

基于直方图修改的图像密文域可逆信息隐藏

郑淑丽, 李丹丹, 胡东辉, 张云玲

(合肥工业大学 计算机与信息学院, 安徽 合肥 230009)

摘 要: 提出了基于块平滑度排序和直方图修改的图像密文域可逆信息隐藏算法. 首先对图像进行分块, 块平滑度排序以及对每块进行置乱加密; 然后依据直方图修改的规则在密文块中隐藏秘密信息; 最后既可以先进行图像解密再提取信息, 也可以先提取信息再进行图像解密. 实验仿真结果表明, 此算法不仅实现了信息提取和图像解密完全分离, 且与现有算法相比, 在实现零误差高隐藏容量的同时进一步提高了非满载情况下的图像质量.

关键词: 块平滑度排序; 直方图修改; 图像密文域; 可逆信息隐藏

中图分类号: TP309

文献标识码: A

文章编号: 1000-7180(2015)12-0105-05

Reversible Data Hiding in Encrypted Images by Histogram Modification

ZHENG Shu-li, LI Dan-dan, HU Dong-hui, ZHANG Yun-ling

(School of Computer and Information, Hefei University of Technology, Hefei 230009, China)

Abstract: A novel reversible data hiding in encrypted domain is proposed based on block sorting and histogram modification. The first work divides image into blocks and blocks sorting, and each block is permuted by scrambling encryption. Then, the histogram of each block is modified to vacate room for secret data. Finally, the receiver can decrypt firstly and then extract data, the inverse process is also viable. Experiments show that the operator of data extraction and image decryption is completely separable in the proposed method, and compared with the existing methods, the proposed method has improved embedding capacity while maintaining zero error rate, and has better image quality while under-capacity.

Key words: block sorting; histogram modification; encrypted images; reversible data hiding

1 引言

加密算法被广泛用于保证用户数据的安全性和隐私性. 加密算法的应用也对图像隐写带来了新的挑战: 图像加密后丧失了原有的数据结构特征, 导致绝大多数非密文域可逆信息隐藏算法^[1]失效. 因此, 在图像密文域中进行可逆信息隐藏成为云环境下面向隐私保护的图像信息隐藏的关键问题之一.

文献^[2]中提出, 将原始图像用流密码进行异或加密后分块, 通过对部分加密像素的 3 个最低有效位取反来嵌入信息, 并且利用自然图像的相关性实现信息提取和图像恢复. 但是, 该方案隐藏容量有

限, 并且当隐藏容量增加时会出现数据提取和图像恢复误差. 文献^[3]在文献^[2]的基础上进行了改进, 通过边缘匹配技术和改进的波动度量函数进一步提高了最大隐藏容量并降低了信息提取的错误率.

文献^[4]中采用低密度奇偶校验矩阵压缩密文图像的最低有效位来创建空余空间进行信息隐藏, 实现了信息提取和图像解密的可分离. 然而, 该方案隐藏容量有限. 由于在密文图像中进行无损创建空余空间比较困难且效率低, 文献^[5]中提出了一个新的密文域可逆信息隐藏方案: 在加密之前创建空余空间, 保证在较高的隐写质量条件下信息隐藏容量得到了有效地提高, 但该方案计算复杂度高. 文献

收稿日期: 2015-02-02; 修回日期: 2015-03-26

基金项目: 国家自然科学基金(61272540)

[6]中采用流密码加密产生密文图像,选取一类像素的第4个最低有效位,并用奇偶校验矩阵无损压缩后与待隐藏的信息一起嵌入到此类像素的第4个最低有效位,但信息隐藏容量和图像质量均欠佳.

本文结合直方图修改的思想提出了基于块平滑度排序及直方图修改的图像密文域可逆信息隐藏方法.

2 本文算法

本文算法的流程图如图1所示.

