抗SPA攻击的快速LSB均衡隐藏算法

韩杰思[1]，沈建京[1]，彭韶峰[2]

(1. 解放军信息工程大学理学院 郑州 450001; 2. 西南电子电信技术研究所 成都 610041)

【摘要】提出了一种新的LSB隐藏方法，根据待嵌载体图像像素值的奇偶性和嵌入信息的内容，选择像素值加1或加2的嵌入方式，使得SPA(sample pair analysis)攻击的假设条件在嵌入前后保持平衡，致使SPA攻击失效。在使用该方法嵌入率达到100%时，SPA攻击的估计值仍然小于判决门限。实验不仅验证了新方法抵抗SPA攻击的能力，也验证了新方法可以抵抗RS等检测。新方法嵌入方式简单，且无需在嵌入后再做附加处理，便于实现。

关 键 词 攻击; 均衡; 像素; SPA攻击; 信息隐写

中图分类号 TP393 **文献标识码** A doi:10.3969/j.issn.1001-0548.2010.05.025

Quick Equilibrium LSB Steganography Method Resisting SPA

HAN Jie-si[1], SHEN Jian-jing[1], and PENG Shao-feng[2]

(1. Institute of Science, Information and Engineering University Zhengzhou 450001;

2. Institute of Southwest Electron. &Telecom. Techniques Chengdu 610041)

Abstract A new LSB steganography method is proposed. According to the parity of carrier's image pixel to be embedded and the content of embedded information, the embedded way of the pixel adding 1 or 2 is chosen to make the hypothesis of SPA (sample pair analysis) attack keep balance before or after the embedding, causing SPA attack disable. When the proposed algorithm is used to make the embedding rate reaching 100%, the estimated value of the SPA attack is still smaller than judge threshold. Experimental results validate that the new method not only can resist the SPA attack, but also can resist the test such as RS. The embedding mode of new method is convenient to achieve without additional disposal after embedding.

Key words equilibrium; pixels; SPA steganalysis; steganography

信息隐藏技术以多媒体为载体，将重要信息隐藏其中，以实现隐秘通信，是信息安全领域的重要研究方向。20世纪90年代以来，信息隐藏经历了10余年的发展，已有很多隐藏算法问世。而其中最为经典、应用范围最广的当属LSB隐藏，其原理是将秘密信息的比特流隐藏到载体图像的最低有效位(least significant bits)，隐蔽性好、隐藏量大、且计算简单。目前，已有多个公开的隐藏软件使用该种隐藏方法，如Invisible Secrets4、S-Tools、Steganos等。

很多专家学者尝试对LSB隐藏进行攻击，提出了多种检测算法。文献[1]的PoVs方法被最早提出来，它假设秘密信息是服从均匀分布的，通过比较秘密信息的理论频率分布和隐秘载体样本分布进行检测。该方法对连续LSB嵌入有较好的检测能力，并可估计出嵌入信息的长度，但对扩散、随机嵌入等非连续嵌入的检测效果却不理想。文献[2]提出的RQP方法是针对彩色图像LSB隐藏的检测方法，它基于LSB隐藏会引起图像具有更多相近颜色对，当图像中有大量相近颜色对出现则认为存在秘密信息。但该方法不适用于独立颜色数较多的彩色图像和灰度图像。此后，文献[3]提出了既可对连续的LSB隐藏进行检测，又适用于分散LSB嵌入和随机LSB嵌入的检测方法，检测载体包含灰度和彩色图像。该方法将图像像素分为规则组、奇异组和不可用组3类，通过统计规则组和奇异组数量的变化估计嵌入长度，这就是经典的RS方法。文献[4]将RS的思想运用于音频文件的隐藏检测，提出了一种基于样本对分析的音频检测方法。文献[5]提出的SPA方法根据概率理论对LSB嵌入机理进行了深入的探讨。该方法通过合理的构造准素集，即满足一定条件的像素值对的集合，使得集合的势随着LSB的嵌入改变。该方法理论上包容了RS检测方法，在LSB上嵌入比率大于3%时，能较准确估计嵌入信息长度。

上述检测方法中，RS和SPA的检测效果最为理

收稿日期：2009 – 03 – 19; 修回日期：2009 – 07 – 31
基金项目：部级基金项目
作者简介：韩杰思(1981 –)，男，博士生，主要从事信息隐藏、隐藏检测及智能处理方面的研究.

