

随机背包公钥密码的分析与改进

王青龙 赵祥模

(长安大学信息工程学院 西安 710064)

摘 要 针对随机背包公钥密码方案,提出一种私钥恢复攻击方法。发现 Wang 等人所构造的随机背包公钥方案实际上是隐含使用了一个特殊的超递增背包。通过使用普通超递增背包代替该特殊超递增背包,将超递增背包隐藏在随机选择的背包中,对原方案进行了改进,提出一种新的基于中国剩余定理的背包公钥密码方案。改进后的方案消除了原方案存在的设计缺陷,能够抵抗针对原方案提出的格规约攻击、低密度攻击以及 shamir 攻击。

关键词 随机背包,背包公钥密码,中国剩余定理,格规约

中图分类号 TP309 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2015.6.034

Analysis and Improvement of Public Key Cryptosystem Using Random Knapsacks

WANG Qing-long ZHAO Xiang-mo

(School of Information Engineering, Chang'an University, Xi'an 710064, China)

Abstract A new key recovery attack against Wang et al.'s cryptosystem which was built using random knapsacks was proposed in this paper. We found out that it is not a real random knapsack public key cryptosystem. Actually, a special super increasing knapsack is unobviously used in their scheme. By substituting the special super increasing knapsack with normal super increasing knapsack and hiding the normal super increasing knapsack into a random knapsack, we proposed an improved knapsack public key cryptosystem based on Chinese reminder theorem. Our scheme revises the shortage of the Wang et al.'s scheme and can resist the lattice basis reduction algorithm attack and low-density attack, as well as Shamir attack.

Keywords Random knapsack, Knapsack public key cryptosystem, Chinese reminder theorem, Lattice basis reduction algorithm

1 概述

背包公钥密码体制作为最早出现的公钥密码之一^[1],一直是密码学研究的一个主要内容。与目前广泛使用的 RSA 体制不同,背包问题是一个 NP 完全性问题,并且背包公钥密码由于容易设计与分析以及运算速度快的特性而获得了大量研究。遗憾的是绝大多数提出的背包公钥密码方案后来都被发现是不安全的。

背包公钥密码难以实现安全性的原因在于:1)因为不同于基于大整数分解问题和离散对数问题所设计的公钥密码体制能够实现可证明安全,背包公钥密码很难实现可证明安全;2)针对各种背包公钥密码体制提出的攻击方法非常强大,这些攻击方法包括 shamir 攻击^[2]、联立丢番图逼近攻击^[3]、低密度攻击^[4]以及各种格攻击^[5,6];3)因为绝大多数背包公钥密码都是基于陷门背包所设计的,实现上对陷门背包的随机化隐藏不足。如何设计安全的背包公钥密码体制一直是背包密码研究的核心问题。

近年来,一些新的背包公钥密码方案不断被提出^[7-13]。其中 Murakami 等人提出了两个不同的基于中国剩余定理和

随机背包构造的公钥密码方案^[8,9],然而 Peng 等人发现这两个方案都是不安全的,通过使用联立丢番图逼近攻击,他们提出了具体的恢复私钥攻击方法^[14]。2010 年,王等人也提出了一个基于中国剩余定理的随机背包公钥密码方案^[10](以下也称为王方案),但该方案同样被发现是不安全的^[15]。在文献[15]中,古等人对王方案的安全性按照公钥背包范数 $\|A\|_\infty$ 对应的二进制比特长度分情况进行了讨论,但他们提出的恢复私钥攻击思想(文献[15]定理一)和恢复明文攻击实验(文献[15]表一)针对的是王方案的特殊情况,一般情况下,文献[10]中的方案符合的是文献[15]定理二指出的情形,也就是其背包密度比较低,容易遭受低密度攻击。但是对大于 500×500 规模的情况,目前还缺乏有效的格规约方法,因此可以通过增加背包公钥的长度达到抵抗低密度攻击的目的。从这个意义上说,文献[15]的攻击并没有对王方案造成实质性威胁。文献[12]同样基于中国剩余定理构造背包公钥密码方案,但其采用了预编码方式。

由上述可知,大多数基于中国剩余定理的背包公钥方案都被发现是不安全的。本文的贡献是提出一种新的基于中国剩余定理构造的背包公钥密码方案,该方案没有采用预编

到稿日期:2014-07-09 返修日期:2014-09-06 本文受基金项目国家自然科学基金(61272436,61272404)资助。

王青龙(1970—),男,博士,副教授,主要研究方向为公钥密码算法研究及应用,E-mail:ql_wang@outlook.com;赵祥模(1960—),男,博士,教授,主要研究方向为智能交通、交通信息化、信息安全。

