

文章编号: 1001-0920(2007)04-0423-05

一种可抵御 RS 统计分析的图像信息隐藏方案

罗向阳, 高山青, 刘 镔, 刘粉林

(解放军信息工程大学 信息工程学院, 郑州 450002)

摘要: 通过动态补偿隐藏信息后的图像, 给出一种可抵御 RS 分析的 LSB 隐藏方案. 该方案基于混沌系统产生随机序列选择嵌入位置并进行 LSB 嵌入, 对嵌入信息后的图像进行动态补偿, 补偿后的图像即使信息嵌入率接近于 100%, RS 方法得到的估计值仍将低于判决阈值, 从而作出错误判决. 混沌系统初值和动态补偿参数可进一步提高系统的安全性. 实验表明, 该方案可有效抵抗经典 RS 方法及其多种改进方法的分析.

关键词: 信息隐藏; LSB 隐藏; RS 分析; 混沌系统; 动态补偿

中图分类号: TP309

文献标识码: A

An image steganography scheme resisting RS statistical analysis

LUO Xiang-yang, GAO Shan-qing, LIU Bin, LIU Fen-lin

(Institute of Information Engineering, Information Engineering University, Zhengzhou 450002, China.

Correspondent: LUO Xiang-yang, E-mail: xiangyangluo@126.com)

Abstract: Through dynamically compensating the pixel values of the LSB embedded image, a novel LSB steganography method is presented against RS analysis. This scheme embeds message in the LSB plane of the carrier image randomly via chaotic system, then makes a dynamic compensation on the steg-image. Even though the embedding ratio is near 100% in the steg-image, such dynamic compensation can make RS steganalysis get a estimate value, which is lower than the threshold and will causes an incorrect judgement. Moreover, the initial value of the chaotic system and the selection parameters of the compensation are used to improve the security of steganography system. Experimental results show that this approach also can resist some other improved RS steganalysis methods availably.

Key words: Steganography; LSB embedding; RS steganalysis; Chaos system; Dynamic compensation

1 引言

近年来出现了许多针对图像空域 LSB (Least Significant Bits) 隐藏的分析方法, 能够比较精确地判断图像中是否含有 LSB 隐藏信息. 比较重要的有 χ^2 -分析方法^[1], RQP 分析方法^[2], RS 分析方法^[3], SPA 分析方法^[4]等. 其中, RS 分析方法通过统计图像中正则组和奇异组的数量来估计信息嵌入率, 当信息非顺序嵌入时可较为精确地估计隐藏长度. SPA 方法基于样本对进行统计分析, 当嵌入在 LSB 上的信息的比例大于 3% 时, 该方法能以相当高的精度估计出隐藏信息的长度. 文献[5]通过大量的实验评估了 RS 和 SPA 等分析方法的可靠性, 指出这两种方法是目前 LSB 隐藏分析方法中检测效果最好的方法.

事实上, 基于统计特性的分析方法大都是针对自然图像满足某些统计假设来设计的, 因此隐藏者为了避免隐藏行为被发现, 可以有意识地对嵌入信息后的图像进行调整, 使得载密图像仍然满足那些重要的统计特性. 如: 对 RS 分析方法, 文献[6]给出了一种通过对载体图像置乱后像素值随机加减 1 来嵌入信息, 并利用图像未嵌入信息的部分来调节 RS 统计度量的 SES 方法, 但遗憾的是该方法隐藏量一般不能超过 50%. 文献[7]通过选择适当的嵌入位置进行嵌入以抵抗 RS 攻击, 但其嵌入率至多为 20%. 文献[8]也提出了一种以一定比率加减 1 来进行随机嵌入的可抵抗 RS 分析的密写方法, 但该方法抵抗 RS 分析的能力强弱依赖于像素值加减 1 的比率选取.

收稿日期: 2005-11-16; 修回日期: 2006-03-21.

基金项目: 国家自然科学基金项目(60374004); 河南省杰出青年基金项目(0412000200); 河南省高校杰出科研人才创新工程项目(2001 KYCX008); 河南省科技攻关项目(0623021500).

