基于稀疏表示的密写编码

张新鹏,王朔中
(上海大学通信与信息工程学院,上海 200072)

摘 要: 密写编码技术以占用较多的载体数据为代价来减少对载体数据的修改量,从而降低信息隐藏引起的失真.本文首先将密写编码方法的构造转化为一个数据的稀疏表示问题,然后提出密写编码构造算法.利用该构造算法可得到一系列密写编码方法,并进一步研究密写编码的组合形式,在不同占用率条件下获得了良好的编码性能,优于矩阵密写编码和游动密写编码.

关键词: 密写;编码;稀疏表示
中图分类号: TP309.7 **文献标识码:** A **文章编号:** 0372-2112 (2007) 10-1892-05

Steganographic Encoding Based on Sparse Representation

ZHANG Xin-peng, WANG Shuo-zhong
(*School of Communication and Information Engineering, Shanghai University, Shanghai* 200072, *China*)

Abstract: A data-hider can reduce the amount of alterations necessary to be introduced into a cover signal for data hiding by using stego-encoding techniques. In this paper, construction of the generalized stego-encoding technique is described in a form of sparse representation. With this representation, a series of stego-coding methods are obtained, among which the previously introduced matrix encoding may be viewed as a special case. It is then demonstrated that a suitable combination of different stego-encoding schemes can provide improved performance under a given ratio between the amount of host data and that of secret data, which is better than the performance of the matrix encoding and the running encoding schemes.

Key words: steganography; encoding; sparse representation

1 引言

作为信息安全的新兴领域,信息隐藏包括数字水印和数字密写(steganography)两个主要分支.数字水印用于保护多媒体作品的知识产权,主要技术难点是实现高度的鲁棒性,即抵御侵权者恶意攻击和常规信号处理的能力.而密写的基本目的是隐蔽通信,即以图像、音频等数字媒体为掩护,将秘密消息嵌入载体信号内进行传输.其关键是将"正在通信"这一事实隐蔽起来使之不为外界所知,因此隐蔽性是衡量密写技术优劣的最重要标准.

目前针对密写的主要对抗措施是密写分析(steganalysis),就是对多媒体信号进行统计特性检测,判断其中是否存在额外的秘密信息.迄今已出现了针对不同载体类型、不同密写算法的多种分析方法[1~3].为了抵御密写分析,有的密写方法在数据嵌入时尽可能保持原有的统计特性,还有一些方法是在密写后进行适当补偿,将统计特性恢复到原来的状态[3].一般说来,密写嵌入的内容越多,载体数据的统计特性的异常性就越明显,分析者也就越容易察觉秘密信息的存在.因此提高密写安全性的另一种有效途径是尽量减少对原始载体数据的改动.密写编码就属于这一类方法.

密写编码技术是在信息嵌入时以占用较多的载体数据为代价,换取对载体数据的较少改动,因此失真较小,统计特性的变化也不明显,使密写分析更加困难.例如,文献[4]将载体二值图像分成 $m \times n$ 的小块,在每个小块中最多改动2个象素值就可以嵌入 $\lfloor \log_2(mn+1) \rfloor$ 比特秘密数据.而矩阵编码可以在 2^l-1 个象素中最多改动1个象素的最不重要位(LSB)便可以嵌入 l 比特秘密信息,大大减少了对载体数据的改动[5].文献[6]研究了一类密写编码的性能,这类密写编码可由分组纠错编码逆向导出.而游动密写编码并不是基于分组形式的,而是将秘密信息和载体数据都作为比特流处理,每一秘密比特都由连续若干载体比特表示[7].最近,

收稿日期:2005-12-20;修回日期:2007-08-12
基金项目:国家自然科学基金(No.60502039);上海市科委基础研究重点项目(No.04JC14037);上海市青年科技启明星计划(No.06QA14022);上海市重点学科建设项目(No.T0102)

Fridrich 又基于 LT 码提出了另一种用于密写的湿纸(wet paper)编码[8,9],应用这种方法密写者可以自由选择嵌入位置,而接收者可以在不知晓嵌入位置的条件下提取秘密数据.