码方式。通过对王方案的深入分析,发现该方案实际上并不是真正的随机背包,本质上是隐含使用了一种特殊的超递增背包,而这种特殊超递增背包的使用使得方案的公钥背包呈现出一种规律性现象,该现象的存在为寻找方案使用的保密模数提供了途径,并在此基础上提出一种恢复私钥攻击方法。同时,在对王方案的安全性深入分析的基础上,通过使用普通的超递增背包取代原方案中的特殊超递增背包,我们提出了一种改进的方案。通过选择适当的参数,改进后的方案可以抵抗已知的针对背包公钥的攻击。

2 王方案介绍

密钥生成:随机选取 n 维背包向量 $u=(u_1, \dots, u_n)$, 其中 $u_i (1 \leq i \leq n)$ 为正整数。计算向量 $v=(v_1, \dots, v_n)$, 其中 $v_i = u_i - 2^{n-i}, 1 \leq i \leq n$ 。随机选取两个不同的素数 p, q , 满足 $p \geq \sum_{i=1}^n u_i, q \geq \max(\sum_{v_i > 0} v_i, -\sum_{v_i < 0} v_i)$ 。使用中国剩余定理计算向量 $A=(a_1, \dots, a_n)$, 其中

$$a_i = u_i \bmod p, a_i = v_i \bmod q \quad (1)$$

输出背包向量 A 为公钥, 私钥为 p, q 。

加密:对于 n 比特长二进制明文 $(m)_2 = m_1 \dots m_n$, 加密后的密文 $c = a_1 m_1 + \dots + a_n m_n$ 。

解密:对于给定密文 c , 计算 $c_p = c \bmod p, c_q = c \bmod q$, 其中 c_p 为模 p 非负最小剩余, c_q 为模 q 绝对最小剩余。则对应二进制明文 $(m)_2 = (c_p - c_q)_2$ 。

2.1 王方案安全性分析

与文献[15]的攻击不同,此处我们提出另一种针对王方案的攻击方法,该方法可以实现对私钥的获取,从而彻底破解王方案。首先介绍已知 $M=p \times q$ 下的攻击方法。

当已知 M 时,由式(1)可得

$$a_i = u_i \bmod p, a_i = u_i - 2^{n-i} \bmod q \quad (2)$$

即存在整数 k_1, k_2 满足 $(a_i - u_i) = k_1 p, (a_i + 2^{n-i} - u_i) = k_2 q$ 。进而可得

$$(a_i - u_i) \times (a_i + 2^{n-i} - u_i) = 0 \bmod M \quad (3)$$

解此一元二次方程可得到 u_i , 最后由

$$\begin{cases} p = \text{GCD}(a_i - u_i, M) \\ q = \text{GCD}(a_i + 2^{n-i} - u_i, M) \end{cases} \quad (4)$$

求得私钥 p, q 。

2.1.1 举例说明

我们以文献[11]中所给例子为例具体说明该攻击过程。王方案中的例子为:随机向量 $u=(65, 39, 21, 17, 19, 45, 10, 9)$, 对应向量 $v=(-63, -25, -11, 1, 11, 41, 8, 8)$, 私钥 $p=191, q=199$ 。可得 $M=191 \times 199=38009$ 。公钥 $A=(3121, 1567, 785, 399, 210, 19108, 9560, 4784)$ 。此时的攻击方式为:根据式(3)任意选取 $i=5$, 由公钥可知 $a_5=210$ 。代入式(3)得 $(210 - u_5)(218 - u_5) = 0 \bmod 38009$, 化简后得

$$u_5^2 - 428u_5 + 7771 = 0 \quad (5)$$

解此方程得 u_5 两个值分别为 409 和 19, 因为 u_i 不可能大于 a_i , 所以 u_5 值等于 19。进而由式(4)可得 $p=191, q=199$ 。

2.1.2 关于 M 的安全性分析

由上述可知,一旦获取 M , 就能够得到王方案的私钥。下面我们对 M 的安全性进行分析。由上例中公钥 A 可发现一个现象,除 210 和 19108 外,其余有 $a_i \approx 2a_{i+1}$ 这个现象,比

