一种基于扩展加减覆盖集的隐写方法

夏冰冰,赵险峰,王明生
(中国科学院信息工程研究所,北京 100093)

摘 要: G-LSB-M隐写方法是一种±1隐写嵌入方法,通过减少嵌入时的修改次数提高隐写的嵌入效率.该方法嵌入时所用的加减覆盖集只能通过穷举搜索构造,当嵌入消息分段长度 n 较大时,穷举搜索的计算代价过高导致无法实现.为了解决这一问题,本文提出了基于扩展加减覆盖集的隐写方法,通过从基础加减覆盖集中去除若干非必需的元素,能够以较小的计算代价构造出扩展加减覆盖集,避免了G-LSB-M方法中的穷举搜索困难,使得使用更长的信息分段进行嵌入成为可能.该方法降低了隐写时的平均修改次数,提高了嵌入效率和隐写的隐蔽性.

关键词: 扩展加减覆盖集;LSB匹配;隐写;嵌入效率
中图分类号: TN918 **文献标识码:** A **文章编号:** 0372-2112 (2014) 06-1168-05
电子学报URL: http://www.ejournal.org.cn **DOI:** 10.3969/j.issn.0372-2112.2014.06.020

Steganography Based on Extended Sum and Difference Covering Set

XIA Bing-bing, ZHAO Xian-feng, WANG Ming-sheng
(*Institute of Information Engineering, Chinese Academy of Sciences, Beijing* 100093, *China*)

Abstract: Generalized least significant bit matching (G-LSB-M) steganography scheme is a ±1 embedding method which minimizes the number of modifications per pixel to improve the embedding efficiency. The sum and difference covering set (SDCS) used for embedding can only be obtained through exhaustive search, which is hard to implement when the number of message bits increases. To solve this problem, we provide a novel steganography method based on the extended SDCS (ESDCS). The ESDCS is constructed by removing redundant elements from the so-called basic SDCS without exhaustive search, which implies that longer message segments could be used in the embedding process. The proposed method reduces the expect number of modifications and thus improves the embedding efficiency as well as the security of steganography.

Key words: extended sum and difference covering set; LSB matching; steganography; embedding efficiency

1 引言

现代隐写术以不可感知的方式将隐蔽信息嵌入数字图像、音频、视频、文本等载体数据中,实现隐蔽信息的传递或存储.嵌入过程对载体数据感知质量的影响很小,使得嵌入隐蔽信息后的数字内容(称为"隐文")与原始载体数据(称为"原文")很难被人类感知系统区分开[1,2].

然而,隐写对载体数据分布的改变能够被某些统计量反应出来,这为隐写分析提供了依据.通过选择对隐写造成的扰动较为敏感的统计量作为特征,隐写分析者可以训练出有效的分类器判断待测样本中是否包含隐蔽信息[3~6].每嵌入1比特信息时对载体数据进行修改的平均修改量是衡量隐写方法安全性的重要指标之一.在嵌入信息长度不变的前提下,如何减少嵌入时的平均修改量成为了近年来隐写研究的热点[7].

LSB替换方法[8]是一种嵌入隐蔽信息的常用方法,通过修改载体数据的最低比特位LSB(Least Significant Bit)表达隐蔽信息.这类嵌入方法对载体数据每个样点值的修改幅度恒定为1,因此其嵌入修改量可以用嵌入时的修改次数(即需要修改的载体样点值数量)衡量.LSB替换方法嵌入1比特信息的平均修改次数为0.5次.LSB匹配[9]是Sharp提出的一种改进LSB替换方法的隐写方法,在需要修改载体样点值的LSB位置时随机选择+1或-1操作,消除了LSB替换方法嵌入时造成的样点直方图非对称性,提高了隐写的安全性.该方法并未减少嵌入时的平均修改次数,但却提供了一种全新的思路.隐写者可以在嵌入过程中有目的的选择+1或-1操作,从而在每次修改操作时表达更多信息.降低隐写嵌入的平均修改量.Mielikainer[10]提出的LSB Matching Revisited隐写方法运用了这种思想,以一对样点值为嵌入对象,使用这两个样点值的奇偶关系表达额