想，也成为业内的经典方法。之后对LSB隐藏的改进都是为了能抵抗该两种检测。文献[6]提出了3种方法：(1) 像素值随机的加1或者减1；(2) 像素值加1；(3) 像素值减1。这些方法产生的隐秘图像的直方图是对原始载体图像直方图的平滑，保持了图像的直方图统计特性，使得PoVs方法不再有效。同时，这些方法保证了规则组和奇异组的数量不再随信息嵌入而变化，所以同样可以抵抗RS攻击。文献[7-8]提出了一种基于动态补偿的LSB隐藏方法。该方法在随机间隔LSB嵌入后，在隐秘图像选择某个区域进行补偿，即对选中区域内所有的像素进行加1(或者减1)，而区域的选择是动态的，目的是通过寻找最佳的补偿使得SPA分析得到一个较小的隐藏信息比率估计。文献[9]提出了一种按计算的比例混合使用两种替换方法的嵌入算法，使得SPA算法的检测值趋于最小。

本文通过分析SPA方法的原理，提出了一种可以抵抗SPA方法的LSB隐藏算法。该方法改变了传统LSB的替换嵌入方式，在秘密信息比特与嵌入位置像素LSB相同时加2(或者减2)；不同时对像素值加1(或者减1)。提取时判断像素的奇偶性，若为奇数则提取1；反之提取0，同样实现盲提取。由于本文方法保证了SPA中的假设 $E\{|U_{m=i}^{j}X_{2m+1}|\}=E\{|U_{m=i}^{j}Y_{2m+1}|\}$ 在嵌入前后都成立，所以方法能抵抗SPA检测，最后的实验在验证该结论的同时，也验证其抵抗其他检测的能力。

1　SPA攻击方法

SPA攻击方法的基本原理基于有限状态机理论，有限状态机的状态是选择的样本对的多重集。对自然图像而言，相邻像素对所构成的多重集之间有某种固定的关系。随机LSB嵌入后会引起这些多重集的改变，从而破坏固定的统计关系。

假定选择的载体图像大小为 $M\times N$，$L=M\times N$。用 $s_1,s_2,\cdots,s_L$ 表示图像的像素值，图像的一个像素值对可记为 (s_i,s_j)，$1\leqslant i$，$j\leqslant L$。令 P 是从图像中抽取的一组样本对，u 和 v 是两个相邻像素的值，$0\leqslant u\leqslant 2^b-1$，$0\leqslant v\leqslant 2^b-1$，其中 b 是每个样本值的比特数，则 P 可看作是一个由一系列二元组 (u,v) 构成的多重集。用 D_n 表示 P 的子多重集，其中 $0\leqslant n\leqslant 2^b-1$，$n$ 是一个固定的整数，表示相邻像素的差值，即 $D_n=\{(u,v)\in P\,\|\,u-v|=n\}$；而对每个整数 m 而言，$0\leqslant m\leqslant 2^b-1$，定义 $C_m=\{(u,v)\in P\,\|\,\lfloor u/2\rfloor-\lfloor v/2\rfloor|=m\}$，其中 $\lfloor *\rfloor$ 指不大于 $*$ 的最大整数。

因此，D_n 和 C_m 就构成了 P 的两个划分，而 D_{2m} 包含在 C_m 中。C_m 可以划分成 X_{2m-1}、X_{2m}、Y_{2m} 和 Y_{2m+1}，其中 X_{2m} 和 Y_{2m} 构成 D_{2m} 的划分。同理，D_{2m+1} 可划分为 X_{2m+1} 和 Y_{2m+1}，有 $X_{2m+1}=D_{2m+1}\cap C_{m+1}$，$Y_{2m+1}=D_{2m+1}\cap C_m$，$0\leqslant m\leqslant 2^b-2$。对于 D_{2m+1} 中的样本对 (u,v)，$|u-v|=2m+1$，其中样本对中较大元素为偶数的样本对属于 X_{2m+1}，较大元素为奇数的样本对属于 Y_{2m+1}。