本文基于数据的稀疏表示提出一类新的密写编码方法.数据稀疏表示是一个较新的研究领域,在图像恢复、图像压缩、盲源分离等方面有广泛的应用[9,10].本文首先将密写编码方法的构造转化为数据稀疏表示问题,然后给出密写编码的构造算法,根据该算法可构造一族密写编码方法,并进一步研究不同占用率(密写所占用的载体数据量与秘密数据量之比)条件下密写编码方法的组合,由此获得的编码方案性能优于矩阵编码和游动密写编码的性能.

2　密写编码的稀疏表示模型

称载体数据中可用于承载秘密信息的数据空间为"可用空间",例如 LSB 密写中整个最低位平面即为可用空间.将要嵌入的秘密信息分成许多长度为 k 比特的段,密写编码就是以可用空间中的 n 比特来表示每一个秘密信息段($n>k$),将可用空间中的 n 比特记为 $\boldsymbol{v}=[v_1,v_2,\cdots,v_n]^{\mathrm{T}}$,被表示的秘密信息段为 $\boldsymbol{x}=[x_1,x_2,\cdots,x_k]^{\mathrm{T}}$.向量 $\boldsymbol{v}$ 共有 2^n 种可能,而秘密信息段 $\boldsymbol{x}$ 有 2^k 种可能,也就是说用 $\boldsymbol{v}$ 的多种状态表示某一种 $\boldsymbol{x}$,密写就是将 $\boldsymbol{v}$ 由原始状态改变为对应于秘密信息段 $\boldsymbol{x}$ 并与原始状态最接近的状态.这种 $\boldsymbol{v}$ 的多种状态与秘密信息段 $\boldsymbol{x}$ 的某一情况的对应关系即密写编码.与普通密写相比,秘密信息占用的空间变大了,而对原始数据的改动却减少了.因此,在可用空间大于秘密信息数据量的情况下,密写编码可以达到减小失真的目的.

记密写前 $\boldsymbol{v}$ 的原始状态为 $\boldsymbol{v}_o$,密写后为 $\boldsymbol{v}_s$,定义 $\boldsymbol{v}_s$ 与秘密信息段 $\boldsymbol{x}$ 的对应关系如下:

$$\boldsymbol{D}\cdot\boldsymbol{v}_s=\boldsymbol{x} \tag{1}$$

这里 $\boldsymbol{D}$ 是大小为 $k\times n$ 的二进制矩阵,运算符号"·"表示矩阵与向量的模 2 乘法.也就是说矩阵 $\boldsymbol{D}$ 规定了密写编码方法,本文的目的即构造 $\boldsymbol{D}$ 以获得好的密写编码性能.

记

$$\boldsymbol{v}_d=\boldsymbol{v}_s+\boldsymbol{v}_o \tag{2}$$

可见 $\boldsymbol{v}_d$ 中为 1 的元素表示密写对载体数据的修改.记

$$\boldsymbol{y}=\boldsymbol{x}+\boldsymbol{D}\cdot\boldsymbol{v}_o \tag{3}$$

若给定密写编码方法 $\boldsymbol{D}$、秘密信息段 $\boldsymbol{x}$ 和原始载体数据 $\boldsymbol{v}_o$,则向量 $\boldsymbol{y}$ 也已确定.由式(1),有

$$\boldsymbol{D}\cdot\boldsymbol{v}_d=\boldsymbol{y} \tag{4}$$

秘密信息在嵌入前通常经过加密,因此 $\boldsymbol{x}$ 可看作随机向量,$\boldsymbol{y}$ 也可同样地看作随机向量.因此,构造一个好的密写编码方法即找到一个矩阵 $\boldsymbol{D}$,使得对任意的 $\boldsymbol{y}$ 都有一个稀疏表示,即存在含有少量非零元素(即值为 1 的元素)的向量 $\boldsymbol{v}_d$ 满足式(4).编码过程即根据式(3)计算向量 $\boldsymbol{y}$,然后将 $\boldsymbol{y}$ 稀疏表示为 $\boldsymbol{v}_d$,根据 $\boldsymbol{v}_d$ 修改载体数据.解码时根据 $\boldsymbol{D}$ 和 $\boldsymbol{v}_s$ 按照式(1)求出秘密信息段 $\boldsymbol{x}$ 即可.