收稿日期:2012-10-23;修回日期:2013-07-31;责任编辑:梅志强
基金项目:北京市自然科学基金课题(No.4112063);国家自然科学基金课题(No.61170281,No.61303259);中国科学院战略性先导科技专项课题(No.XDA06030600);中科院信工所密码基金(No.Y3Z0012102)

外的信息比特,从而将嵌入1比特信息的平均修改次数降低至0.375次.Li等人[11]将这一思路推广至更一般化的情况,提出了G-LSB-M(Generalized LSB Matching)隐写嵌入方法.Li等人证明了LSB Matching Revisited隐写方法是G-LSB-M在嵌入消息分段长度 $n=2$ 时的一个特例;当 n 值增加时,G-LSB-M能够达到更小的平均修改次数,其理论极限值为0.2271.然而G-LSB-M方法的构造依靠对有限循环群 $\mathbb{Z}_{2^n}$ 上的加减覆盖集(SDCS,Sum and Difference Covering Set)进行穷举搜索,当 $n>6$ 时其计算代价过高导致难以实现[11].

为了解决G-LSB-M面临的问题,本文提出了一种构造扩展的加减覆盖集(E-SDCS,Extended SDCS)的方法.该方法无需穷举搜索,能够以较小的计算代价构造出扩展加减覆盖集.使用扩展加减覆盖集嵌入隐蔽信息时,无论 n 为何值嵌入每段信息的修改次数均不超过2次.这意味着,在嵌入信息总量不变的情况下,随着 n 的增加,嵌入所需的信息分段数量减少,同时嵌入每段信息的计算复杂度却并未显著增长,因而缩短了嵌入所需的时间,减小了嵌入时的平均修改次数,提高了隐写的嵌入效率和隐蔽性.

2　G-LSB-M隐写方法

G-LSB-M是Li等人[11]提出的一种隐写嵌入方法.令 $\boldsymbol{X}=\{x_1,x_2,\cdots,x_n\}$ 表示载体样点值序列,$\boldsymbol{M}=\{m_1,m_2,\cdots,m_n\}$ 表示嵌入的信息比特序列,则G-LSB-M嵌入方法的基本思路是寻找满足如下条件的序列 $\boldsymbol{Y}=\{y_1,y_2,\cdots,y_n\}$ 作为嵌入隐蔽信息后的样点值序列:

(1) $f(\boldsymbol{Y})=\left(\sum_i a_i y_i\right)_{\bmod 2^n}=M_{10}$,其中 M_{10} 表示待嵌入的信息序列 $\boldsymbol{M}$ 转换成十进制整数的结果.系数序列 $A=\{a_1,a_2,\cdots,a_n\}$ 为该方法中需要设计的参数,其取值会影响嵌入时的平均修改量.

(2) $\|\boldsymbol{Y}-\boldsymbol{X}\|$ 尽可能小,即嵌入过程对载体的扰动尽可能小.

令 $\boldsymbol{\Delta}=\{\delta_1,\delta_2,\cdots,\delta_n\}$ 表示嵌入过程对载体的扰动,即 $\boldsymbol{\Delta}=\boldsymbol{Y}-\boldsymbol{X}$,则有:

$$\begin{aligned} f(\boldsymbol{\Delta})&=f(\boldsymbol{Y}-\boldsymbol{X})=(f(\boldsymbol{Y})-f(\boldsymbol{X}))_{\bmod 2^n}\\ &=(M_{10}-f(\boldsymbol{X}))_{\bmod 2^n}\end{aligned}\tag{1}$$

为了便于理解,将上式等号左端的 $f(\boldsymbol{\Delta})$ 展开,得到:

$$\left(\sum_j \alpha_i\delta_i\right)_{\bmod 2^n}=(M_{10}-f(\boldsymbol{X}))_{\bmod 2^n}\tag{2}$$

在确定系数序列 $A=\{a_1,a_2,\cdots,a_n\}$ 之后,对于给定的载体 $\boldsymbol{X}$ 和信息 $\boldsymbol{M}$,寻找满足公式(2)的扰动序列 $\boldsymbol{\Delta}$ 即可完成隐写嵌入.