如 $3121 \approx 2 \times 1567, 1567 \approx 2 \times 785$ 。而 210 和 19108 之所以不满足这样的现象在于,有模 M 运算在内,即有同余式 $210 \approx 2 \times 19108 \bmod M$, 可得

$$210 \approx 2 \times 19108 - kM \quad (6)$$

此处 k 为整数,进一步分析可知, k 必为 1, 因为 $a_i < M$, 所以有 $2a_i < 2M$ 。由式(6)简单可得 $M \approx 38006$, 与实际值 38009 非常接近。

从实验结果看,这种现象并非特例,而是王方案的普遍结果,该现象可以从理论上得到进一步解释:由式(2)可知 $a_i = u_i \bmod p, a_{i+1} = u_{i+1} \bmod p$, 得

$$\begin{aligned} a_i - 2a_{i+1} &= u_i - 2u_{i+1} \bmod p \Rightarrow (a_i - 2a_{i+1}) - (u_i - 2u_{i+1}) \\ &= 0 \bmod p \end{aligned} \quad (7)$$

同样由式(2)可知

$$\begin{aligned} a_i &= u_i - 2^{n-i} \bmod q, a_{i+1} = u_{i+1} - 2^{n-(i+1)} \bmod q, \text{得} \\ a_i - 2a_{i+1} &= u_i - 2u_{i+1} \bmod q \Rightarrow (a_i - 2a_{i+1}) - (u_i - 2u_{i+1}) \\ &= 0 \bmod q \end{aligned} \quad (8)$$

由式(7)、式(8)简单可得 $a_i - 2a_{i+1} = kM + (u_i - 2u_{i+1})$, 此处 k 为一整数。因为 $u_i - 2u_{i+1} < p \ll M$, 所以有 $a_i - 2a_{i+1} \approx kM$, 也就是有 $a_i \approx 2a_{i+1} \bmod M$ 。

理论分析表明:背包公钥中存在的现象是王方案所固有的,属于方案设计上的缺陷,并且这种现象的存在使得对公钥的随机置换起不到任何安全作用,因为根据此现象可以很容易对置换后的公钥进行排序。需要指出的是,尽管文献[11]提到可以使用二阶可逆整数矩阵进一步隐藏密钥信息,但并没有给出如何得到这样一个矩阵,因为不仅该二阶矩阵自身须为整数矩阵,其逆矩阵同样须为整数矩阵才能解密。虽然选取 $GF(p_1)$ 上的矩阵满足这样的要求,但因为王方案同时又涉及到 $GF(p)$ 和 $GF(q)$ 上的运算,当素数 p_1, p, q 不相等时,这种跨不同域的运算很难保障解密算法正常解密,如何选择这些参数并不是一个简单问题,因此文献[10]提出的方法实际上并不具有可行性。

由上述分析可知,王方案的安全性严格依赖 M 的保密(并不需要知道 M 的分解),一旦 M 泄露,方案将被彻底攻破,但是其方案设计上的内在性不足导致公钥暴露关于 M 的很大信息,使得通过强力搜索最终得到 M 称为一种可行方法。

另外,王等人称文献[10]是一种基于随机背包的方案,但实际上其仍然隐含使用了一种超递增背包。由 $v_i = u_i - 2^{n-i}$, 可得 $2^{n-i} = u_i - v_i$, 而显然 $2^{n-1}, 2^{n-2}, \dots, 2^1, 2^0$ 构成了超递增背包。基于此分析,我们提出一种改进的方案,改进的关键是用一般的超递增背包取代 $2^{n-1}, 2^{n-2}, \dots, 2^1, 2^0$ 这一特殊超递增背包。

3 改进的方案

方案设置:任选一超递增背包 $b_1, \dots, b_n$, 再任选两个背包 $u=(u_1, \dots, u_n)$ 和 $v=(v_1, \dots, v_n)$, u_i, v_i 为正整数且满足 $b_i = u_i + v_i, i=1, \dots, n$ 。任选两个整数 M_1, M_2 , 满足 $M_1 \geq \sum_{i=1}^n u_i, M_2 \geq \sum_{i=1}^n v_i$, 并且满足 $\text{GCD}(M_1, M_2) = 1$ 。令 $M = M_1 M_2$, 使用中国剩余定理计算向量 $A=(a_1, \dots, a_n)$, 其中

$$a_i = u_i \bmod M_1, a_i = v_i \bmod M_2 \quad (9)$$

输出背包向量 A 为公钥, 私钥为 M_1, M_2 。

加密: 对于 n 比特长二进制明文 $(m)_2 = m_1 \cdots m_n$, 加密后的密文 $c = a_1 m_1 + \cdots + a_n m_n$ 。