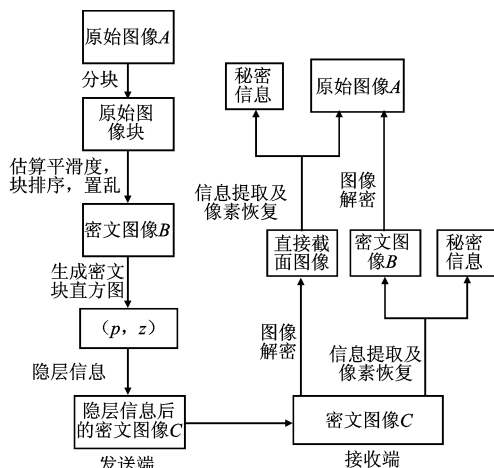


图1 本文算法的总框架

2.1 发送端

2.1.1 图像预处理

数字图像的相邻像素之间往往具有较强的相似性,也称为平滑度.根据基于直方图修改隐藏信息的规则,隐藏容量与直方图峰值点像素的个数成正比,也就是说,直方图变化幅度越大,隐藏容量越大.因此,为了保证较高的图像质量,在信息隐藏之前,需要对图像块进行平滑度排序.

图像块在加密前后直方图保存不变的特性是本文利用直方图修改隐藏信息所需要的,因此要保证图像像素值未发生变化.其中,置乱加密^[10]主要是通过改变像素点的位置将原本清晰的图像变得杂乱无章失去原来的面目,以达到加密图像的目的,但像素自身取值不发生变化.

假设原始图像A大小为 $M \times N$,其预处理的具体实现过程如下所示.

步骤1 块划分:将A均匀划分成 n 个互不重叠的图像块,每个图像块有 $m \times m$ 个像素组成.

步骤2 根据式(1)计算每个图像块的波动度量函数值 d 来估算每个图像块的平滑度,显然, d 越

小,图像越平滑,直方图越集中,越有利于用直方图修改的方法进行可逆信息隐藏.因此,按照平滑块优先选择的原则将图像块依据 d 的值进行由低到高的排序.其中, $b(i, j)$ 为像素值, $2 \leq i, j \leq m-2$.

$$d =$$

$$\left| b(i, j) - \frac{b(i-1, j) + b(i+1, j) + b(i, j-1) + b(i, j+1)}{4} \right| \quad (1)$$

获得已排序的图像块序列:

$$A = \{A_1, A_2, \dots, A_n\}.$$

步骤3 依次对A中的图像块进行置乱加密,得到密文块序列 $B = \{B_1, B_2, \dots, B_n\}$.为了得到更好的加密效果,可以进行多次置乱,并且置乱次数可以作为加密密钥.

2.1.2 密文域中信息隐藏过程

为了提高隐藏容量,本文算法依次在 $B_t (1 \leq t \leq n)$ 生成的直方图中选取三对峰值点和零值点,在保证每个零值点和峰值点对互不重叠的条件下,在峰值点中隐藏信息.

隐藏容量的高低是由峰值点个数决定的,每个峰值点可以隐藏1位信息.隐藏信息后,图像质量是可以保证的,因为核心理念是对像素值进行 ± 1 操作,只是稍微改变像素值,因而可以具有很好的图像质量.基于直方图修改的可逆信息隐藏算法的实现步骤如下所示.

步骤1 选取直方图中的峰值点:生成每个密文块对应的直方图 $H(b)$,选取直方图中三个最大值点 $H(p_1)$, $H(p_2)$ 和 $H(p_3)$,记录其对应的像素值为 p_1 , p_2 和 p_3 ,满足 $0 < p_1 < p_2 < p_3 < 255$,如图2(a)所示,选取三个峰值点有10, 15和20.

步骤2 分别在 $(0, p_1)$ 和 $(p_3, 255)$ 区间内选择两个最小值点 $H(z_1)$ 和 $H(z_6)$,其对应的像素值记为 z_1 和 z_6 , $0 \leq z_1 < p_1$, $p_3 < z_6 \leq 255$.