作者简介: 罗向阳(1978—), 男, 湖北荆门人, 讲师, 博士生, 从事信息隐藏技术、图像处理等研究; 刘粉林(1964—), 男, 江苏溧阳人, 教授, 博士生导师, 从事信息安全技术、控制理论等研究.

本文基于RS方法的前提假设,给出了一种可抵御RS方法分析的图像信息隐藏方案,简记为RRS.该方案基于混沌系统产生的随机序列选择嵌入位置,进行空域LSB随机嵌入,并对嵌入信息后的图像进行动态补偿.进行像素值补偿的区域位置和形状可以自由选取,例如:矩形、圆形或者三角形区域.将混沌系统的初值和图像补偿区域的选择参数作为系统密钥的一部分,可提高系统的安全性.实验表明:即使图像中嵌入率接近100%,本文的方案也能有效抵抗RS方法的攻击.

2 RS分析方法简述

假定载体图像中像素取值属于一个集合 V ,如:对于8-bit灰度图像, $V = \{0, 1, \dots, 255\}$.利用描述函数 f 来考察图像空间相关性, f 表示一个实数 $f(v_1, v_2, \dots, v_n)$ 和由 n 个空间上连续的像素组成的像素组 $G = (v_1, v_2, \dots, v_n)$ 之间的对应关系.例如:用

$$f(v_1, v_2, \dots, v_n) = \frac{1}{n-1} \sum_{i=1}^{n-1} |v_{i+1} - v_i| \quad (1)$$

来衡量 G 的平滑度, G 中的噪声越多,判别函数 f 的值越大.LSB嵌入信息增加了图像的噪声, f 的值也将随之增加.LSB位嵌入过程可以用翻转函数 $F_1: 0 \leftrightarrow 1, 2 \leftrightarrow 3, \dots, 254 \leftrightarrow 255$ 描述.同理,定义一个LSB偏移翻转函数 $F_{-1}: -1 \leftrightarrow 0, 1 \leftrightarrow 2, \dots, 253 \leftrightarrow 254, 255 \leftrightarrow 256$; F_0 为恒等变换: $F_0(v) = v, \forall v \in V$.这三类翻转函数构成了翻转函数的集合 $F = \{F_1, F_0, F_{-1}\}$.

对一组像素 $G = (v_1, v_2, \dots, v_n)$,若 $f(F(G)) > f(G)$,称 G 是正则的;若 $f(F(G)) < f(G)$,称 G 是奇异的;若 $f(F(G)) = f(G)$,称 G 是不变的.这里 $F(G)$ 是指将 F 运用到向量 $G = (v_1, v_2, \dots, v_n)$ 的各个分量中. M 是一个值为0,1的 n 元组,其形为 $[M(1), M(2), \dots, M(n)]$,则基于 M 的交换组 $F_M(G)$ 为

$$(F_{M(1)}(v_1), F_{M(2)}(v_2), \dots, F_{M(n)}(v_n)). \quad (2)$$

用 R_M 表示 F_M 作用后正则组占整个像素组的比率, S_M 表示 F_M 作用后奇异组占整个像素组的比率;类似地,用 R_{-M} 表示 F_{-M} 作用后正则组的比率, S_{-M} 表示 F_{-M} 作用后奇异组的比率.这里 $-M$ 由 M 中的各个元素取负数得到.如 $M = (0, 1, 1, 0)$,则 $-M = (0, -1, -1, 0)$.

RS分析方法基于自然图像具有下列属性:

$$E\{R_M\} = E\{R_{-M}\}, E\{S_M\} = E\{S_{-M}\}, \quad (3)$$

并由此得到

$$2(d_1 + d_0)z^2 + (d_{-0} - d_{-1} - d_1 - 3d_0)z + d_0 - d_{-0} = 0, \quad (4)$$

其中

$$\begin{aligned} d_0 &= R_M(p/2) - S_M(p/2), \\ d_1 &= R_M(1-p/2) - S_M(1-p/2), \\ d_{-0} &= R_{-M}(p/2) - S_{-M}(p/2), \\ d_{-1} &= R_{-M}(1-p/2) - S_{-M}(1-p/2). \end{aligned}$$

进而得到信息的嵌入比率 $p = z/(z-1/2)$,其中 z 是方程(4)中绝对值较小的根.