解密: 对于给定密文 c , 计算 $c_p = c \bmod M_1, c_q = c \bmod M_2$ 。令 $b = c_p + c_q$, 由 b 和超递增背包 $b_1, \cdots, b_n$ 恢复出明文。

3.1 举例说明

系统参数: 选取超递增背包 $(b_1, \cdots, b_8) = (150, 230, 400, 825, 2130, 4521, 8700, 19320)$, 任选 $u = (50, 120, 80, 350, 750, 2900, 5300, 7210)$, $v = (100, 110, 320, 475, 1380, 1621, 3400, 12110)$ 。选取 $M_1 = 16763, M_2 = 19531$ 。有 $M = 327398153$ 。使用中国剩余定理计算得公开钥 $A = (242946209, 147849780, 52987923, 116268518, 180018607, 248279693, 262597695, 236063776)$ 。

加密: 设待加密明文二进制信息为 $m = 11010110$, 则密文 $c = 1017941895$ 。

解密: $c_p = 1017941895 \bmod 16763 = 8720, c_q = 1017941895 \bmod 19531 = 5706, b = 14426$ 。按照普通超递增背包的解密方式简单计算可恢复明文为 11010110。

4 安全性分析

4.1 低密度攻击

因为本文方案构造过程中使用了中国剩余定理, 使得方案的背包密度只有大约 0.5, 正常情况下显然容易受到低密度攻击。但是低密度攻击需要使用到格规约算法, 而针对大于 500×500 规模的情况目前还没有有效的格规约方法, 因此, 我们可以选取足够大的参数来达到抵抗低密度攻击的效果, 比如可以选取 $n = 1000$ 。

4.2 Shamir 攻击

至于 Shamir 攻击, 因为其是针对普通超递增背包构造的方案, 但本文方案并不是直接基于超递增背包构造的, 而是将其隐含在两个随机背包中, 本文方案中的公钥背包构造方法与直接使用超递增背包构造生成的公钥背包方法完全不同, 因此我们认为 Shamir 攻击并不适用于本文方案。

4.3 联立丢番图逼近攻击

联立丢番图逼近攻击利用了背包公钥系统隐含的一些信息。Peng 等人之所以能够通过联立逼近攻击攻破 Murakami 的随机背包公钥方案^[8,9], 是因为在文献[8]中公钥背包实际上包含了 $a_i = v s_i \bmod p, i = [1, n], b_i = v t_i \bmod p, i = [1, m], c_j = w t_j \bmod q, j = [1, m]$ 3 部分, 后面两部分都是用来隐藏 t_j , 文献[14]的恢复私钥攻击正是利用了这一信息。文献[9]实际上是基于两个背包构造的, 其中一个是完全由随机数组成的, 另一个背包是由部分随机数和部分超递增背包共同组成的, 从而导致方案中隐藏包含了信息 $p \gg q$ 。而本方案中公钥只由一部分组成, 因此 Peng 等人针对文献[8]提出的联立丢番图逼近攻击方法并不适用于本文方案。同时由本文方案中 u, v 的随机性可知 $\|U\|_\infty \approx \|V\|_\infty, M_1 \approx M_2$, 因此 Peng 等人针对文献[9]的联立丢番图逼近攻击方法也不适用于本文方案。由此可知联立丢番图逼近攻击并不适用于本文方案, 因为攻击者没有办法获取足够的信息使用联立丢番图逼近攻击。

至于文献[15]提到的攻击方法, 同样因为本方案中 $M_1,$

M_2 在二进制长度上大约相同, 所以文献[15]的攻击方式也不适用本文方案。

同时改进后的方案弥补了原方案中存在的公钥背包泄露 M 信息的缺陷, 并且即使攻击者获得了 M , 因为 u_i, v_i 之间并不存在规律性关系, 所以并不能得到前述式对应的方程, 也就不能由此得到私钥 M_1 和 M_2 。另外与原方案不同的是, 改进后的方案通过对公钥背包进行随机置换可以提高安全性。

需要指出的是: 本方案使用了中国剩余定理, 在已知 M 情况下, 其安全性相等于分解大整数困难问题, 而不再是普通背包方案所依赖的 NP 困难问题。但本方案 M 是保密的, 攻击者并不能得到 M 。另外本文方案和其它绝大多数已有的背包方案一样, 未能提出可证明的安全方法, 设计可证明安全的背包密码方案还有待进一步的研究。