步骤3 在 (p_1, p_2) 区间范围内选取两个最小值点 $H(z_2)$ 和 $H(z_3)$.在 (p_2, p_3) 区间范围内选取两个最小值点 $H(z_4)$ 和 $H(z_5)$.

步骤4 分别比较 $H(z_1)$ 和 $H(z_2)$, $H(z_3)$ 和 $H(z_4)$, $H(z_5)$ 和 $H(z_6)$ 的大小,若 $H(z_1)$, $H(z_4)$ 和 $H(z_6)$ 为该组中较小的一个.则 (p_1, z_1) , (p_2, z_4) 和 (p_3, z_6) 为所选取的峰值点和零值点对.图2(a)所示,峰值点和零值点:(10, 3), (15, 17)和(20, 23).

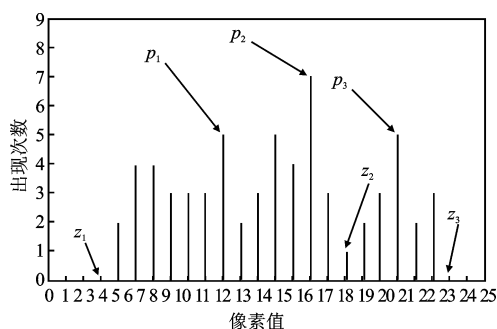
步骤5 信息隐藏:依次扫描 B_t 中预处理后的像素,根据下面的式(2)和式(3)修改 b 为 b' 以隐藏二进制秘密信息 s .图2(b)表示隐藏信息后的密文

块直方图.

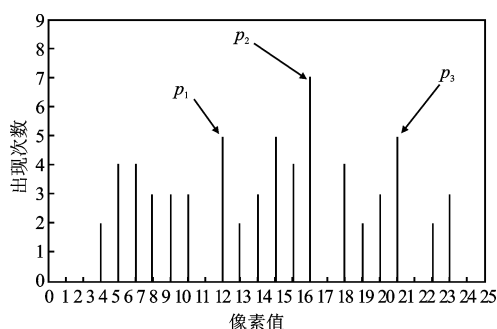
$$b' = \begin{cases} p, & s = 0 \& b = p \\ p + d, & s = 1 \& b = p \\ b + d, & (p < b < z) \parallel (p > b > z) \\ b, & \text{other} \end{cases} \quad (2)$$

$$d = \begin{cases} +1, & z > p \\ -1, & z < p \end{cases} \quad (3)$$

步骤 6 重复以上操作,直至将所有的秘密信息隐藏到图像中,最终得到含秘密信息的密文图像 C. 输出图像 C 和辅助信息,其中辅助信息包含 (p, z) 和块平滑度顺序.



(a) 信息隐藏前



(b) 信息隐藏后

图 2 块直方图示例图

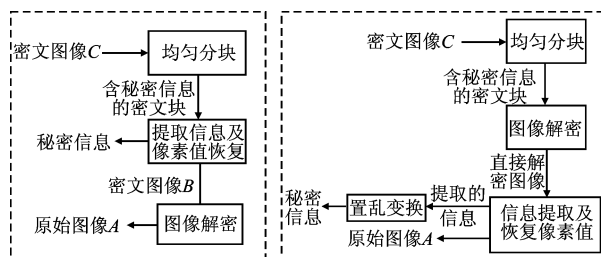
2.2 接收端

2.2.1 接收端的操作顺序分析

接收端的图像解密和信息提取过程顺序满足灵活性,即接收端既可以完成图 3(a)所示的操作,也可以完成图 3(b)所示的操作.也就是说,当接收者拥有解密密钥和数据提取密钥时,其可以进行先提取信息再图像解密,同样也可以先图像解密再提取信息.这个特性在文献[4-6]中是不具备的.

2.2.2 解密、信息提取和原始图像恢复

解密:输入接收到的图像和辅助信息,首先对图像进行均匀分块,再利用解密密钥和置乱变换依次对每个图像块中像素的位置进行置乱,获得直接解



(a) 先提取信息再解密

(b) 先解密再提取信息

图 3 收端两种不同的操作

密图像,其与原始图像在内容上大体一致.