3　密写编码方法的构造

本节在给定参数 n、k 的情况下构造密写编码方法,即寻找矩阵 $\boldsymbol{D}$ 以及对向量 $\boldsymbol{y}$ 的稀疏表示方法.

如前所述,$\boldsymbol{D}$ 是由 n 个长度为 k 的二进制列向量组成的矩阵,对 $\boldsymbol{y}$ 的稀疏表示就是将 $\boldsymbol{y}$ 表示为尽量少的若干个 $\boldsymbol{D}$ 中列向量的和.长度为 k 的二元列向量共有 2^k 种,我们将通过如下步骤在其中挑选 n 个构成矩阵 $\boldsymbol{D}$:

步骤 1:将不全为 0 的长度为 k 的 2^k-1 种二元列向量全部列出,记为 $\boldsymbol{w}(1),\boldsymbol{w}(2),\cdots,\boldsymbol{w}(2^k-1)$,并用仅含有一个"1"元素的 k 个二元列向量构成集合 $\boldsymbol{S}_D$.

步骤 2:将每个二元列向量 $\boldsymbol{w}(i)$ 表示成 $d(i)$ 个 $\boldsymbol{S}_D$ 中向量的和,并将这 $d(i)$ 个向量构成集合 $\boldsymbol{S}(i)$,实际上 $d(i)$ 即 $\boldsymbol{w}(i)$ 中"1"元素的个数($i=1,2,\cdots,2^k-1$).

步骤 3:在所有 $d(i)$ 中找到一个最大值,设为 $d(m)$,若有多个 $d(i)$ 中达到最大值,任取其中一个作为 $d(m)$.

步骤 4:用 $\boldsymbol{w}(m)$ 与所有 $d(i)$ 为 1 的向量相加,不妨设 $\boldsymbol{w}(m)$ 与其中一个 $\boldsymbol{w}(i)$ 的和为 $\boldsymbol{w}(j)$,如果 $d(j)$ 大于 2,则将 $d(j)$ 值改为 2,并将 $\boldsymbol{S}(j)$ 改为 $\boldsymbol{S}(i)$ 与 $\{\boldsymbol{w}(m)\}$ 的并集;再用 $\boldsymbol{w}(m)$ 与所有 $d(i)$ 为 2 的向量相加,如果和向量 $\boldsymbol{w}(j)$ 对应的 $d(j)$ 大于 3,则将 $d(j)$ 值改为 3 并将 $\boldsymbol{S}(j)$ 改为 $\boldsymbol{S}(i)$ 与 $\{\boldsymbol{w}(m)\}$ 的并集;如此继续下去,直到用 $\boldsymbol{w}(m)$ 与所有 $d(i)$ 为 $d(m)-2$ 的向量相加,如果和向量 $\boldsymbol{w}(j)$ 对应的 $d(j)$ 大于 $d(m)-1$,则将其 $d(i)$ 值改为 $d(m)-1$ 并将 $\boldsymbol{S}(j)$ 改为 $\boldsymbol{S}(i)$ 与 $\{\boldsymbol{w}(m)\}$ 的并集.

步骤 5:将 $\boldsymbol{w}(m)$ 加入集合 $\boldsymbol{S}_D$,并将 $d(m)$ 改为 1.

步骤 6:如果 $\boldsymbol{S}_D$ 中包含的向量少于 n 个,则回到步骤 3;否则结束,用集合 $\boldsymbol{S}_D$ 中的 n 个向量(它们对应的 $d(i)$ 都为 1)构成矩阵 $\boldsymbol{D}$.