结束语 鉴于传统方法设计的背包公钥密码方案大多数都被发现是不安全的, 使用新方法设计更安全的背包公钥密码方案成为研究的主要方向, 但这些新的方案也相继被发现是不安全的^[16,17]。其中文献[10]基于中国剩余定理构造随机背包公钥也不失为一种方法, 遗憾的是因为其隐含使用了一个特殊的超递增背包而导致所设计方案的安全性不足。本文针对这一设计上的缺陷, 通过将普通的超递增背包隐藏在随机化后的背包中, 利用中国剩余定理生成公钥背包, 解决了原方案中存在的安全问题。同文献[11]相比较, 本文方案也更具一般性。设计基于中国剩余定理的高密度背包公钥密码方案将是我們下一步研究的内容。

参考文献

- [1] Merkle R C, Hellman M E. Hiding information and signatures in trapdoor knapsacks [J]. IEEE Transactions on Information Theory, 1978, 24(5): 525-530
- [2] Shamir A. A polynomial-time algorithm for breaking the basic Merkle-Hellman[C]//Proceedings of the 23rd Annual Symposium on Foundations of Computer Science, 1982. Washington: IEEE, 1982: 145-152
- [3] Lagarias J C. Knapsack public key cryptosystems and Diophantine approximation[M]//Advances in Cryptology. New York: Plenum, 1984: 3-23
- [4] Coster M J, Joux A, LaMacheia B A, et al. Improved low-density subset sum algorithms [J]. Computational Complexity, 1992, 2(2): 111-128
- [5] Nasako T, Murakami Y, Kasahara M. Security of a class of knapsack public-key cryptosystems against low-density attack [J]. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2008, E91-A(10): 2889-2892
- [6] Wang Bao-cang, Hu Lei. Lattice Attack on the Knapsack Cipher 0/255[C]//Proceedings of the 2012 Fourth International Conference on Intelligent Networking and Collaborative Systems, 2012. Washington: IEEE, 2012: 577-580
- [7] Murakami Y, Kasahara M. New Trapdoor Sequences in Modular Knapsack Cryptosystem[C]//7th International Conference on Computing and Convergence Technology, 2012. Washington: IEEE, 2012: 604-609
- [8] Murakami Y, Kasahara M. A differential knapsack publickey

- cryptosystem[C]//6th International Conference on Computer Sciences and Convergence Information Technology. Washington; IEEE, 2011; 613-617
- [9] Murakami Y. A New Construction of Knapsack PKC by Using A Random Sequence[C]//Global Telecommunications Conference. Washington; IEEE, 2009; 1-6
- [10] 王保仓, 韦永壮, 胡予濮. 基于随机背包的公钥密码[J]. 电子与信息学报, 2010, 32(7): 1580-1584
Wang Bao-cang, Wei Yong-zhuang, Hu Yu-pu. Public Key Cryptosystem Using Random Knapsacks[J]. Journal of Electronics & Information Technology, 2010, 32(7): 1580-1584
- [11] 王保仓, 胡予濮. 高密度背包型公钥密码体制的设计[J]. 电子与信息学报, 2006, 28(12): 2390-2393
Wang Bao-cang, Hu Yu-pu. Knapsack-Type Public-Key Cryptosystem with High Density[J]. Journal of Electronics & Information Technology, 2006, 28(12): 2390-2393
- [12] Murakami Y, Nasako T. Knapsack Public-Key Cryptosystem Using Chinese Remainder Theorem[DB/OL]. 2014-9-6. <http://eprint.iacr.org/2007/107.pdf>
- [13] Wang Bao-cang, Hu Yu-pu. Quadratic compact knapsack publickey cryptosystem[J]. Computers & Mathematics with Applications, 2010, 59(1): 194-206
- [14] Peng Li-qiang, Zuo Jin-yin, Hu Lei, et al. Analysis of Two Public Key Cryptosystems Based on Randomized Knapsack Sequences [J]. Chinese Journal of Electronics, 2014, 23(1): 175-178
- [15] 古春生, 于志敏, 景征骏. 基于随机背包公钥密码的攻击[J]. 计算机应用研究, 2012, 29(9): 3486-3488
Gu Chun-sheng, Yu Zhi-min, Jing Zheng-jun. Attack on random knapsack-based public key cryptosystems[J]. Application Research of Computers, 2012, 29(9): 3486-3488
- [16] Lee M S. Improved cryptanalysis of a knapsack-based probabilistic encryption scheme[J]. Information Sciences, 2013, 222(2): 779-783
- [17] Rastaghi R, Oskouei H R D. Cryptanalysis of a Public-key Cryptosystem Using Lattice Basis Reduction Algorithm[J]. International Journal of Computer Science, 2012, 9(1): 110-117