系数序列 A 的设计是构造G-LSB-M嵌入方法的难点.Li等人指出,设计系数序列 A 的过程等价于寻找有限循环群 $\mathbb{Z}_{2^n}$ 上的加减覆盖集 $A=\{a_1,a_2,\cdots,a_n\}$,满足对于 $\forall z\in\mathbb{Z}_{2^n}$,$\exists\boldsymbol{\Delta}=\{\delta_1,\delta_2,\cdots,\delta_n\}$,$\delta_1\in\{0,\pm1\}$ 使得 $f(\boldsymbol{\Delta})=\left(\sum_j a_i\delta_i\right)_{\bmod 2^n}=z$.

对于每个有限循环群 $\mathbb{Z}_{2^n}$,可能存在多个满足上述条件的加减覆盖集,且各个集合对应的G-LSB-M隐写嵌入方法的平均修改量也存在差异.寻找平均修改次数最低的加减覆盖集 A 只能通过穷举搜索.然而,当 $n>6$ 时,穷举搜索的计算代价过于庞大,实际应用中难以实现[1].Li等人提出使用 $A_t^n=\{t^0,t^1,\cdots,t^{n-1}\}$,$t=2$or3 作为替代,但实验结果显示 A_2^n 的平均修改次数与理论最佳值相差较大;A_3^n 的平均修改次数虽比 A_2^n 小,但难以求得精确的表达式.

3　基于扩展加减覆盖集的隐写方法

为了解决G-LSB-M面临的问题,本文提出了一种构造扩展的加减覆盖集(E-SDCS,Extended SDCS)的方法.该方法无需穷举搜索,能够以较小的计算代价构造出扩展加减覆盖集.使用扩展的加减覆盖集嵌入隐蔽信息时,无论信息分段长度 n 为何值,其嵌入修改次数均不会超过2次.随着 n 的增长,使用扩展加减覆盖集进行隐写嵌入的平均修改次数逐渐减少,嵌入效率比G-LSB-M方法更高.

3.1　基础加减覆盖集的构造

容易验证,集合 $A^0=\{1,2,\cdots,2^{n-1}\}$ 是有限循环群 $\mathbb{Z}_{2^n}$ 的一个加减覆盖集,对于 $\forall z\in\mathbb{Z}_{2^n}$:

(1)若 $z=0$,则 $\boldsymbol{\Delta}=\{0,0,\cdots,0\}$ 可使得 $f(\boldsymbol{\Delta})=0$

(2)若 $z\in[1,2^{n-1}]$,则只需令 $\delta_z=1$、其余 $\delta_i=0$ 即可满足 $f(\boldsymbol{\Delta})=z$

(3)若 $z\in(2^{n-1},2^n)$,则只需令 $\delta_{2^n-z}=-1$、其余 $\delta_i=0$,,此时有

$$f(\boldsymbol{\Delta})=(-(2^n-z))_{\bmod 2^n}=z\tag{3}$$

称集合 $A^0=\{1,2,\cdots,2^{n-1}\}$ 为有限循环群 $\mathbb{Z}_{2^n}$ 的基础加减覆盖集.

3.2　扩展加减覆盖集的构造

从基础加减覆盖集中取出若干非必要的元素,能够在保持其加减覆盖特性的前提下减小其元素个数,获得扩展加减覆盖集.将 A^0 中的元素从 $m+1$ 开始按顺序划分为每 $2m+1$ 个一组,只保留每组中间位置的元素,去掉其余的 $2m$ 个,由此得到 $A^m=\{1,2,\cdots,m,2m+1,2\times(2m+1),3\times(2m+1),\cdots\}$ 仍然是有限循环群 $\mathbb{Z}_{2^n}$ 的一个加减覆盖集:

(1)若 $z=0$,则 $\boldsymbol{\Delta}=\{0,0,\cdots,0\}$ 可使得 $f(\boldsymbol{\Delta})=0$