3 RRS方法原理

RRS方法的基本原理是:通过对嵌入后的图像进行像素值补偿,使得补偿后的图像仍能保证式(3)成立,从而使得RS分析方法失效.

文献[4]讨论了RS方法与SPA方法的相关性,指出式(3)等价于

$$E\{|X|\} = E\{|Y|\}. \quad (5)$$

其中: $| \cdot |$ 表示多重集的势;多重集 X 和 Y 的定义如下:

$$X = \{X_i\}_{i=1}^{2^b-1}, Y = \{Y_i\}_{i=1}^{2^b-1}, \quad (6)$$

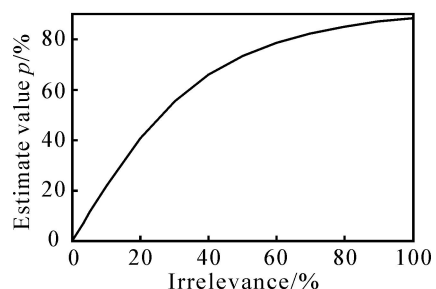
X_i 和 Y_i 都是由一系列二元组 (u, v) 构成的多重集; u 和 v 是两个相邻像素的值, $0 \leq u, v \leq 2^b - 1$; b 是表示每个样本值的比特数,且有 $|u - v| = i$,即相邻像素对中的两个像素的值差为 i ; (u, v) 中较大的元素值为偶数的样本对属于 X ,较大的元素值为奇数的样本对属于 Y .

一般地,图像在LSB隐写后, $|X|$ 与 $|Y|$ 的大小将发生偏离,本文用 $\frac{||Y| - |X||}{|Y| + |X|}$ 来表征嵌入

信息后 $|Y|$ 和 $|X|$ 的偏离度,记为 δ .图1(b)给出了使用RS分析方法时, δ 的变化对原始图像Lena图



(a) 原始Lena图像



(b) 偏离度对检测结果的影响

图1 Lena图像在不同嵌入率下的偏离度

像(见图 1(a)) 检测结果的影响,显示了 LSB 嵌入率的估计值 p 与偏离度 d 之间的关系.

RRS 方法就是通过对载密图像进行像素值补偿来修正 $|X|$ 与 $|Y|$ 的偏离,使得补偿后图像的 $|X|$ 与 $|Y|$ 仍然十分接近,并使 RS 方法检测得到的估计值为一个低于判决门限的较小值,从而使 RS 方法检测失效.

4 RRS 方案

记载体图像为 I ,嵌入信息为 S ,嵌入信息后得到的图像为 I' ,对 I' 进行像素值补偿后得到的图像为 I'' .设图像的宽和高分别为 $W = M, H = N, M$ 和 N 分别为图像水平和垂直方向上的像素的数量. RRS 方案首先进行 LSB 信息的嵌入,然后对图像的部分区域进行整体像素值补偿.在进行补偿之前需要对载密图像进行简单的预处理. RRS 方案的结构示意如图 2 所示,具体的嵌入算法、补偿算法和提取算法如下.

4.1 嵌入算法

步骤如下:

- 1) 图像索引. 将载体图像 I 的像素按由左及右、由上至下的顺序进行索引,记为 $c_1, c_2, \dots, c_{M \times N}$.
- 2) 生成随机序列. 依据初始密钥 K ,利用加扰数字混沌系统生成一个随机序列 $k_1, k_2, \dots, k_{M \times N}$.
- 3) 选择嵌入位置. 信息的嵌入位置根据混沌系统产生的随机序列选择.
- 4) 嵌入 LSB 信息. 用信息比特替换对应位置的 LSB 位,得到载密图像 I' .