上述算法中,步骤 1、2 的作用是初始化,先将 k 个线性无关的列向量置于 $\boldsymbol{S}_D$ 中,并将 $\boldsymbol{y}$ 的所有状态表示为 $\boldsymbol{S}_D$ 中向量的和.步骤 3 是寻找 $\boldsymbol{y}$ 的所有状态中稀疏性最差的状态,步骤 5 则将这个状态作为一个向量置于 $\boldsymbol{S}_D$ 中,从步骤 3 到步骤 5 循环一次 $\boldsymbol{S}_D$ 中向量的个数就增加 1,而步骤 4 是更新 $d(j)$ 和 $\boldsymbol{S}(j)$ 以适应新的 $\boldsymbol{S}_D$,即将 $\boldsymbol{w}(j)$ 表示为新的 $\boldsymbol{S}_D$ 中列向量的和.当上述算法结束时,$\boldsymbol{S}_D$ 即矩阵 $\boldsymbol{D}$ 诸列的集合.

表 1 给出了 $n=6$、$k=4$ 时密写编码的构造过程.

初始时 S_D 中只包含前 4 个向量 $w(1)$、$w(2)$、$w(3)$、$w(4)$,而最大的 $d(i)$是 $d(15)=4$.第一次循环时将 $w(15)$加入 S_D,并更新 $d(15)$为 1、$S(15)$为{$w(15)$};此时 $w(11)\sim w(14)$的稀疏表示方法也会因 S_D 的更新而变化,即可表示成 S_D 中 2 个向量的和,因此 $d(11)\sim d(14)$、$S(11)\sim S(14)$也得到更新.第二次循环时将 $w(5)$加入 S_D,并更新 $d(5)$、$S(5)$.最后得到矩阵

$$\boldsymbol{D}=\begin{bmatrix}0&0&0&1&0&1\\0&0&1&0&0&1\\0&1&0&0&1&1\\1&0&0&0&1&1\end{bmatrix} \tag{5}$$

例如 $v_o=[001101]$、秘密信息段 $x=[1101]$,根据式(3)求出 $y=[1110]^{\mathrm{T}}$,从表 1 中可以看出 y 可表示成 $w(1)$与 $w(15)$的和,$w(1)$与 $w(15)$分别是 D 的第一列和第六列,因此 $v_d=[100001]$,即将 v_o 改为 $v_s=[101100]$.

表 1 (6,4)密写编码的构造过程

列向量 $w(i)$	初始状态		第一次循环		第二次循环	
	$d(i)$	$S(i)$	$d(i)$	$S(i)$	$d(i)$	$S(i)$
$w(1)=[0001]^{\mathrm{T}}$	1	$w(1)$	1	$w(1)$	1	$w(1)$
$w(2)=[0010]^{\mathrm{T}}$	1	$w(2)$	1	$w(2)$	1	$w(2)$
$w(3)=[0100]^{\mathrm{T}}$	1	$w(3)$	1	$w(3)$	1	$w(3)$
$w(4)=[1000]^{\mathrm{T}}$	1	$w(4)$	1	$w(4)$	1	$w(4)$
$w(5)=[0011]^{\mathrm{T}}$	2	$w(1)w(2)$	2	$w(1)w(2)$	1	$w(5)$
$w(6)=[0101]^{\mathrm{T}}$	2	$w(1)w(3)$	2	$w(1)w(3)$	2	$w(1)w(3)$
…	…	…	…	…	…	…
$w(14)=[1110]^{\mathrm{T}}$	3	$w(2)w(3)$ $w(4)$	2	$w(1)$ $w(15)$	2	$w(1)$ $w(15)$
$w(15)=[1111]^{\mathrm{T}}$	4	$w(1)\sim w(4)$	1	$w(15)$	1	$w(15)$