(2)若 $z\in[1,2^{n-1}]$,则按 z 的取值进一步细分进行讨论:

若 $z=(2m+1)k, k\in\mathbb{Z}^+$,只需令 $\delta_{k+m}=1$、其余 $\delta_i=0$ 即可满足 $f(\boldsymbol{\Delta})=z$;

若 $z=(2m+1)k-\theta, k\in\mathbb{Z}^+, \theta\in[1,m]$,只需令 $\delta_{k+m}=1$、$\delta_\theta=-1$、其余 $\delta_i=0$ 即可满足 $f(\boldsymbol{\Delta})=z$;

若 $z=(2m+1)k+\theta, k\in\mathbb{Z}^+, \theta\in[1,m]$,只需令 δ_{k+m}、$\delta_\theta=1$、其余 $\delta_i=0$ 即可满足 $f(\boldsymbol{\Delta})=z$;

(3)若 $z\in(2^{n-1},2^n)$,则有 $2^n-z\in[0,2^{n-1}]$,此时可以按第(1)、(2)种情况的方法寻找 $\boldsymbol{\Delta}$ 使其满足 $f(\boldsymbol{\Delta})=2^n-z$,然后以 $-\boldsymbol{\Delta}$ 作为最终结果即可.容易验证:

$$f(-\boldsymbol{\Delta})=(2^n-z)_{\bmod 2^n}=z \tag{4}$$

称集合 $A^m=\{1,2,\cdots,m,2m+1,2\times(2m+1),3\times(2m+1),\cdots\}$.为有限循环群 $\mathbb{Z}_{2^n}$ 的 m 阶扩展加减覆盖集.

以 $n=8, m=5$ 的情况为例说明高阶加减覆盖集的构造方法.当 $n=8$ 时,基础加减覆盖集 A^0 包含 $2^{8-1}=128$ 个元素,即 $A^0=\{1,2,\cdots,128\}$.首先将 A^0 中的元素从 6 开始按顺序划分为每 11 个一组:

$$\begin{aligned}&A^0=\\&\{(1,2,3,4,5),\\&(6,7,8,9,10,11,12,13,14,15,16),\\&(17,18,19,20,21,22,23,24,25,26,27),\\&\vdots\\&(116,117,118,119,120,121,122,123,124,125,126),\\&(127,128).\end{aligned} \tag{5}$$

保留每个分组中的中间元素,去除其他元素即可得到 A^5.注意式(5)中的最后一组只包含两个元素,因此任意保留其中一个即可.由此得到 $\mathbb{Z}_{2^8}$ 的一个 5 阶扩展加减覆盖集

$$\boldsymbol{A}^5=\{1,2,3,4,5,11,22,33,\cdots,110,121,127\} \tag{6}$$

m 阶扩展加减覆盖集 A^m 所包含的元素个数为 $\left\lceil\frac{2^{n-1}-m}{2m+1}\right\rceil+m$,约为基础加减覆盖集 A^0 的 $\frac{1}{2m+1}$.其嵌入 1 比特信息的平均修改次数为

$$\frac{\frac{1}{2m+1}\times1+\frac{2m}{2m+1}\times2}{n}=\frac{4m}{n(2m+1)} \tag{7}$$

3.3 基于扩展加减覆盖集的隐写方法

使用扩展加减覆盖集嵌入隐蔽信息时,无论信息分段长度 n 为何值,修改次数均不会超过 2 次.以下给出一个使用 A^5 嵌入隐蔽信息的实例.