4.2 补偿算法

4.2.1 补偿预处理

由于在补偿算法中要将部分图像的像素值加 1,图像中像素值为 255 的像素其像素值加 1 后为 256,这超出了 8 位比特所能表示的范畴.因此,需要对含有值为 255 像素的图像进行预处理.具体操作为:扫描载密图像的所有像素,将像素值为 255 的修改为 253.显然,这样的修改对图像的影响很小,不会引起视觉上的差异,同时既保证了相邻像素之间差值的奇偶性不变,又不影响提取信息的正确性.若采用对像素值减 1 的方法对图像进行补偿,则应

进行相应的预处理(如:将 0 值像素改为 2 值像素),使用于嵌入的载体不含 0 值像素.

4.2.2 动态补偿方法

用 $|*|$ 表示嵌入信息后的图像中多重集 $*$ 的势, $|*|$ 表示嵌入信息后的图像进行补偿后多重集 $*$ 的势.图像进行 LSB 嵌入信息后 $|Y|$ 和 $|X|$ 的偏离度将变大,补偿算法的目的是消除这种变化.假设像素值的差为 i 的相邻像素对在嵌入信息后是均匀分布的,那么将载密图像的一半紧密相连的像素的值均加上 1,像素值的差为 i 的相邻像素对的总数量几乎不变(只在分界线附近有相当微小的变化),而由于像素值整体加 1,像素值的奇偶性发生了互换.对整幅图像中的 $|Y_i|$ 而言,其大小减少了约 $|Y_i|/2$,但增加了约 $|X_i|/2$,从而,修改像素值后得到的 $|Y_i| = |Y_i|/2 + |X_i|/2$.同理, $|X_i| = |Y_i|/2 + |X_i|/2$.因此修改一半图像的像素值后, $|Y_i| = |X_i|$.RS 方法利用方程 (4) 得到的 p 将很小.

上述情况是理想的,实际上图像在嵌入信息后,尤其是嵌入的信息量比较大时,像素值差为 i 的相邻像素对的分布可能变得不均匀.如果仍对一半图像的像素值进行整体加 1 操作,得到的 $|Y|$ 和 $|X|$ 的大小仍可能有较大的差异,RS 方法得到的估计值可能大于设定的判决门限,从而 RS 方法仍将作出图像中含有隐藏信息的正确判断.如当 Lena 图像中隐藏了 90% 的信息时, $p = 0.1873$,RS 方法的估计值 $p = 91.77\%$.补偿图像一半的像素值后得到的 $p = 0.0094$, p 值为 5.02%,当判决门限低于该估计值时,RS 仍将正确地判决图像中含有隐藏信息.这意味着简单地将图像一半的像素值加 1 是不够的,应根据具体的图像对其补偿范围进行动态选择.

一个简单的选择方法是行遍历.设图像的补偿范围为 $0 \sim j$ 行, $1 \leq j \leq N - 2$ (当 j 为 $N - 1$ 时,整个图像的像素值均加 1,只是 X_i 和 Y_i 发生了交换,但偏离度将不发生变化). j 从 1 开始,对从第 $0 \sim j$ 行内的所有像素值加 1,统计并计算相应的 p_j ,然后 j 依次递加 1,得到 $N - 2$ 种情况下的 p_j ,选取最