信息提取及图像恢复:对接收到的图像块进行置乱解密后,像素值并未发生任何变化,即图像块的直方图保持不变.信息提取和原始图像恢复是同时进行的.图 3 所示的两种情况下,信息的提取过程基本相同,唯一不同的是:图 3(b)是在直接解密图像中提取信息,解密后信息的位置发生了变化,因此需要利用置乱变换进行位置变换,得到所隐藏的原始信息.信息提取的同时对像素值进行恢复,即可得到原始图像 A. 具体的实现步骤如下所示.

步骤 1 信息提取:根据块平滑度顺序以及峰值点和零值点对,逐个扫描图像块中的像素,根据式(4)提取所隐藏的信息.

$$s = \begin{cases} 0, & b' = p \\ 1, & b' = p + d \end{cases} \quad (4)$$

步骤 2 图像恢复:信息提取的同时根据式(5)修改 b' 为 b 得到无损恢复的图像.

$$b = \begin{cases} p, & b' = p + d \\ b' - d, & (p + d > b' > z) \parallel (z > b' > p + d) \\ b', & \text{other} \end{cases} \quad (5)$$

2.3 溢出问题

在灰度图像中,像素值存在两种边界情况,即像素值为 0 或 255. 为了避免边界值像素在信息隐藏过程中出现上溢和下溢的问题,那么在信息隐藏之前要对边界值像素进行预处理.预处理的方法主要是通过通过对边界值像素点加上或减去 1 并建立标记位进行标注.在发送端,依次扫描密文块中的像素,当像素值为 0 或 255 时,此时将像素值相应地变为 1 或 254,且标记位记为 0;当像素值为 1 或 254 时,此时像素值不发生任何变化,且标记位记为 1.

在接收端,为了无损恢复出原始图像,需要还原边界像素值.当标记位为 1,且像素值为 1 或 254 时,则表明像素值未发生变化.当标记位为 0,且像素值为 254 时,则表明原来的像素值为 255. 当标记

位为 0,且像素值为 1 时,则表明原来的像素值为 0.

这些标记信息的大小是由像素值 0、1、254、255 出现的次数决定的,即这些像素出现次数的总和,以比特为单位. 位这些标记信息可以作为辅助信息发送给接收者,或者作为待隐藏信息的一部分嵌入到图像中去,但后者在一定程度上降低了实际的隐藏容量.

3 实验及分析

为了验证本文算法的性能,选取图像库中大小为 $512 \times 512 \times 8$ 比特的灰度图像进行试验,包括 Lena、Baboon、Man、Barbara、Boats、Lake、Plane、Pepper. 其中,PSNR-rec 表示恢复图像与原始图像间的峰值信噪比,PSNR 表示直接解密图像与原始图像的峰值信噪比.

在本文方案中,采取在每块中选取多点对进行信息隐藏来提高隐藏容量. 以 $512 \times 512 \times 8$ 的灰度图像为例,表 1 所示为每块选取三个点对进行一次隐藏情况,分块前后隐藏容量的对比. 图像的相邻像素之间存在很强的相关性,分块后既可以有效提高隐藏容量,同时零值点个数也有明显增加,极大地方便了信息隐藏时峰值点和零值点的选取.

表 1 分块前后隐藏容量对比 bit

图像	分块前	分块后
Lena	2966	5833
Baboon	8157	10406
Man	2725	4088
Boats	5270	6856
Lake	1368	1680