我们引入占用率、更改率两个参数用于描述密写编码的性能.占用率为每嵌入 1 比特秘密信息所消耗的载体可用空间大小,也就是载体数据量与嵌入数据量的比值,即

$$R_C=n/k \tag{6}$$

如果固定载体信号,嵌入量(率)越大,则占用率越小,反之亦然.更改率则为每嵌入 1 比特秘密信息引起的可用空间比特改动的平均个数.可以认为 y 的 2^k 种情况等概率出现,而每一种情况所需的比特改动数即其对应的 $d(i)$值(如果 y 是全"0"向量,则不需任何改动),因此,更改率

$$R_A=\frac{1}{2^k k}\sum_{i=1}^{2^k-1}d(i) \tag{7}$$

如果 $n=k$,那么 D 只有 k 列,并且各列仅含有一个"1"元素,相当于没有进行编码的普通密写,占用率为 1、更改率为 0.5.如果固定 k、逐渐增大 n,那么占用率会相应地增大、而更改率减小.可见密写编码是以牺牲占用率为代价,换取小的更改率.当 $n=2^k-1$ 时,D 中包含了所有不全为 0 的长度为 k 的列向量,$d(i)$都为 1,也就是说如果 v_o 恰好对应秘密信息段 x 则不用任何改动,否则仅改动 1 比特即可,事实上这就是矩阵编码[5].而如果 $n>2^k-1$,D 中必有重复的列向量,这样一来增大占用率并不继续使更改率减小,因此我们不考虑这种情况.经计算,用本节算法构造的部分密写编码的性能如表 2 所示.

表 2 部分密写编码性能

k	n	占用率 R_C	更改率 R_A
1	1	1.00	0.50
2	3	1.50	0.38
3	4	1.33	0.42
3	5	1.67	0.38
3	6	2.00	0.33
3	7	2.33	0.29
4	5	1.25	0.39
4	6	1.50	0.38
4	7	1.75	0.36
4	8	2.00	0.34
4	9	2.25	0.33

4 不同占用率条件下的密写编码组合

在载体数据可用空间明显大于秘密信息量的情况下,应用密写编码可以显著减少对载体数据的修改量.实际应用中往往给定载体数据的可用空间和秘密信息量(即给定占用率),需要构造更改率最小的密写编码方法.一个简单做法就是在众多可能方案中选择占用率不大于给定占用率并具有最小更改率的(n,k)密写编码方法.而实际上我们可以利用密写编码组合方法得到更好的性能.

考虑两种密写编码方法(n_1,k_1)、(n_2,k_2),设其占用率和更改率分别为 R_C^1、R_A^1 和 R_C^2、R_A^2.如果一部分秘密信息以第一种密写编码方法嵌入,另一部分以第二种密写编码方法嵌入,易知总的占用率和更改率如下:

$$R_C=\alpha\cdot R_C^1+(1-\alpha)\cdot R_C^2 \tag{8}$$

$$R_A=\alpha\cdot R_A^1+(1-\alpha)\cdot R_A^2 \tag{9}$$

这里 α 是两部分秘密信息划分的比例$(0\leqslant\alpha\leqslant1)$.如果将$(R_C^1,R_A^1)$和$(R_C^2,R_A^2)$看作二维空间中的两个点,那么组合后的$(R_C,R_A)$必然落在两点间的线段上.考虑将多种密写编码方法进行组合,设其性能为(R_C^1,R_A^1),(R_C^2,R_A^2),…,(R_C^t,R_A^t),并分别用于嵌入比例为 α_i 的秘密信息$(\alpha_1+\alpha_2+\cdots+\alpha_t=1)$,易知组合后的总占用率和总更改率实际就是多种密写编码方法性能的线性组合:

$$R_C=\sum_{i=1}^{t}\alpha_i\cdot R_C^i,\quad R_A=\sum_{i=1}^{t}\alpha_i\cdot R_A^i \tag{10}$$

为得到最佳的组合密写编码方法,我们先绘出所有密写编码方法性能对应的点,然后将其中的一部分点连接起来构成一条分段线性的下凸折线,使其它密写编

码方法性能对应的点及两点间连线都位于这条折线上方.那么,所有可能的组合密写编码方法性能也必然位于这条分段折线的上方.也就是说,这条折线就表示了通过组合编码方法可以获得的最佳性能.