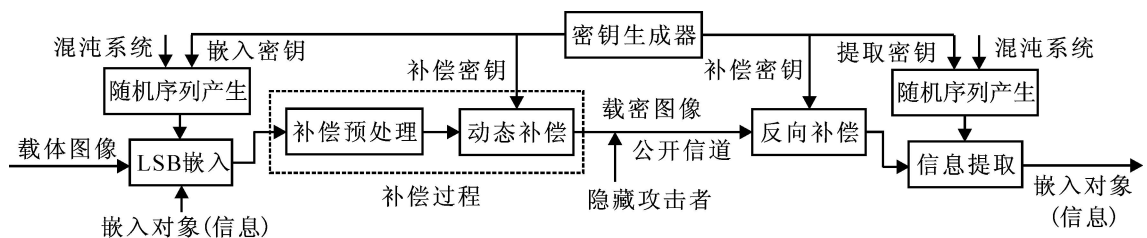


图 2 RRS 方案模型

小的偏离度 \min , 则图像的补偿范围为 \min 对应的 $0 \sim j$ 行的范围。

设判决门限为 2%, 含有 90% LSB 嵌入信息的图像 Lena 经过行遍历方式下的补偿后, 在 $j = 241$ 时找到最小的偏离度为 2.3736×10^{-4} , 用 RS 方法进行分析得到的嵌入比率值 $p = 0.64\%$, 该值远小于判决门限值, 因此, RS 分析将作出 Lena 图像中不存在隐藏信息的错误判断。对于含有 100% LSB 隐藏信息的 Lena 图像, 经过上述方式下的动态补偿后, 使用 RS 方法得到的检测值为 0.83%, 也低于判决门限。

4.3 提取算法

提取是补偿过程和嵌入过程的逆过程。首先根据补偿密钥 K , 将相应范围内的像素值进行减 1 操作, 从而将图像 I 恢复为补偿前的图像 I' ; 然后将 I' 的像素按由左及右、由上至下的顺序索引为 $c_1, c_2, \dots, c_{M \times N}$, 再根据嵌入密钥 K , 利用嵌入算法中给出的混沌系统生成相应的随机序列 $k_1, k_2, \dots, k_{M \times N}$; 最后在图像中找到和随机序列中相应位置的像素, 并从它们的 LSB 位上提取出嵌入的信息。

5 实验结果与分析

RRS 方法首先利用数字混沌产生的随机序列确定进行 LSB 嵌入的像素位置。实验中采用文献 [9] 提出的一种加扰数字混沌系统。该系统采用加扰和扩散的方法来改善数字化混沌系统的动力学特征退化, 具有长周期、随机性好等动力学特性, 采用该系统使得隐藏系统具有更高的安全性。该混沌系统描述如下^[9]。

考虑如下一个具有 $[0, a], [a, b], [b, 1 - a], [1 - a, 1]$ 4 个子区间的一维分段线性混沌映射:

$$g(x) = \begin{cases} 4x, & 0 \leq x < a; \\ 2 - 4x, & a \leq x < b; \\ 4x - 2, & b \leq x < 1 - a; \\ -4x, & 1 - a \leq x \leq 1. \end{cases} \quad (7)$$

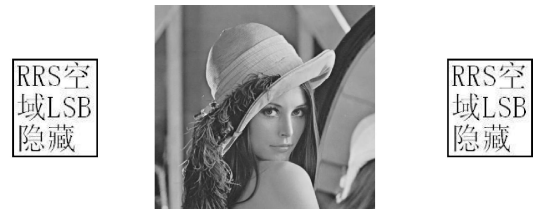
选择对 $g(x)$ 定义区间的第 3 子区间 $c_3 = [b, 1 - a]$ 进行扩散, 将片段 c_3 按照 $e:1 - e$ 的比例分成两段 $c_{31} = [b, b + e/r], c_{32} = [b + e/r, 1 - a]$, e 为扩散系数, r 为常量, x 为初值。取 $a = 0.25, b = 0.5, r = 4$, 按照选择性扩散的扰动算法形成新的分段线性混沌映射

$$f(x) = \begin{cases} g(x), & x \in c_3; \\ g\left(\frac{4}{2e}(x - 0.5)\right), & x \in c_{31}; \\ g\left(\frac{x - (0.5 + e/4)}{1 - e} + 0.75\right), & x \in c_{32}. \end{cases} \quad (8)$$

其中: $e \in (0, 1)$ 为扩散系数, $x \in (0, 1)$, 其初值为 x_0 。算法中 e 和 x 的取值均为实数。构造混沌序列时, 根据初始密钥 K 即可得到 x_0 和 e 。