表 3 本文算法与文献[2]、[3]、[4]的 capacity 和 PSNR

图像	本文方案		文献[4]方案		文献[5]方案		文献[6]方案	
	Capacity/bit	PSNR/dB	Capacity/bit	PSNR/dB	Capacity/bit	PSNR/dB	Capacity/bit	PSNR/dB
Lena	49140	48.02	1024	37.95	1298	38.06	8960	37.96
Baboon	13105	48.92	256	37.92	324	38.35	4354	31.86
Man	47562	47.96	986	38.25	1024	38.30	8900	38.05
Barbara	11297	49.01	252	37.92	334	38.42	4340	32.02
Boats	59846	49.31	1024	38.05	1024	37.95	8957	31.96
Lake	19023	47.89	326	38.19	386	38.92	4608	31.92
Plane	48650	48.05	1024	37.94	1296	38.08	8956	37.96
Pepper	46641	49.02	1296	38.02	1296	38.05	8956	31.85

图 4 的两幅图像所示为 Lena 图像利用本文算法在不同的块大小下隐藏容量和 PSNR 的变化情况. 从图 4(a)的曲线图可以看出,当 m 在 2 到 4 之间时隐藏容量较高,这是因为当块越大时,密文块个

在块大小相同的情况下,本文方案与文献[2]和文献[3]中的方案进行了比较. 以 Lena 图像为例,实验结果由表 2 中可以看出,在原始图像可以无损恢复的前提下,本文方案将文献[2]、文献[3]方案中的 1023 bit 提高到了 26470 bit. 这主要是在每个密文块中选取多个峰值点进行修改来隐藏信息,使得隐藏容量得到提高.

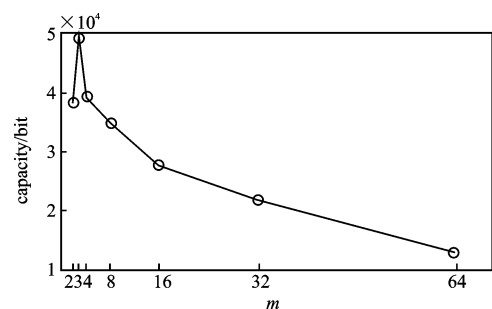
表 2 块大小相同时不同方案的隐藏容量、图像质量、错误率

块大小	方案	Capacity/bit	PSNR-rec/dB	错误率/%
4×4	文献[2]	16380	43.50	15.04
	文献[3]	16380	51.91	4.84
	本文方案	39264	$+\infty$	0
8×8	文献[2]	4095	57.90	1.03
	文献[3]	4095	59.02	0.45
	本文方案	34410	$+\infty$	0
16×16	文献[2]	1023	$+\infty$	0
	文献[3]	1023	$+\infty$	0
	本文方案	26470	$+\infty$	0

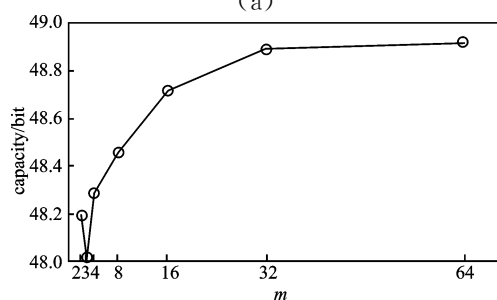
从表 3 可以看出,在隐藏容量方面,本文方案均高于文献[2]、文献[3]和文献[4]中的方案. 主要是因为图像的相邻像素具有很强的相关性,图像块置乱加密前后直方图保持不变的特性,本文方案在每块中选取多个峰值点用于隐藏信息. 由于在信息隐藏过程中优先选取平滑度较高的块来操作,所以在非满载的情况下,本文方案的 PSNR 比文献[3]、文献[4]和文献[6]都高,都不小于 48.02 dB,保证了较高的图像质量.

数变少,峰值点和零值点对的个数变少,以致于隐藏容量变少. 但在 m 为 2 时隐藏容量变小是因为块很小,同样也会造成峰值点和零值点对的个数减少. 从图 4(b)中的曲线可以看出,随着块大小的增大,直

接解密图像与原始图像之间的 PSNR 成上升趋势. 当 m 由 2 增加到 3 时, PSNR 下降. 因此, 在保证较好的图像质量条件下, 若想获得较高的隐藏容量, 密文块大小可以设置为 3×3 .