(上接第 138 页)

像机理的不同,造成自然图像和计算机生成图像之间存在明显的纹理特征差异。基于此,本文在 HSV 颜色空间提取了图像及其下采样图像的局部二进制计数模式直方图特征,结合 SVM 分类器实现了自然图像和计算机生成图像的鉴别。与现有算法相比,本文算法在降低特征维度的同时取得了较高的识别率。

参 考 文 献

- [1] 万国富. 基于分形维数的自然图像盲鉴别算法研究[D]. 长春: 吉林大学, 2013
Wan Guo-fu. Research on natural image blind identifying algorithm based on fractal dimension[D]. Changchun: Jilin University, 2013
- [2] 张震, 杨宇豪. 基于 Benford 模型的自然图像与计算机生成图像的鉴别[J]. 北京工业大学学报, 2013, 39(6): 930-935
Zhang Zhen, Yang Yu-hao. Distinguishing computer graphics from natural image based on Benford model[J]. Journal of Beijing University of Technology, 2013, 39(6): 930-935
- [3] Lyu S, Farid H. How realistic is photorealistic? [J]. IEEE Transactions on Signal Processing, 2005, 53(2): 845-850
- [4] 郑二功, 平西建. 一种基于相邻像素一致性的数码照片与计算机图像鉴别方法[J]. 计算机研究与发展, 2009, 46(增刊 1): 258-262
Zheng Er-gong, Ping Xi-jian. Identifying computer graphics from digital photographs based on coherence of adjacent pixels[J]. Journal of Computer Research and Development, 2009, 46(Suppl 1): 258-262
- [5] Xu B, Wang J, Liu G, et al. Photorealistic computer graphics forensics based on leading digit law[J]. Journal of Electronics (China), 2011, 28(1): 95-100
- [6] Wu R, Li X, Yang B. Identifying computer generated graphics via histogram features[C]//2011 18th IEEE International Conference on Image Processing (ICIP). IEEE, 2011: 1933-1936
- [7] Li Z, Ye J, Shi Y Q. Distinguishing computer graphics from photographic images using local binary patterns[M]//Digital Forensics and Watermarking. Springer Berlin Heidelberg, 2013: 228-241
- [8] Dehnie S, Sencar T, Memon N. Digital image forensics for identifying computer generated and digital camera images[C]//2006 IEEE International Conference on Image Processing. IEEE, 2006: 2313-2316
- [9] Dirik A E, Bayram S, Sencar H T, et al. New features to identify computer generated images[C]//IEEE International Conference on Image Processing, 2007 (ICIP 2007). IEEE, 2007, 4: 433-436
- [10] 郭克. 自然图像和计算机生成图像检测方法研究[D]. 宁波: 宁波大学, 2012
Guo Ke. Research on the detection methods of natural images and computer-generated images[D]. Ningbo: Ningbo University, 2012
- [11] Zhao Y, Huang D, Jia W. Completed local binary count for rotation invariant texture classification [J]. IEEE Trans. Image Process., 2012, 21(10): 4492-4497
- [12] 李文祥, 张涛, 郑二功, 等. 基于二阶差分统计量的自然图像与计算机图形的鉴别[J]. 计算机辅助设计与图形学学报, 2010, 22(9): 1613-1618
Li Wen-xiang, Zhang Tao, Zheng Er-gong, et al. Discrimination between natural images and photorealistic computer graphics using second-order difference statistics[J]. Journal of Computer-Aided Design & Computer Graphics, 2010, 22(9): 1613-1618
- [13] Ker A D. Steganalysis of LSB matching in grayscale images[J]. Signal Processing Letters, IEEE, 2005, 12(6): 441-444
- [14] Chang C C, Lin C J. LIBSVM: a library for support vector machines[J]. ACM Transactions on Intelligent Systems and Technology (TIST), 2011, 2(3): 27
- [15] Ng T T, Chang S F, Hsu J, et al. Columbia photographic images and photorealistic computer graphics dataset[R]. Columbia University, ADVENT Technical Report, 2005: 205-2004