5.1 隐藏与提取实验

对图像 Lena 进行实验, 实验结果如图 3 所示。可以看出, 采用 RRS 方法嵌入信息前后, Lena 图像视觉效果良好, 且能正确提取出嵌入信息。



(a) 秘密信息 (b) 嵌入信息的图像 (c) 提取信息

图 3 秘密信息的嵌入与提取

5.2 RRS 方法用于典型图像的实验

为验证 RRS 方法的可靠性, 首先对一些典型的图像进行了隐藏与分析实验。实验用图共 24 幅标准灰度图像。每幅图像考虑嵌入比率为 3%, 5%, 10%, 20%, ..., 90% 等多种情况, 所有图像中采用本文给出的 LSB 嵌入和加 1 补偿算法, 动态补偿中图像的补偿范围采用 4.2.2 节中的方法选择。判决门限值设为 2%, 表 1 给出了这 24 幅含有 LSB 隐藏信息的图像动态补偿前后, 利用 RS 方法进行分析得到的嵌入比率的平均估计值。

表 1 动态补偿对 RS 分析方法的结果影响 %

嵌入比率	检测结果均值	
	补偿前	补偿后
3	3.33	0.02
5	5.26	0.03
10	10.89	0.06
20	21.14	0.11
30	31.30	0.04
40	41.28	0.06
50	51.56	0.10
60	61.64	0.11
70	71.33	0.04
80	81.47	0.06
90	89.75	0.10
99	94.36	0.13

由表 1 可知, 按照 4.2.2 节描述的方法选择图像补偿范围后, RS 方法得到的隐藏信息比率的估计值大大减小, RS 的检测结果均值最大仅为 0.13%, 远低于判决门限。

5.3 平均方块间隔选择补偿区域对 RRS 方法性能的影响

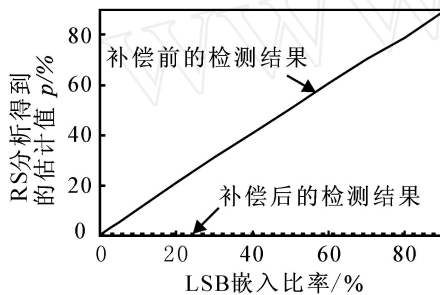
显然, 图像的补偿区域可以自由选取, 可以是矩

形,也可以选择一块(或多块)其他形状的区域,但补偿区域的选择可能会对补偿的效果产生影响.动态补偿的目的是保证得到某种补偿方式下较小的,从而使 RS 分析得到一个较小的隐藏信息比率估计值 p .

本文对采用平均间隔方块方式的补偿进行了实验.实验图像采用与上节相同的图像组,在图像中选择若干块 $i \times i$ 区域作为图像的补偿范围,其中 $32 \leq i \leq 128$,如图 4(a) 所示. i 的大小根据补偿后得到的各个偏离度中最小的偏离度 \min_i 来确定.图 4(b) 给出了采用平均间隔方法选择图像补偿范围后对 RS 方法的影响.



(a) 平均间隔法选取图像补偿区域



(b) Lena 图像采用平均间隔法补偿前后 RS 检测结果

图 4 补偿区域的选择对隐藏算法性能的影响

由图 4(b) 知,补偿区域采用平均间隔块的方式,即使在嵌入率高达 90% 的情况下,进行像素补偿后,RS 分析得到的隐藏比率仍然低于判决阈值.因此,隐藏方案仍能抵御 RS 方法的分析.

5.4 RRS 方法对其他分析方法的抵御能力测试

为进一步检测本文方法抵抗 X^2 -统计攻击、经典 RS 及其改进方法分析的能力,选用 2 000 幅图像(来自数码相机)进行了实验.首先,在这些图像中以随机嵌入的方式嵌入 10%、50% 和 90% 的 LSB 信息;然后对这 3 组图像进行动态补偿,并对补偿后的图像利用上述各种分析方法分别进行检测.其中,RS 的多种改进方法来自于文献 [1, 5, 10],这些方法采用了相关差分、优化掩码或最小二乘等手段,检测精度和可靠性比传统方法有一定程度的提高.实验结果表明,RRS 方法能有效地抵抗这些检测方法的

分析.