图 1 给出了占用率在[1,3]之间 $k\leqslant 7$ 的所有密写编码方法的性能(圆圈表示),顺次连接密写编码方法(1,1)、(8,7)、(7,6)、(11,7)、(12,7)、(7,3)、(15,4)构成一条下凸折线,使得其它密写编码方法或组合密写编码方法的性能都在它上方,也就是说利用这些密写编码方法进行组合得到的性能一定不会优于这条折线.若给定占用率 2.10,将 38% 的秘密信息用密写编码方法(12,7)嵌入、62% 的秘密信息用密写编码方法(7,3)嵌入,可获得最小的更改率 0.305(星号标出).如果不采用密写编码组合方法,最佳密写编码方法为(14,7),更改率为 0.315,劣于组合方法.需要注意的是图 1 仅考虑了 $k\leqslant 7$ 的密写编码方法,如果 k 的范围更大,可以获得更好的密写编码性能.

图 1 中还给出了矩阵编码和游动编码的性能,分别用"+"和"×"表示并用虚线连接.由于矩阵编码是本文所述稀疏表示密写编码的特例,所以图中"×"与"○"重合,并且连接"×"的虚线有一段与实线重合.两条虚线都在实线上方,可见稀疏表示密写编码优于矩阵编码和游动编码.

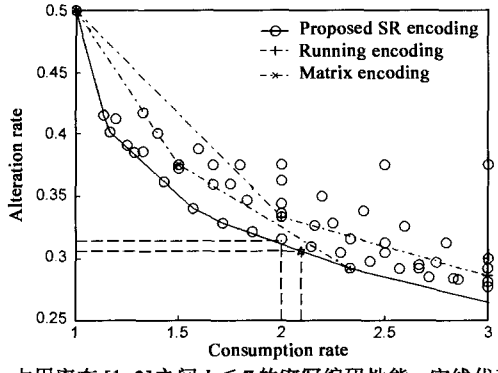

图 1　占用率在 [1, 3]之间 $k\leqslant 7$ 的密写编码性能.实线代表组合编码可获得的最佳性能.当占用率为 2.10 时,组合方法获得的最小更改率为 0.305,优于非组合方法的最小更改率 0.315.两条虚线分别代表矩阵编码和游动编码的性能,劣于本文方法性能

当应用最不重要位(LSB)替换技术隐藏秘密信息时,如果不采用密写编码方法且秘密信息量是载体图像像素数的 1/4 时(即平均有 1/8 的像素被改变),应用文献[2]中的密写分析方法可以比较准确地察觉秘密信息的存在(利用 500 幅原始图像和 500 幅含密图像进行实验,准确检测率为 83.2%,虚警率为 7.6%).而应用本文的密写编码方法进行嵌入,可以取占用率为 4,此时仅用 5.9% 的像素被改变,同样的密写分析方法在相同虚警率条件下准确检测率仅有 61.4%.可见密写编码方法可以显著降低密写分析的准确检测率,大大提高密写安全性.

5　结论与讨论

本文根据数据稀疏表示模型提出了密写编码的一种构造算法,根据此算法可以构造一系列不同的密写编码方法,通过消耗较多的载体数据减少信息隐藏引起的失真.本文进一步研究了密写编码的组合形式,可以在不同占用率条件下获得更好的性能.

经过密写编码嵌入的秘密信息对干扰更加敏感,轻微改动含密载体数据可能对秘密信息的提取造成很大影响.事实上密写通常应用于无噪传输环境,例如在互联网传输数字图像或音频载体,而且如果一旦接收者无法提取干扰后的秘密信息,还可以一定的方式通知发送者重新进行隐蔽通信.所以密写编码在增加密写安全性的同时,并不会给密写应用带来较大的局限.