对于自然图像而言，大量的统计表明：

$$E\{|X_{2m+1}|\}=E\{|Y_{2m+1}|\} \tag{1}$$

其中 $|*|$ 表示集合的势，而SPA攻击正是基于该重要的假设。

对待测图像各样本集的统计可推导出程(对待测图像各集合都作 A' 标记)：

$$\begin{aligned}&\frac{(|C_m|-|C_{m+1}|)p^2}{4}-\\&\frac{(|D'_{2m}|-|D'_{2m+2}|+2|Y'_{2m+1}|-2|X'_{2m+1}|)p}{2}+\\&|Y'_{2m+1}|-|X'_{2m+1}|=0\\&\qquad 0\leqslant m\leqslant 2^b-1\end{aligned} \tag{2}$$

$$\begin{aligned}&\frac{(2|C_0|-|C_1|)p^2}{4}-\\&\frac{(2|D'_0|-|D'_2|+2|Y'_2|-2|X'_2|)p}{2}+\\&|Y'_1|-|X'_1|=0\\&\qquad m=0\end{aligned} \tag{3}$$

解其中任意一个方程就可得到隐藏信息比率 p 的估计。

考虑到假设条件对隐藏信息比率估计精度的影响，文献[5]给出了更可靠的假设：

$$E\{|U_{m=i}^{j}X_{2m+1}|\}=E\{|U_{m=i}^{j}Y_{2m+1}|\} \tag{4}$$

以式(4)代替假设条件式(1)，可推导出更可靠的方程：

$$\frac{(|C_i|-|C_{j+1}|)p^2}{4}-\frac{\left(|D'_{2i}|-|D'_{2j+2}|+2\sum_{m=i}^{j}(|Y'_{2m+1}|-|X'_{2m+1}|)\right)p}{2}+\sum_{m=i}^{j}(|Y'_{2m+1}|-|X'_{2m+1}|)=0\qquad 1\leqslant i\leqslant m\leqslant j\leqslant 2^b-1 \tag{5}$$

$$\frac{2(|C_0|-|C_{j+1}|)p^2}{4}-\frac{\left(2|D'_0|-|D'_{2j+2}|+2\sum_{m=i}^{j}(|Y'_{2m+1}|-|X'_{2m+1}|)\right)p}{2}+\sum_{m=i}^{j}(|Y'_{2m+1}|-|X'_{2m+1}|)=0\qquad i=0 \tag{6}$$

通过解其中任意一个方程就可得到较为精确的嵌入率的估计。文献[5]还给出了重要参数的经验值，当 $i=0$， $j=30$，判定门限值为0.018时，通过解方程可以得到最精确的嵌入比率估计，平均误差为0.023。

综上所述，针对一个待测图像，首先统计图像中相邻像素值高7位、大小差值为0和31的像素对的数量，记为 C_0 和 C_{31}；接着计算 $|Y'_{2m+1}|$ 和 $|X'_{2m+1}|$，$m=0,1,\cdots,30$)，并计算 D'_0 和 D'_{62}；最后将得到的参数代入式(6)求解，即可得到嵌入信息比率 p 的估计值。

2 抵抗SPA攻击的LSB隐藏算法

2.1 抵抗SPA攻击的分析

SPA方法是基于假设式(4)为前提，当图像进行LSB替换隐藏后，$|U^j_{m=i}X_{2m+1}|$ 和 $|U^j_{m=i}Y_{2m+1}|$ 将发生变化，从而破坏式(4)的平衡。文献[7]中对 Y_{2m+1} 和 X_{2m+1} 的差值在嵌入前后的变化对SPA方法得到的嵌入率估计值造成的影响进行了分析，有：

$$\delta_{i,j}=\frac{\left\|U^j_{m=i}Y'_{2m+1}|-|U^j_{m=i}X'_{2m+1}\right\|}{|U^j_{m=i}Y'_{2m+1}|+|U^j_{m=i}X'_{2m+1}|} \tag{7}$$

式(7)表征嵌入信息后 $U^j_{m=i}X'_{2m+1}$ 和 $U^j_{m=i}Y'_{2m+1}$ 的偏离度。检测得到的估计值随着 $\delta_{i,j}$ 的增大而增大,即 $\left\|U^j_{m=i}Y'_{2m+1}|-|U^j_{m=i}X'_{2m+1}\right\|$ 越接近0，$\delta_{i,j}$ 就越小，得到的嵌入率估计值也就越小。要使SPA检测达到的嵌入率估计值低于判决门限，就必须使 $\delta_{i,j}$ 的值足够小。