6 结 语

本文首先基于一个改进的混沌系统产生随机数,利用该随机数完成信息 LSB 嵌入;然后,通过对简单的空域 LSB 隐藏信息后的图像进行补偿预处理和动态补偿操作,给出了一种可有效抵御 RS 分析的 LSB 信息隐藏方法.混沌系统的初值和动态补偿区域的选择参数作为密钥的一部分,可进一步提高隐藏系统的安全性.文中用两种易于实现的补偿方式,即行扫描和随机间隔块的方法,进行了动态补偿实验.实验结果表明,本文方案对 X^2 -统计攻击、经典 RS 及其多种改进方法具有较强的抵御能力.

参考文献(References)

- [1] Westfeld A. Detecting low embedding rates[C]. Proc Information Hiding Workshop. Berlin: Springer-Verlag, 2002: 324-339.
- [2] Fridrich J, Du R, Meng L. Steganalysis of LSB encoding in color images[C]. Proc IEEE Int Conf on Multimedia and Expo. New York, 2000, 3: 1279-1282.
- [3] Fridrich J, Goljan M. Practical steganalysis of digital images — State of the art [C]. Security and Watermarking of Multimedia Contents. San Jose, 2002, : 1-13.
- [4] Sorina Dumitrescu, Wu XL, Wang Z. Detection of LSB steganography via sample pair analysis[J]. IEEE Trans on Signal Processing, 2003, 51(7): 1995-2007.
- [5] Andrew D Ker. Improved detection of LSB steganography in grayscale image [C]. Proc the 6th Information Hiding Workshop. Berlin: Springer-Verlag, 2004: 97-115.
- [6] Jeong Jae Yu, Jae Won Han, Kwang Su Lee, et al. A secure steganographic scheme against statistical analyses [C]. IWDW 2003. Berlin: Springer-Verlag, 2004: 497-507.
- [7] 吕述望, 陈庆元, 刘振华, 等. 对 RS 攻击的分析及抗 RS 攻击的隐写算法[J]. 中山大学学报, 2004, 43(增 2): 5-9.
(Lü S W, Chen Q Y, Liu Z H. Studying RS steganalysis and a steganographic algorithm which can resist this steganalysis[J]. J of Zhongshan University, 2004, 43(S2): 5-9.)
- [8] 张新鹏, 王朔中, 张开文. 抗统计分析的 LSB 密写方案 [J]. 中国图像图形学报, 2003, 8(9): 1055-1060.
(Zhang X P, Wang S Z, Zhang K W. A novel LSB steganography scheme against statistical analysis[J]. J of Image and Graphics, 2003, 8(9): 1055-1060.)

(下转第 435 页)

方法所实现的算法复杂度仍然较高,需要进一步简化算法。同时,本系统是一个模型系统,要建立起一个完整高效的、有实用价值的网络入侵检测系统,仍需要进行大量的研究工作。

参考文献(References)

