载体像素 $(c_1,c_2,\cdots,c_{73})$。

步骤 4 生成载密图像。在嵌入头信息和秘密消息后，可以得到载密像素 $\boldsymbol{s}$。使用共享密钥 K 将 $\boldsymbol{s}$

恢复为大小为 $h_C \times w_C$ 的载密图像，设为 S，最后将载密图像 S 发送给接收者。

3.2 提取过程

下面给出从载密图像 S 中提取秘密消息 $\boldsymbol{m}$ 的过程。

步骤 1　提取头信息 h。首先根据共享密钥 K 置乱载密图像 S，设置乱后的载密像素为 $\boldsymbol{s}=(s_1, s_2, \cdots, s_N)$，然后提取载密像素 s_1 的 LSB 作为标志位 f。若 $f=0$，则分别提取载密像素 $(s_2, s_3, \cdots, s_{25})$ 和 $(s_{26}, s_{27}, \cdots, s_{49})$ 的 LSB，按顺序构成次 LSB 层和 LSB 层承载的秘密消息长度，设为 L_2 和 L_1；同理，若 $f=1$，则分别提取载密像素 $(s_2, s_3, \cdots, s_{25})$，$(s_{26}, s_{27}, \cdots, s_{49})$ 和 $(s_{50}, s_{51}, \cdots, s_{73})$ 的 LSB，按顺序构成第 3 层 LSB、次 LSB 层和 LSB 层承载的秘密消息长度，设为 L_3, L_2 和 L_1。

步骤 2　根据头信息 h 使用 STC 提取秘密消息。根据共享密钥 K 重新生成 STC 的奇偶校验矩阵 $\boldsymbol{H}$。若 $f=0$，即嵌入过程使用 2 层 STC，则使用 STC 分别从载密像素 $(s_{50}, s_{51}, \cdots, s_N)$ 的次 LSB 层和 LSB 层提取长度为 L_2 和 L_1 bit 的秘密消息，构成长度为 $L=L_1+L_2$ 的秘密消息 $\boldsymbol{m}$；若 $f=1$，即嵌入过程使用 3 层 STC，则使用 STC 分别从载密像素 $(s_{74}, s_{75}, \cdots, s_N)$ 的第 3 层 LSB、次 LSB 和 LSB 提取长度为 L_3，L_2 和 L_1 bit 的秘密消息，构成长度为 $L=(L_1+L_2+L_3)$ bit 的秘密消息 $\boldsymbol{m}$。

4　实验结果与分析

选择 BOSSbase1.01 图像库[13]为实验图像库，该图像库中的图像来源于 8 个不同的数码相机，经过重新裁剪得到 10000 幅大小为 512×512 的未压缩灰度空域图像，图像格式为 pgm。根据嵌入率，使用伪随机数发生器来生成二元随机秘密消息，用于模拟经过加密的秘密消息。使用通用隐写分析来评估隐写方法的安全性。在实验中，本文方法用到的高斯滤波器宽度 w 的取值范围为 [0,1]，调整因子 q 的取值范围为 [1,1.5]。对于给定的参数 w 和 q，针对不同的嵌入率和载体图像，根据表 1 给出的算法得到高阈值 th，用于选择嵌入区域，并分别使用 2 层和 3 层 STC 嵌入秘密消息，最后在所有结果中选择抵抗通用隐写分析性能最好的结果。在实验中选择 0.05, 0.10, 0.15, 0.20 位/像素作为本文方法的嵌入率，这是因为：当嵌入率超过 0.25 位/像素时，BOSSbase1.01 中会有大量的载体图像经过 Canny 边缘检测得到的边缘像素数量少于像素总数量的 25%，即使用本文方法不能在这些图像中嵌入超过 25%的秘密消息。

在抵抗通用隐写分析的实验中，用于性能对比的隐写方法有：EALMR[7], EBIS[11], HUGO[3], S-UNIWARD[5]和本文方法。分别使用以上 5 种隐写方法在 BOSSbase1.01 图像库上嵌入二元随机秘密消息，嵌入率为 0.05, 0.10, 0.15 和 0.20 位/像素。使用集成分类器(Ensemble Classifier)[14]进行训练和测试。所有图像库中均选择 50%的图像用于训练，剩余 50%用于测试。测试结果用最小平均分类错误率来 P_{E} 表示，$P_{\mathrm{E}}=\min_{P_{\mathrm{FA}}}\left[(P_{\mathrm{FA}}+P_{\mathrm{MD}}(P_{\mathrm{FA}}))/2\right]$，其中 P_{FA} 表示虚警率，P_{MD} 表示漏检率。P_{E} 越大，表明隐写方法抵抗隐写分析的能力越强，即隐写方法越安全。当载体图像和载密图像不能区分时，P_{E} 接近 0.5。

首先考察本文方法与基于边信息同步的隐写方法(EALMR[7], EBIS[11])抵抗 686 维 SPAM 隐写分析[2]的性能对比。对于 EALMR，参数设置与文献[7]中一致，使用 LMR[6]嵌入消息。对于 EBIS，参数设置与文献[11]中一致，使用 LMR[6]嵌入消息。检测结果如图 1 所示。从图 1 可以看出，相对于 2 种基于边信息同步的隐写方法，在所给的 4 种嵌入率情况下，SPAM 检测本文方法的错误率 P_{E} 更高，即本文方法抵抗 SPAM 的能力更强，主要因为本文方法使用 Canny 边缘检测方法能够精确地选择边缘像素，并使用高效的多层 STC 在边缘像素上嵌入消息，将嵌入修改集中在边缘区域。

