蜜网系统在检测新型Rootkit中的应用

涂溢彬[1,2],饶云波[1,3],廖 云[2],周明天[1]
(1.电子科技大学 计算机学院,四川 成都 610054;
2.东方电机股份有限公司,四川 德阳 618000;
3.成都东软信息技术学院,四川 成都 611844)

摘 要:文中对Rootkit的攻击原理进行分析,提出一种检测和分类Rootkit类型的新方法,提供给系统管理员和安全研究人员分析Rootkit特征的能力。同时研究了蜜网系统的体系结构及关键技术,并提出了蜜网系统在检测新型Rootkit中的一种应用,收集攻击者入侵后的活动数据并进行分析。所设计的系统在检测新型Rootkit方面运行良好。

关键词:网络安全;蜜网;安全策略;黑客
中图分类号:TP392 **文献标识码**:A **文章编号**:1673-629X(2008)01-0181-04

Honeynet System Applied in New Pattern Rootkit

TU Yi-bin[1,2],RAO Yun-bo[1,3],LIAO Yun[2],ZHOU Ming-tian[1]
(1.School of Computer Sci. & Eng.,Univ. of Electronic Sci. & Tech. of China,Chengdu 610054,China;
2.Dongfang Electrical Manchinery Co.,Ltd,Deyang 618000,China;
3.Neusoft Institute of Information,Chengdu 611844,China)

Abstract:Conducts an analysis about the fundamentals of Rootkit's attacks,comes up a new method of testing and grouping Rootkit's categories,offers the capacity of analyzing the Rootkit to the system managers and security researchers. Meantime,researches the structure of honeynet system and the key technology,and presents an application when the honeynet is testing a new of Rootkit,collects the moving data after the hacker invaded and conducts an analysis. The designed system runs well in the aspect of testing the new type of Rootkit.

Key words:network security;honeynet;security policy;hacker

0 引 言

随着计算机在各行各业应用的深入和普及,已经在各行各业得到广泛应用,其中包括政府、军队、银行等敏感部门。大量信息在计算机中存储和网络中传输,保证网络的安全已经成为国家安全的重要组成部分。同时针对网络攻击的频繁性和复杂性。传统的信息安全技术如防火强、IDS系统、访问控制、加密传输等,大都采用的是被动的安全策略,只有当黑客攻击行为发生后,才能对其被动地防御。

目前比较广泛使用的一种攻击技术是Rootkit,存在于Linux,Solaris和Windows等各种操作系统上[1],能以超级用户身份访问系统,同时在被攻击的系统上清除攻击痕迹,隐藏其攻击行为[2,3]。Rootkit的类型主要有:应用程序级Rootkit,系统工具级Rootkit和内核级Rootkit。内核级Rootkit是计算机系统安全领域最近出现的一种攻击方法。现在主要有两种方法来检测被入侵系统:一种是运用特征分析法;另一种是比较法。常见的检测方式有[4]:用现有的GPL工具检测Rootkit,维护系统完整性的GPL工具,黑盒分析法检测Rootkit等。但是现有的Rootkit检测技术和检测方法只能判断系统中是否安装某种已知Rootkit[5]。这些技术和方法只能指出系统被Rootkit感染,但无法确定它是哪种类型的Rootkit。文中研究提出一种方法来检测新型Rootkit和已知Rootkit的修改版本,并通过搭建蜜网系统检测Rootkit,分析和分类攻击者编写的各类Rootkit的漏洞利用特征,其目标是提供给计算机安全人员一种方法来识别和分析Rookit的类型。

收稿日期:2007-03-29
基金项目:四川省教育科研资助项目(2004B016)
作者简介:涂溢彬(1968-),男,四川射洪人,高级工程师,硕士研究生,研究方向为软件工程、信息安全;周明天,教授,博士生导师,研究方向为计算机网络、分布对象技术、中间件技术、并行分布处理、网络与信息系统安全等。

1 Rootkit的攻击原理

从攻击者的角度出发,分析一些可能被Rootkit使

用的攻击方法。文中重点分析内核级 Rootkit 的攻击目标:系统调用函数、系统调用表、系统调用入口函数、中断描述符表。

1.1 攻击系统调用函数

Linux 中所有的系统调用在内核中都由一个函数来实现,这些函数的名字通常都以 sys_ 开头,称为系统调用函数。内核级 Rootkit 可以修改这些系统调用函数,使得它们可以执行 Rootkit 提供的恶意代码。目前还没有出现这种类型的 Rootkit,但在实现上是可行的,分析如下:

所有的系统调用函数符号都被内核输出,因此可加载内核模块 LKM 可以获得这些符号地址。LKM 形式的 Rootkit 知道系统调用函数的地址后,可以修改系统调用函数的指令代码,使得在这个系统调用函数中调用 Rootkit 提供的恶意代码。

1.2 攻击系统调用表

攻击系统调用表是内核级 Rootkit 最常用的一种方法,主要有下面两种类型:修改系统调用表的内核级 Rootkit 和重定向系统调用表的内核级 Rookit。

1.2.1 修改系统调用表

这种类型的 Rootkit 修改位于系统调用表中的一些系统调用函数地址,它利用 Linux 操作系统中的特性可加载内核模块(LKM)[6],把系统调用表中的一些系统调用函数地址重定向到含有恶意代码的系统调用函数地址[7]。可加载内核模块(LKM)也适用于各类 UNIX 操作系统[6]。替换的系统调用函数可以用做隐藏文件和进程等各种功能。