文献[7]中提出的DCLS方法(可抵御SPA方法分析的动态补偿LSB隐藏方法)在秘密信息随机间隔嵌入完成后，对隐秘图像的统计参量 $|U^j_{m=i}Y'_{2m+1}|$ 和 $|U^j_{m=i}X'_{2m+1}|$ 进行补偿，以达到消除 $U^j_{m=i}X'_{2m+1}$ 和 $U^j_{m=i}Y'_{2m+1}$ 偏离度的目的。然而直接将图像一半的像素值加1是不够的，必须对图像动态地进行补偿。文中介绍使用穷尽的方法，逐行递增对图像进行补偿，对每种补偿情况均计算 $\delta^i_{0,30}$ ($1\leqslant i\leqslant N-2$， N 为图像总行数)，取最小的偏离度，确定其所对应的补偿为最佳补偿。而图像的补偿区域是任意的，可以是随机选取的矩形，也可以是图像中一块其他形状的区域。

2.2 抵抗SPA攻击的快速LSB隐藏算法

DCLS方法可以成功地抵抗SPA攻击，但在完成嵌入后需要通过对隐秘图像进行复杂的动态补偿寻求最佳补偿，其过程繁琐，计算量太大。

前面已经分析了要想抵抗SPA攻击，就必须保证(4)的平衡，使 $\delta_{i,j}$ 达到一个很小的值。(可以通过嵌入后的补偿实现，也可以在嵌入时)。本文的创新之处就是通过改变秘密信息在载体图像LSB上的嵌入方式，使 $\left\|U^j_{m=i}Y_{2m+1}|-|U^j_{m=i}X_{2m+1}\right\|$ 在隐藏前后保持不变，从而使SPA攻击的估计值一直处于低于门限的状态。下面分别对算法的各个部分进行介绍。

2.2.1 载体图像的预处理

本文方法在嵌入时不再是替换像素的LSB，而是根据情况对像素值做部分加1和部分加2的处理。若选中的像素为254或255，则分别做加2和加1,嵌入后都将达到256，显然不在像素值的范围内。如果在嵌入时遇到值为254或255的像素做跳过处理，在提取时将无法判断该像素是未经嵌入的，还是其他像素做加2或加1嵌入后变成的。

本文所采取的策略是不挑选含有值为254和255的像素的图像作为载体，或者对载体图像中所有值为255的像素做减2，所有值为254的像素做减1的预处理，保证图像中所有像素的最大值为253。当然，在确定载体后(无论是选择合适图像还是对图像进行预处理)，先对其进行一次SPA检测，保证对载体检测后得到的信息嵌入比率的估计值小于门限值。

本文的嵌入方法也可根据情况对像素值做部分减1和部分减2处理，所以选择载体图像时就要选择不含有值为0和1的像素的图像，或者对载体图像中所有值为0的像素做加2的预处理，对所有值为1的像素做加1的预处理，保证图像中所有像素的最小值为2。

2.2.2 信息的嵌入

由于SPA攻击是针对随机LSB嵌入，所以本文也采用随机嵌入[10]。随机间隔嵌入使用伪随机数发生器，用收发双方共享的种子产生随机序列，把秘密信息随机地扩散到载体图像中，形成隐秘载体图像。令产生的随机序列为 $k_1,k_2,\cdots,k_{l(m)}$，其中 $l(m)$ 是秘密信息的长度，且：

$$\begin{cases} j_1=k_1 \\ j_i=j_{i-1}+k_1 & i\geqslant 2 \end{cases}$$

式中 j_i 是整个图像中用于隐藏秘密信息的像素位置序列。

在嵌入时，本文假设秘密信息的嵌入是随机嵌入，则像素值差为 $2m+1$ 的相邻像素对嵌入信息前后在图像中都是均匀分布的。通常，进行LSB替换嵌入后图像 $\delta_{0,30}$ 的值将变大，主要是 $|U^j_{m=i}Y'_{2m+1}|-|U^j_{m=i}X'_{2m+1}|$ 值将变大，要使值趋近于0，才能降低 $\delta_{0,30}$ 的值，从而使SPA攻击得到的估计值小于门限值。