(a)

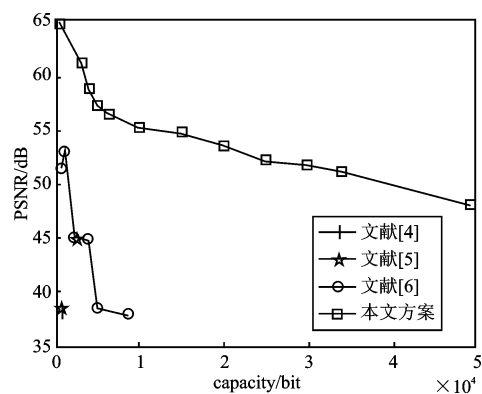


(b)

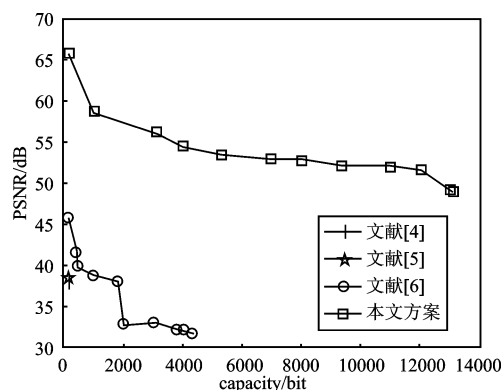
图4 m 与 capacity、PSNR 之间的关系

图 5 的两幅图分别为图像 Lena、Baboon 利用本文算法、文献[2]、文献[3]和文献[4]在不同隐藏容量下 PSNR 的对比图. 其中图中曲线是在原始图像可以零误差恢复的前提下选取最佳 m 值得到的. 从图中可以看出, 本文提出的方案明显提高了隐藏容量, 其 PSNR 值均高于 48.02 dB, 保证了高图像质量. 在相同的隐藏容量下, 本文方法的 PSNR 高于文献[2]、文献[3]和文献[4]中的方案; 而在 PSNR 值一定情况下, 隐藏容量得到提高. 同时, 本文方案产生的辅助信息较少. 因此可以证明本文方法不仅在隐藏容量还是在 PSNR 方面都具有良好的优越性.

由图 5 可以看出, 本文方案在平滑的 Lena 图像上的实验结果优于 Baboon 图像. 主要原因是平滑度越高的图像越适合利用基于直方图修改的可逆信息隐藏方法, 并且采取的块平滑度排序策略使得平滑度越高的图像块优先使用. 因此, 相较于复杂图像, 平滑图像在隐藏容量上具有优势, 也就是说, Lena 的最大隐藏容量大于 baboon 的. 在非满载情况下, 当待隐藏的信息容量相等时, 在 Lena 中只需更少的密文块即可隐藏完成, 因此带来的失真小, 即 PSNR 值高.



(a) Lena



(b) Baboon

图5 不同方法的 capacity-PSNR 曲线比较

4 结束语

本文提出了基于块平滑度排序和直方图修改的图像密文域可逆信息隐藏方案, 针对现有文献存在的不足, 提出了 3 种策略. 实验证明, 提出的块平滑度排序、选取多对峰值点和零值点以及修改峰值点像素值都很好利用了图像相邻像素之间的相关性, 在保证高图像质量的前提下, 很好地提高了隐藏容量. 同时, 块平滑度排序策略的使用, 使得本文方案在非满载荷的应用中具有很好的竞争力.

参考文献:

- [1] Tian J. Reversible data embedding using a difference experience[J]. IEEE Transactions on Circuits and Systems for Video Technology, 2003, 13(8): 890-896.
- [2] Zhang X. Reversible data hiding in encrypted image [J]. IEEE Signal Processing Letters, 2011, 18(4): 255-258.
- [3] Hong W, Chen T S, Wu H Y. An improved reversible data hiding in encrypted images using side match[J]. IEEE Signal Processing Letters, 2012, 19(4): 199-202.