载体序列 $\boldsymbol{X}=\{42,194,223,90,175,76,136,213,153,86,77,116,108,92,143,190,109\}$,待嵌入的信息序列 $\boldsymbol{M}=\{0,0,1,1,1,1,0,1\}$.首先使用公式给出的 A^5 计算 $f(\boldsymbol{X})$

$$f(\boldsymbol{X})=\left(\sum_i a_i x_i\right)_{\bmod 2^8}=(109842)_{\bmod 256}=18 \tag{8}$$

然后计算 $f(\boldsymbol{\Delta})$

$$f(\boldsymbol{\Delta})=(M_{10}-f(X))_{\bmod 2^8}=(61-18)_{\bmod 256}=43 \tag{9}$$

A^5 中与 43 最接近的元素为 $a_9=44$,且 $43=44-1$,故令 $\delta_9=1, \delta_1=-1$,其余 $\delta_i=0$,即可满足 $f(\boldsymbol{\Delta})=43$.由此可计算出嵌入隐蔽信息后的序列 $\boldsymbol{Y}$

$$\begin{aligned}\boldsymbol{Y}&=\boldsymbol{X}+\boldsymbol{\Delta}\\&=\{41,194,223,90,175,76,136,213,\\&\quad 154,86,77,116,108,92,143,190,109\}\end{aligned} \tag{10}$$

提取信息时,首先计算 $f(\boldsymbol{Y})$

$$f(\boldsymbol{Y})=\left(\sum_i a_i y_i\right)_{\bmod 2^8}=(109885)_{\bmod 256}=61 \tag{11}$$

然后将结果转换为长度为 8 的二进制序列即可得到信息序列 $\boldsymbol{M}$

$$\boldsymbol{M}=(61)_2=\{0,0,1,1,1,1,0,1\} \tag{12}$$

4 性能分析及实验结果

使用扩展加减覆盖集进行隐写嵌入,避免了 G-LSB-M 方法在构造加减覆盖集时的穷举操作,使得隐写者在嵌入时可以使用更长的信息分段,从而进一步降低嵌入过程的计算复杂度.本文从 BOSSRank[12] 的载体图库中随机选取 100 张 512×512 的灰度图像,分别使用扩展加减覆盖集方法和 G-LSB-M 方法嵌入相同长度(10000 比特)的隐蔽信息,计算每张图像的平均嵌入时间进行比较,结果如表 1 所示.从实验结果可以看出,随着嵌入消息分段长度的提高,使用扩展加减覆盖集嵌入隐蔽信息花费的平均嵌入时间也逐渐减小.这是由于当信息分段长度增加时,分段数量随之下降;而每个分段嵌入时的修改次数始终不超过 2 次(参见 3.2 节的分析和实例),各个分段的嵌入时间并未明显增加.

表 1 平均嵌入时间(单位:ms)

嵌入方法 \ 信息分段长度	2	3	4	5	6	7	8	9	10
G-LSB-M	77.14	50.30	37.40	30.55	25.60	--	--	--	--
1 阶扩展加减覆盖集	75.95	49.48	37.24	29.60	25.66	22.45	20.20	18.19	15.91
2 阶扩展加减覆盖集	72.33	49.41	36.84	29.42	25.15	21.62	19.16	17.59	16.33
3 阶扩展加减覆盖集	--	49.35	37.08	30.08	5.47	21.78	19.22	16.97	15.33
4 阶扩展加减覆盖集	--	47.87	36.66	29.52	25.33	21.45	19.30	17.72	15.83

值得注意的是,表 1 所示的平均嵌入时间并不包含构造加减覆盖集的时间消耗.这是因为在实际的隐写嵌入过程中,隐写者根据选定的隐蔽信息长度 n 构造出加减覆盖集后,即可反复使用该加减覆盖集进行多次隐写嵌入.

嵌入效率是衡量基于嵌入编码的隐写方法性能的一种常用指标,能够客观地比较各种隐写方法在不同负载率下的综合性能.嵌入效率的物理意义是隐写者平均修改 1 个载体样点值时所能嵌入的隐蔽信息数量,其计算公式为

$$e = \frac{\alpha}{d} = \frac{\frac{n}{N}}{\frac{\mathrm{E}(\boldsymbol{\Delta})}{N}} = \frac{n}{\mathrm{E}(\boldsymbol{\Delta})} \tag{13}$$