本文首先考虑对于秘密信息和选取位置LSB相同的情况不做处理，不同的情况做像素值加1处理，实际上就是对替换LSB隐藏后的图像中那些LSB由1被替换成0的位置的像素进行加2操作。进行如此操作的目的就是使部分 Y'_{2m+1} 转变成 X'_{2m+1} (主要是 Y'_1 到 X'_1 的转变，通常图像中 Y_1 和 X_1 的比例最大)，从而使 $|U^j_{m=i}Y'_{2m+1}|-|U^j_{m=i}X'_{2m+1}|$ 的值下降，趋近于0。

本文实现的SPA攻击以假设式(4)为前提，求解式(6)。使用标准测试图像boat.bmp进行测试，如图1所示。原图本身不含有值为254和255的像素，故无需进行预处理。对原图进行SPA攻击，得到的 $\delta_{0,30}$ 为0.003 0、估计值为0.015 2，低于门限值0.018，可以用作载体图像。在使用LSB随机替换隐藏，进行40%的秘密信息嵌入后，用SPA攻击得到的 $\delta_{0,30}$ 为0.087、估计值为0.392，接近实际嵌入比率。而使用上面提出的嵌入方式进行40%的秘密信息嵌入后，用SPA攻击得到的 $\delta_{0,30}$ 为0.004 2、估计值为0.016，小于门限值，SPA攻击会得出无隐藏的判决结果。但从结果可以看出，嵌入率为40%时，SPA攻击的估计值已经接近门限值了，于是提高嵌入率进行测试。果然，使用上面提出的嵌入方式，嵌入率为90%时，进行SPA攻击得到的估计值为0.023 8，已经高于门限值了，SPA攻击同样会得出有隐藏的判决结果。所存在的问题仍然是 $|U^j_{m=i}Y'_{2m+1}|-|U^j_{m=i}X'_{2m+1}|$ 的值不够小。于是本文对上面的嵌入方式进行改进，改进的最终嵌入如下。

(1) 嵌入时，若选中的像素是奇数且嵌入比特为1，则像素值加2；若选中像素是奇数且嵌入比特为0，则像素值加1。

(2) 若选中的像素是偶数且嵌入比特为1，则像素值加1；若选中的像素是偶数且嵌入比特为0，则像素值加2。

图1　原始boat图

图2　嵌入率为40%的boat图

图3　嵌入率为90%的boat图

(3) 可将所有的加法操作换成减法操作，达到的效果一致。

改进后的方法与前面的嵌入方式不同的是对原本嵌入时不需要修改的像素进行加2处理。改进的目的是在不改变像素奇偶性的情况下，对部分 Y'_{2m+1} 与 X'_{2m+1} 进行相互转化(如像素值对(1,0)隐藏后变成(1,2)，就完成了从 Y'_1 到 X'_1 的转化，反之同理)，使二者的势更加接近，即 $|U^j_{m=i}Y'_{2m+1}|-|U^j_{m=i}X'_{2m+1}|$ 的值更加趋近于0。本文称该操作为势的均衡。

使用改进的嵌入方法对boat.bmp进行40%的信息嵌入，得到的隐秘图像如图2所示。对该隐秘图形进行SPA攻击，得到的 $\delta_{0,30}$ 为0.001 1、估计值为0.004 9，远小于门限值。随着秘密信息的继续嵌入，$\delta_{0,30}$ 和估计值会增大。对boat.bmp进行90%的信息嵌入，得到的隐秘图像如图3所示。进行SPA攻击，得到的 $\delta_{0,30}$ 为0.002 8，略低于原始图像，得到的估计值为0.011，仍然低于门限值。

2.2.3　信息的提取

信息提取的过程与嵌入相反。接收方只需得到和发送方同样的伪随机数发生器的种子，便可生成相应的伪随机序列，进而得到秘密信息在图像中的嵌入位置。若对应位置的像素值为奇数，则提取出信息1；反之，则提取出信息0。

不难看出，提取的过程实际上与替换隐藏的提取过程完全一样，那是因为本文的嵌入方式对图像像素LSB的修改情况和替换LSB隐藏是一样的。

从预处理、信息嵌入和信息提取的整个过程来看，本文算法的实现非常简单，即在信息嵌入时用一个巧妙的方法就达到了抵抗SPA攻击的目的，嵌入和提取部分的计算复杂度较传统LSB替换隐藏没有任何增加。