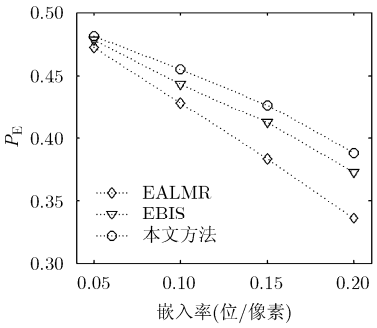

图 1　3 种隐写方法抵抗 SPAM 隐写分析的实验结果

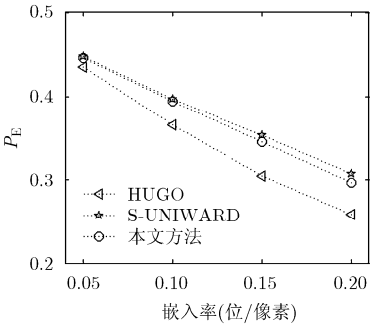

图 2　3 种隐写方法抵抗 SRM 隐写分析的实验结果

其次考察本文方法与基于最小化嵌入失真的隐写方法(HUGO[3], S-UNIWARD[5])抵抗 34671 维空域富模型(Spatial Rich Model, SRM)隐写分析[15]的性能对比。对于 HUGO，使用 $T=255$ 来消除 $T=90$ 带来的安全问题。对于 S-UNIWARD，参数设置与文献[5]中一致，参数 σ 取值为 $\sigma=1$。检测结果如图 2 所示。从图 2 可以看出，在所给的 4 种嵌入率情况下，本文方法抵抗 SRM 的性能优于 HUGO，并在较小嵌入率情况下与 S-UNIWARD 相当，这主要因为：在较小嵌入率情况下，本文方法中 Canny 边缘检测方法所选择的边缘区域与 S-UNIWARD 的嵌入区域比较相近，都能很好地选择出纹理最复杂的区域用于承载秘密消息。

5 结束语

本文结合边缘检测和高效自适应隐写编码，提出了一种不需要同步边信息的自适应空域隐写方法。实验表明：本文方法抵抗常见通用隐写分析方法的性能优于已有的 3 种自适应隐写方法，并在较小嵌入率情况下与 S-UNIWARD 性能相当。在未来的工作中考虑使用更加精确的边缘检测算法来检测边缘区域，进而改进本文方法的性能。

参 考 文 献

[1] Filler T, Judas J, and Fridrich J. Minimizing additive distortion in steganography using syndrome-trellis codes[J]. *IEEE Transactions on Information Forensics and Security*, 2011, 6(3): 920–935.

[2] Pevný T, Bas P, and Fridrich J. Steganalysis by subtractive pixel adjacency matrix[J]. *IEEE Transactions on Information Forensics and Security*, 2010, 5(2): 215–224.

[3] Pevný T, Filler T, and Bas P. Using high-dimensional image models to perform highly undetectable steganography[C]. Proceedings of 12th International Workshop on Information Hiding, Calgary, Canada, 2010: 161–177.

[4] Holub V and Fridrich J. Designing steganographic distortion using directional filters[C]. Proceedings of the IEEE International Workshop on Information Forensics and Security (WIFS), Tenerife, Spain, 2012: 234–239.

[5] Holub V, Fridrich J, and Denemark T. Universal distortion function for steganography in an arbitrary domain[J]. *EURASIP Journal on Information Security*, 2014, 2014(1): 1–13.

[6] Mielikainen J. LSB matching revisited[J]. *IEEE Signal Processing Letters*, 2006, 13(5): 285–287.

[7] Luo W, Huang F, and Huang J. Edge adaptive image steganography based on LSB matching revisited[J]. *IEEE Transactions on Information Forensics and Security*, 2010, 5(2): 201–214.

[8] Lu Y, Li X, and Yang B. A secure steganography: noisy region embedding[C]. Proceedings of the 5th International Conference on Intelligent Information Hiding and Multimedia Signal Processing, Kyoto, Japan, 2009: 1046–1051.

[9] Zhang W, Zhang X, and Wang S. A double layered "plus-minus one" data embedding scheme[J]. *IEEE Signal Processing Letters*, 2007, 14(11): 848–851.

[10] Han T, Zhang W, Wang C, *et al.*. Adaptive ±1 steganography in extended noisy region[J]. *The Computer Journal*, 2014, 57(4): 557–566.

[11] Islam S, Modi M R, and Gupta P. Edge-based image steganography[J]. *EURASIP Journal on Information Security*, 2014, 2014(8): 1–14.

[12] Canny J. A computational approach to edge detection[J]. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 1986, PAMI-8(6): 679–698.

[13] Bas P, Filler T, and Pevný T. "Break our steganographic system": the ins and outs of organizing BOSS[C]. Proceedings of the 12th International Workshop on Information Hiding, Calgary, Canada, 2010: 59–70.

[14] Kodovsky J, Fridrich J, and Holub V. Ensemble classifiers for steganalysis of digital media[J]. *IEEE Transactions on Information Forensics and Security*, 2012, 7(2): 432–444.

[15] Fridrich J and Kodovsky J. Rich models for steganalysis of digital images[J]. *IEEE Transactions on Information Forensics and Security*, 2012, 7(3): 868–882.

韩 涛： 男，1986 年生，博士生，研究方向为密码学与信息隐藏.

祝跃飞： 男，1962 年生，教授，研究方向为密码学与网络安全.