其中 α 表示负载率,d 表示平均修改量(Expected Number of Modifications Per Pixel,ENMPP),N 表示嵌入 n 比特隐蔽信息所需占用的嵌入位置数量,$\mathrm{E}(\boldsymbol{\Delta})$ 表示嵌入过程中修改次数的期望.注意到式(7)计算的嵌入 1 比特信息的平均修改次数是式(13)的倒数,将其结果代入式(13)可得到基于高阶扩展加减覆盖集隐写方法的嵌入效率计算公式

$$e = \frac{n(2m+1)}{4m} \tag{14}$$

G-LSB-M 方法在 $n>6$ 时由于穷举搜索的计算复杂度过高而无法构造加减覆盖集,因此本文只计算该方法在 $n=2,3,4,5,6$ 时的嵌入效率并与式(14)进行比较.G-LSB-M 方法的隐写负载率恒定为 1,其平均修改量分别为:$d_2=3/8$,$d_3=1/3$,$d_4=11/32$,$d_5=13/40$,$d_6=116/(6\cdot 2^6)$,由此可计算出相应的嵌入效率:$e_2=2.67$,$e_3=3$,$e_4=2.91$,$e_5=3.08$,$e_6=3.31$.由此可以看出,当 $n\geqslant 7$ 时,根据公式计算的嵌入效率 $e>\frac{n\cdot 2m}{4m}=\frac{n}{2}>\frac{7}{2}>e_6$,即当 $n\geqslant 7$ 时本文提出的基于扩展加减覆盖集的隐写方法的嵌入效率将超过 G-LSB-M 方法.

此外,根据 3.3 节的分析,使用 m 阶扩展加减覆盖集 A^m 嵌入 n 比特信息时的隐写负载率为

$$\alpha = \frac{n}{\left\lceil \frac{2^{n-1}-m}{2m+1} \right\rceil + m} \tag{15}$$

G-LSB-M 方法的隐写负载率恒定为 1,而式(15)给出的基于扩展加减覆盖集隐写方法的负载率通常小于 1(例如,当 $n=6$,$m=3$ 时,$\alpha=0.75$;当 $n=8$,$m=5$ 时,$\alpha=0.47$;当 $n=10$,$m=12$ 时,$\alpha=0.31$).在实际应用中,现代隐写方法多以较低的嵌入率进行嵌入以保证隐写的隐蔽性.基于扩展加减覆盖集的隐写方法虽然负载率低于 G-LSB-M 方法,但仍能满足隐写的实际需求.

使用扩展加减覆盖集的隐写方法解决了 G-LSB-M 方法构造加减覆盖集时依赖穷举搜索的问题,使得隐写者能够使用更大的信息分段长度 n 嵌入隐蔽信息,从而提高了隐写嵌入效率,增强了隐写的隐蔽性.为了验证这一点,本文从 BOSSBase v0.92 图库[12]中随机选取 1000 张 512×512 的位图格式图像作为原文样本集,分别使用本文提出的方法和 G-LSB-M 方法以 0.05bpp 的嵌入率嵌入隐蔽信息生成隐文样本集.本文使用差分像素邻接矩阵(Subtractive Pixel Adjacency Matrix,SPAM)特征[14]作为隐写分析特征,从已制备的 1000 对原文、隐文样本中随机选取 700 对进行训练构造隐写分析分类器,对其余的 300 对样本进行隐写分析.所得的隐写分析 ROC 曲线如图 1 所示.

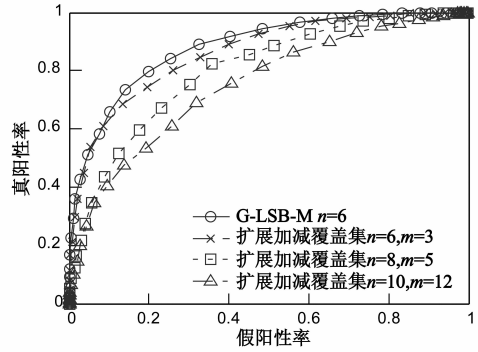


图1　不同编码方法的隐写分析ROC曲线

从图 1 所示的实验结果可以看出,随着 n 值的增加,本文提出的基于扩展加减覆盖集的隐写方法的隐蔽性逐渐提高,且在 $n>6$ 时其隐蔽性优于 G-LSB-M 方法.这是由于使用扩展加减覆盖集嵌入隐蔽信息时的平均修改次数随着 n 值的增加而降低,隐写过程对载体数据统计特征的扰动随之减小.