- [1] 诸葛建伟,王大为,陈昱,等. 基于 D-S 证据理论的网络异常检测方法[J]. 软件学报, 2006, 17(3): 463-471. (Zhuge J W, Wang D W, Chen Y, et al. A network anomaly detector based on the D-S evidence theory[J]. J of Software, 2006, 17(3): 463-471.)
- [2] 杨辉华,王行愚,王勇,等. 基于 KPLS 的网络入侵特征抽取及检测方法[J]. 控制与决策, 2005, 20(3): 251-256. (Yang H H, Wang X Y, Wang Y, et al. KPLS approach for network intrusion feature extraction and detection[J]. Control and Decision, 2005, 20(3): 251-256.)
- [3] Le J, Ghorbani A. Network intrusion detection using an improved competitive learning neural network[C]. Proc of the 2nd Annual Conf on Communication Networks and Services Research. Fredericton: CA Press, 2004: 190-197.
- [4] Zhang C L, Jiang J, Mohamed Kamel. Intrusion detection using hierarchical neural networks [J]. Pattern Recognition Letters, 2005, 26(6): 779-791.
- [5] Cannady J. Neural networks for misuse detection: Initial results[C]. Proc of Recent Advances in Intrusion Detection '98 Conf. Louvain-la-Neuve: CA Press, 1998: 31-47.
- [6] Bivens A, Palagiri C, Smith R, et al. Network-based intrusion detection using neural networks[C]. Proc of Intelligent Engineering Systems through Artificial Neural Networks. NY: IEEE Press, 2002: 579-584.
- [7] Campbell W. Traditional indications and warnings for host based intrusion detection, indication and warning methodology [C]. Proc of CERT Conf '99. West Point: CA Press, 1999: 232-236.
- [8] Feng Y, Wu K G, Wu Z F, et al. Intrusion detection based on dynamic self-organizing map neural network clustering [C]. Proc of the 2nd Int Symposium on Neural Networks. Chongqing: Springer LNCS, 2005: 428-433.
- [9] Ramadas M, Ostermann S, Tjaden B. Detecting anomalous network traffic with self-organizing maps [C]. Proc of Recent Advance in Intrusion Dectcion 2003. Pittsburgh: FL Press, 2003: 46-55.
- [10] Pasemann F. A simple chaotic neuron[J]. Physical D, 1997, 104(2): 205-211.
- [11] Otey M, Parthasarathy S, Ghoting A, et al. Towards NIC based intrusion detection [C]. Proc of the 9th ACM SIGKDD Int Conf on Knowledge Discovery and Data Mining. Washington D C: VA Press, 2003: 723-728.
- [12] Cannady J. Artificial neural networks for misuse detection [C]. Proc of 1998 National Information Systems Security Conf. New York: IEEE Press, 1998: 443-456.
- [13] 张若青,裘丽华. 基于动态神经网络的液压伺服系统故障检测[J]. 机械工程学报, 2002, 38(3): 46-49. (Zhang R Q, Qiu L H. Fault detection of hydraulic servo-system based on dynamic neural network [J]. Chinese J of Mechanical Engineering, 2002, 38(3): 46-49.)
- [14] 姚羽,高福祥,于戈. 基于混沌神经元的延时滥用入侵检测模型[J]. 电子学报, 2004, 32(8): 62-65. (Yao Y, Gao F X, Yu G. The application of chaotic neural network to misuse detection [J]. Acta Electronica Sinica, 2004, 32(8): 62-65.)
- [15] Cunningham R, Lippmann R, Fried D, et al. Evaluating intrusion detection systems without attacking your friends [C]. Proc of 3rd Conf and Workshop on Intrusion Detection and Response. San Diego: CA, 1999: 35-42.
- [16] 姚羽,高福祥,于戈. 基于 ROC 曲线的入侵检测评估方法[J]. 通信学报, 2005, 26(1A): 113-115. (Yao Y, Gao F X, Yu G. IDS evaluation approach based on ROC curves [J]. J of China Institute of Communications, 2005, 26(1A): 113-115.)

(上接第 427 页)

- [9] 刘镇,张永强,刘粉林. 一种新的数字化混沌扰动方案[J]. 计算机科学, 2005, 32(4): 71-74. (Liu B, Zhang Y Q, Liu F L. A new scheme on perturbing digital chaotic systems [J]. Computer Science, 2005, 32(4): 71-74.)
- [10] Luo X Y, Liu B, Liu F L. Improved RS method for detection of LSB steganography[C]. Proc the 2005 Int Conf on Computational Science and Its Applications. Berlin: Springer-Verlag, 2005: 508-516.
- [11] Lu P Z, Luo X Y, Tang Q Y. An improved sample pairs method for detection of LSB embedding[C]. Proc the 6th Information Hiding Workshop. Berlin: Springer-Verlag, 2004: 116-128.