(下转第 115 页)

由表4可以看出:相对与其他两种预测模型,本文方法得到的预测模型的RMSE与MAPE值明显降低.表明本模型预测性能高于其他两种模型.

表4 三种方法的预测误差指标对比

预测方法	RMSE	MAPE
RBF_SVR	1.869 3	0.109 7
混合核函数 SVR	1.560 9	0.087 2
混合核函数 PSO_SVR	1.190 5	0.064 3

在复杂度上,由于支持向量机核函数的计算复杂度与样本个数相关而与参数的变化无关,其时间复杂度一般为 $O(n^3)$ [7].本文构造的混合核函数是符合mercer条件下引用权重系数相加得到新的核函数.相比于传统的径向基核函数基础上只是单纯地增加了核函数的计算量,在时间复杂度没有产生阶数增加的情况下能够有效地增加SVR模型对网络安全态势预测精度.

5 结束语

网络安全态势预测一直是网络安全态势感知的关键问题,它能够有效地预防大规模网络安全事件的发生.本文从影响SVR的性能的两个方向入手,提出了基于PSO的混合核SVR网络安全态势预测模型.该方法在结合了SVR中局部核函数与全局核函数的优点,同时引入粒子群算法对SVR参数进行优化,得到最佳参数组合.预测结果表明该模型能够有效地提高预测精度,反映出关于未来安全的可靠的发展趋势,有助于网络管理者对网络安全事件进行决策.

参考文献:

[1] Jajodia S, Liu P, Swarup V, et al. Cyber situational

awareness[M]. Berlin:Springer, 2010.

- [2] Yuan Quan Shi, Tao Li, Wen Chen. Network security situation prediction using artificial immune system and phase space reconstruction[C]// Applied Mechanics and Materials. Switzerland: trans tech Publications LTD, 2010:3662-3666.
- [3] 尤马彦,凌捷,郝彦军.基于Elman神经网络的网络安全态势预测方法[J]. 计算机科学, 2012, 39(6):61-63+76.
- [4] 王晋东,沈柳青,王坤,等.网络安全态势预测及其在智能防护中的应用[J]. 计算机应用, 2010, 30(6):1480-1482.
- [5] 陈虹,王飞,肖振久.基于PSO_SVR的网络安全态势预测方法[J]. 计算机应用与软件, 2014, 35(8):292-294.
- [6] Elattar E E, Goulermas J, Wu Q H. Electric load forecasting based on locally weighted support vector regression[J]. Systems, Man, and Cybernetics, Part C: Applications and Reviews, IEEE Transactions on, 2010, 40(4):438-447.
- [7] 孙俊,王艳,金夏明,等.基于MSCPSO混合核SVM参数优化的生菜品质检测[J]. 农业机械学报, 2013, 44(9):209-213.

作者简介:

李方伟 男,(1960-),博士,教授.研究方向为移动通信技术与理论、信息安全技术.

罗嘉 男,(1990-),硕士研究生.研究方向为移动通信理论、网络安全态势感知技术. E-mail:125832324@qq.com;

朱江 男,(1977-),博士,副教授.研究方向为认知无线电技术.

张海波 男,(1979-),博士,讲师.研究方向为无线通信资源管理.

(上接第109页)

- [4] Zhang X. Separable reversible data hiding in encrypted image [J]. IEEE Transactions on Information Forensics and Security, 2012, 7(2):826-832.
- [5] Zhang W, Ma K, Yu N. Reversibility improved data hiding in encrypted images [J]. Signal Processing, 2014, 94(11):118-127.
- [6] Zhang X, Qian Z, Feng G, et al. Efficient reversible data hiding in encrypted images [J]. Journal of Visual

Communication and Image Representation, 2014, 25(2):322-328.

作者简介:

郑淑丽 女,(1974-),博士,副教授.研究方向为多媒体内容安全、无线传感网络等.

李丹丹 女,(1989-),博士.研究方向为图像密文域可逆信息隐藏. E-mail:lidandan110506@126.com.