3 实验结果及分析

3.1 本文算法抗SPA攻击的能力

为验证本文对传统LSB嵌入方式的改进可以实现对SPA攻击的抵抗，实验对从groundtruth图像库中随机取出的593幅和文献[5]中列出的24幅实验图像中的10幅进行本文第3部分提出的预处理，将所有处理后进行SPA攻击得到的估计值小于门限值的600幅图像作为实验用图像。然后分别对该600幅图像进行不同比率的嵌入，嵌入比率依次为3%、5%、10%、20%、…、100%多种情况，嵌入的方式分别为传统的替换LSB与本文方法，都使用本文第3部分提到的随机间隔嵌入。为了提高嵌入信息的随机性，首先对嵌入信息进行加密[11]，然后对所有隐藏后的图像进行SPA攻击。表1列出了两种嵌入方式在不同嵌入率下的SPA估计值的平均值。

表1 本文方法较传统方法抵抗SPA攻击的改进

嵌入比率(%)	不同嵌入方式下SPA攻击估计值均值(%)	
	替换LSB嵌入	本文方法嵌入
3	3.44	0.16
5	5.03	0.17
10	10.87	0.22
20	20.19	0.31
30	30.27	0.39
40	40.57	0.50
50	50.74	0.61
60	61.02	0.65
70	70.97	0.78
80	81.23	0.83
90	89.92	0.88
100	98.53	0.94

由表1可知，SPA攻击针对传统的替换LSB嵌入有非常好的检测效果，估计的嵌入比率相当准确。但针对本文提取的嵌入方法却完全失效，对所有的图像均给出了没有隐藏的判决结果，汇总各种嵌入率的情况，SPA估计值的均值最大为0.009 4，低于门限值0.018。所以本文的方法可以成功抵抗SPA攻击。本文的实验程序用Visual C++6.0开发，在产生随机间隔时使用的是VC封装的随机函数，不具备很强的伪随机性。若对此进行改进，实验的效果还会有所提高，同时还可以提高算法的安全性。

3.2 本文算法抗RS攻击的能力

为验证本文对传统LSB嵌入方式的改进可以实现对RS攻击的抵抗，相同的实验用图像采用与上一实验和嵌入比率，实验结果如表2所示。

表2 本文方法较传统方法抵抗RS攻击的改进

嵌入比率(%)	不同嵌入方式下RS攻击估计值均值(%)	
	替换LSB嵌入	本文方法嵌入
3	3.57	0.85
5	5.43	0.97
10	11.03	0.99
20	21.47	0.98
30	31.81	1.02
40	41.90	1.08
50	52.15	1.111
60	62.63	1.114
70	71.98	1.24
80	82.41	1.29
90	90.57	1.67
100	97.92	1.99

通过该实验可以看出，本文方法对RS攻击也有很好的抵抗效果。

由于本文的嵌入方式破坏了LSB替换隐藏时造成的像素值对 $0 \leftrightarrow 1, \cdots, 254 \leftrightarrow 255$ 变换，所以本文方法对卡方类攻击也具有抵抗能力。

参 考 文 献

[1] WESTFELD A, PFITZMANN A. Attacks on steganographic systems[C]//Proceedings of the 3rd International Workshop on Information Hiding. Lecture Notes in Computer Science 1768, Berlin, Germany: Springer-Verlag, 2000, 61-76.

[2] FRIDRICH J, DU Rui, MENG Long . Steganalysis of LSB encoding in color images[C]//ICME2000. Multimedia and Expo. New York: IEEE press, 2000, 1279-1282.

[3] FRIDRICH J, GOLJAN M, DU Rui. Reliable detection of LSB steganography in grayscale and color image[C]// Proceedings of the ACM Workshop on Multimedia and Security, Special Session on Multimedia Security and Watermarking. Ottawa: [s.n.], 2001, 27-30.

[4] ZENG Wei, AI Hao-jun, HU Rui-min, et al. Steganalysis of LSB embedding in audio signals based on sample pair analysis[C]//Wireless Communications, Networking and Mobile Computing. Shanghai: [s.n.], 2007.