5　结论

本文提出了一种基于扩展加减覆盖集的隐写嵌入方法.该方法解决了 G-LSB-M 方法中使用穷举搜索构造加减覆盖集的困难,通过从基础加减覆盖集中去除非必需的元素,能够以较小的计算代价构造出扩展加减覆盖集.使用扩展加减覆盖集嵌入隐蔽信息时,隐写者能够使用更长的信息分段,从而降低了嵌入耗费时间,提高了嵌入效率和隐写的隐蔽性.

参考文献

[1] 钮心忻,杨义先.信息隐写与隐写分析研究框架探讨[J].电子学报,2006,34(z1):2421 – 2424.
NIU X,YANG Y.Study on the frame of information steganography and steganalysis[J].Acta Electronica Sinica,2006,34(21):2421 – 2424.(in Chinese)

[2] PROVOS N. Defending against statistical steganalysis[A]. Proceedings of the 10th USENIX Security Symposium[C]. Washington DC: USENIX, 2001. 323 – 336.

[3] Fridrich J, Goljan M, Hogea D. Steganalysis of JPEG images: Breaking the F5 algorithm[A]. Information Hiding, Lecture Notes in Computer Science[C]. Berlin Heidelberg: Springer, 2002. 310 – 323.

[4] Fridrich J. Feature-based steganalysis for JPEG images and its implications for future design of steganographic schemes[A]. Information Hiding, Lecture Notes in Computer Science[C]. Berlin Heidelberg: Springer, 2005. 67 – 81.

[5] Lyu S, Farid H. Detecting hidden messages using higher-order statistics and support vector machines[A]. Information Hiding, Lecture Notes in Computer Science[C]. Berlin Heidelberg: Springer, 2002. 340 – 354.

[6] Harmsen J J, Pearlman W A. Steganalysis of additive noise modelable information hiding[A]. Proceedings SPIE, Security, Steganography, and Watermarking of Multimedia Contents [C]. Santa Clara, CA: SPIE, 2003. 131 – 142.

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

[8] Petitcolas F A P, Anderson R J, Kuhn M G. Information hiding—A survey[J]. Proceedings of IEEE, 1999, 87(7): 1062 – 1078.

[9] SHARP T. An implementation of key-based digital signal steganography[A]. Information Hiding, Lecture Notes in Computer Science[C]. Berlin Heidelberg: Springer, 2001. 13 – 26.

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

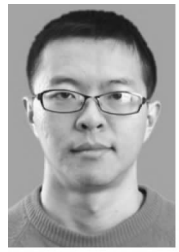
[11] Li X L, Yang B, Cheng D F, Zeng T Y. A generalization of lsb matching[J]. Signal Processing Letter, IEEE, 2009, 16 (2): 69 – 72.

[12] Bas P, Filler T, Pevny T. Break our steganographic system: The ins and outs of organizing BOSS[A]. Information Hiding, Lecture Notes in Computer Science[C]. Berlin Heidelberg: Springer, 2011. 59 – 70.

[13] Li X L, Zeng T Y, Yang B. Improvement of the embedding efficiency of LSB matching by sum and difference covering set[A]. Ostermann J. International Conference on Multimedia and Expro[C]. Hannover Germany: IEEE, 2008. 209 – 212.

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

作者简介



夏冰冰 男, 1983 年 1 月出生. 2013 年于中国科学院信息工程研究所获工学博士学位. 主要研究方向: 隐写码、隐写分析、数字水印等.
E-mail: capricorn-double@hotmail.com

赵险峰 男, 1969 年 6 月出生. 现为中国科学院信息工程研究所研究员、博士生导师, 中国电子学会通信学分会多媒体安全专家委员会委员. 主要研究方向: 隐写与隐写分析、数字水印、信息安全等.

王明生 男, 现为中国科学院信息工程研究所研究员、博士生导师. 主要研究方向: 计算代数、密码学、信息安全等.