本文提出的密写编码方法仅仅规定了秘密信息的表示方法,并未涉及可用空间的选取和具体数据修改方法,所以密写编码可以与多种密写方法结合.尽管应用密写编码可减少数据修改量,有助于抵御密写分析,但安全性不能仅靠密写编码来保障.例如,将密写编码与 LSB 替换技术结合可以大大降低 LSB 翻转个数,但许多敏感的密写分析方法仍然可以察觉密写行为.而如果将密写编码与 LSB 匹配技术(对象素灰度随机加 1 或减 1 的办法修改 LSB)结合起来,安全性会大大提高,因为当前的密写分析仅可通过灰度直方图异常觉察嵌入率很高的 LSB 匹配密写[12].为消除潜在的危险,可以将密写编码与更安全的嵌入技术[13]结合,在这里,象素灰度以一定的概率加 1 或减 1 以保证载体数据的直方图不发生变化.

参考文献:

[1] H Wang, S Wang. Cyber warfare—steganography vs. teganalysis[J]. Communication of the ACM, 2004, 47(10): 76 - 82.

[2] J Fridrich, M Goljan. Practical steganalysis of digital images—state of the art[A]. In Proc. Security and Watermarking of Multimedia Contents IV[C]. Proceedings of SPIE 4675, USA: SPIE, 2002. 1 - 13.

[3] 王朔中,张新鹏,张开文.数字密写与密写分析—互联网时代的信息战技术[D].北京:清华大学出版社,2005 年 4 月.

[4] Y Tseng, Y Chen, H Pan. A secure data hiding scheme for binary images[J]. IEEE Trans Communications, 2002, 50(8): 1227 - 1231.

[5] A Westfeld. F5—a steganographic algorithm[A]. In Proc. 4th International Workshop on Information Hiding[C]. Lecture Notes in Computer Science 2137, Berlin: Springer-Verlag,

2001.289 - 302.

[6] F Willems, M Dijk. Capacity and codes for embedding information in grayscale images[J]. IEEE Trans Information Theory, 2005, 51(3): 1209 - 1214.

[7] X Zhang, S Wang. Dynamical running coding in digital steganography[J]. IEEE Signal Processing Letters, 2006, 13(3): 165 - 168.

[8] J Fridrich, M Goljan, P Lisoněk, D Soukal. Writing on wet paper[A]. In Proc. Security, Steganography, and Watermarking of Multimedia Contents VII[C]. Proceedings of SPIE 5681, USA: SPIE, 2005. 328 - 340.

[9] M Luby. LT codes[A]. In Proc. The 43rd Annual IEEE Symposium on Foundations of Computer Science[C]. USA: IEEE press, 2002. 271 - 282.

[10] M M Bronstein, A M Bronstein, M Zibulevsky, Y Y Zeevi. Blind deconvolution of images using optimal sparse representations[J]. IEEE Trans Image Processing, 2005, 14(6): 726 - 736.

[11] P Bofill, M Zibulevsky. Underdetermined blind source separation using sparse representations[J]. Signal Processing, 2001, 81(11): 2353 - 2362.

[12] A D Ker. Steganalysis of LSB matching in grayscale images[J]. IEEE Signal Processing Letters, 2005, 12(6): 441 - 444.

[13] X Zhang, S Wang, K Zhang. Steganography with least histogram abnormality[A]. In Proc. Second International Workshop on Mathematical Methods, Models, and Architectures for Computer Network Security[C]. Lecture Notes in Computer Science 2776, Berlin: Springer-Verlag, 2003. 395 - 406.

作者简介:

张新鹏 男, 1975 年 9 月出生于黑龙江密山, 2004 年毕业于上海大学通信与信息工程学院, 获工学博士学位, 现为上海大学通信与信息工程学院副教授. 主要从事多媒体信息安全、隐写与反隐写、数字水印、图像处理等方面的研究, 已发表论文八十余篇.

E-mail: xzhang@staff.shu.edu.cn

王朔中 男, 1943 年 9 月生于重庆, 1966 年毕业于北京大学, 1982 年获英国伯明翰大学博士学位, 现任上海大学通信与信息工程学院教授、博士生导师. 研究领域: 图像处理, 音频信号处理, 信息隐藏. E-mail: shuowang@shu.edu.cn