[5] DUMITRESCU S, WU Ao-lin, WANG Zhe. Detection of LSB steganography via sample pair analysis[J]. IEEE

Transactions on Signal Processing, 2003, 51(7): 1995-2007.
[6] 张 涛, 平西建. 空域LSB信息伪装的隐写分析及其对策[J]. 通信学报, 2003, 24(12): 156-163.
ZHANG Tao, PING Xi-jian. Steganalysis of spatial LSB-based steganographic algorithms and countermeasures [J]. Journal of China Institute of Communications, 2003, 24(12): 156-163.
[7] 罗向阳, 陆佩忠, 刘粉林. 一类可抵御SPA分析的动态补偿LSB信息隐藏方法[J]. 计算机学报, 2007, 30(3): 463 - 473.
LUO Xiang-yang, LU Pei-zhong, LIU Fen-lin. A dynamic compensation LSB steganography method defeating SPA[J]. Chinese Journal of Computers, 2007, 30(3): 463-473.
[8] LUO Xiang-yang, HU Zong-yun, YANG Can, et al. A secure LSB steganography system defeating sample pair analysis based on chaos system and dynamic compensation[C]// Advanced Communication Technology on the 8th International Conference. Phoenix Park: [s.n.], 2006.
[9] 田 源, 程义民, 谢于明, 等. 一种抗SPA分析的图像信息隐藏方法[J]. 中国科学技术大学学报, 2008, 38(12): 1376-1380.
TIAN Yuan, CHENG Yi-min, XIE Yu-ming, et al. Steganographic scheme for images against SPA steganalysis [J]. Journal of University of Science and Technology of China, 2008, 38(12): 1376-1380.
[10] 汪小帆, 戴跃伟, 茅耀斌. 信息隐藏技术-方法与应用[M]. 北京: 机械工业出版社, 2001: 124-125.
WANG Xiao-fan, DAN Yue-wei, MAO Yao-bin[M]. Information Hiding Technology-Methods and application. Beijing: China Machine Press, 2001: 124-125.
[11] WANG Hong, PENG Jian-hua, ZHOU Zheng-ou. Design of a new chaos circuit and its encryption to digital information[J]. Journal of Electronic Science and Technology of China, 2004, 2(4): 25-28.

编 辑 蒋 晓

(上接第746页)

[7] POPOVIC M R, GOLDENBERG A A. Modelling of friction using spectral analysis[J]. IEEE Transaction on Robotics and Automation, 1998, 14(1): 114-122.
[8] TAGHIRAD H D, BELANGER P R. Model1ing and parameter identification of harmonic drive systems[J]. J of Dynamic Systems, Measurement, and Control, 1998, 120(6): 439-444.
[9] TUTTLE T D, SEERING W P. A Nonlinear Model of a Harmonic Drive Gear Transmission[J]. IEEE Transaction on Robotics and Automation, 1996, 12(3): 368-374.
[10] LEMMER L, KISS B. Modeling, identification, and control of harmonic drives for mobile vehicles[C]// Proceedings of the IEEE 3rd International Conference on Mechatronics. Budapest: IEEE Press, 2006: 369-374.
[11] CHOI J J, HAN S I, KIM J S. Development of a novel dynamic friction model and precise tracking control using adaptive back-stepping sliding mode controller[J]. Mechatronics, 2006, 16(2): 97-104.
[12] JATTA F, LEGNANI G, VISIOLI, A. Friction compensation in hybrid force/velocity control of industrial manipulators[J]. IEEE Transaction Industry Electronics, 2006, 53(2): 604-613.

编 辑 张 俊

(上接第761页)

[14] 田 宏, 董爱杰. 基于向量矩阵的频繁项集挖掘算法[J]. 大连交通大学学报, 2008, 29(3): 74-77.
TIAN Hong, DONG Ai-jie. A frequent itemsets mining algorithm based on vector matrix[J]. Journal of Dalian Jiaotong University, 2008, 29(3): 74-77.
[15] 张忠平, 李 岩, 杨 静. 基于矩阵的频繁项集挖掘算法[J]. 计算机工程, 2009, 35(1): 84-86.
ZHANG Zhong-ping, LI Yan, YANG Jing. Frequent itemsets mining algorithm based on matrix[J]. Computer Engineering, 2009, 35(1): 84-86.

编 辑 漆 蓉