1.2.2 重定向系统调用表

这类内核级 Rootkit 重定向把系统调用中断处理程序(system_ call)中使用的系统调用表(sys_ call_ table)重定向到内核空间中一个新的系统调用表。新的系统调用表必然包含恶意的 sys_ call 系统调用函数的地址,以及一些未被修改的原始的 sys_ call 系统调用的函数地址。Linux 系统中设备/dev/kmem 提供了对当前运行的内存区域访问权限。如果能够准确定位内存空间,那么便有可能在运行时对内核内存进行覆盖,从而重定向系统调用表的内核级 Rootkit。攻击者通过创建新的系统调用表地址重写原始系统调用表地址来实现这个功能。这类 Rootkit 并不修改原始的系统调用函数地址,因此能够逃避当前检测内核内存空间系统调用表完整性的检测方法。

1.3 攻击系统调用入口函数

每一种实现方式都有一个系统调用入口函数,系统有两种调用实现方式:中断方式的入口函数为中断处理函数 system_ call;SYSENTER/SYSEXIT 方式的入口函数为 Sysenter_ entry。

内核级 Rootkit 通过修改两个系统调用入口函数(system_ call 和 Sysenter_ entry),可以实现各种攻击。攻击系统调用入口函数的内核级[8] Rootkit 既可以不修改系统调用表 sys_ call_ table,也不用重定向它,因此常规的检测系统调用表的方法检测不到这种内核级 Rootkit。这种攻击方法的典型实现有 Enyelkm。

1.4 攻击中断描述符表

Kad 提出了一种攻击中断描述符表的方法[9]。Rootkit 可以使用这种方法修改中断描述符表 IDT,重定向中断处理函数。

中断描述符表 IDT(Interrupt Descriptor Table)是一个有 256 个中断描述符的线性表。每个中断描述符对应一个中断号。当中断发生时,检测权限合法后,会调用这个中断处理函数。Rootkit 可以改变中断描述符的中断处理函数地址,执行 Rootkit 提供的中断处理函数[10]。

2 搭建蜜网系统检测新型 Rootkit

针对 Rootkit 的攻击原理,检测方法的关键组成部分是:需要一个被检测和分类的 Rootkit 的副本,文中将通过建立一个蜜网系统来实现这部分。使用蜜网系统除了能够收集研究所用数据,而且能够提升其所在网络的整体安全性[11]。在网络中搭建蜜罐系统能更有效保护网络,它作为防火墙和入侵检测系统的有效补充,克服了这些系统的固有缺点,同时还能够收集任何针对蜜网中主机的 Rootkit 数据。

2.1 蜜网系统体系结构及关键技术

蜜网系统是一个置于防 Dos 攻击的逆向防火墙后,用于捕捉出入数据的网络系统。逆向防火墙能够限制出入蜜网系统的恶意数据流量,因此这些数据流可被保留、捕捉及控制。任何类型的操作系统都可放置于蜜网系统内。在蜜网中使用的标准系统能够使攻击者错误地认为是一个真实的系统,其目的是有意让攻击者入侵,以便提供给系统管理员关于网络内存的漏洞信息[11]。通过以上分析,图 1 给出一个基本的蜜网基本体系结构。

蜜网体系结构具有三大关键技术:数据捕获、数据控制和数据分析,必须严格遵循这三个原则才可使蜜网系统成功运转。

①数据捕获即信息收集,必须收集所有出入蜜网系统的信息,即监控和记录攻击者在蜜网内的所有行为,最大的挑战在于要搜集尽可能多的数据,而又不被攻击者所察觉。

②数据控制是保护其他网络的计算机,避免其遭

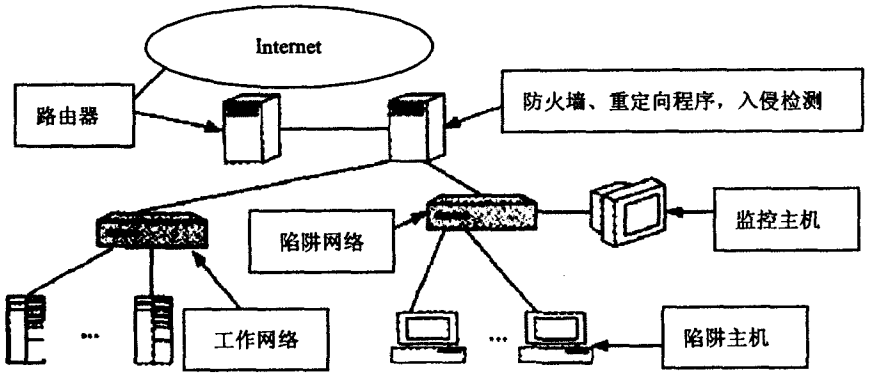

图 1　蜜网的基本体系结构

受来自蜜网中的计算机攻击,是对攻击者在蜜网中对第三方发起攻击行为进行限制的机制。最大的挑战是对攻击数据流进行控制而不能让攻击者怀疑,必须要给攻击者一定的自由度,数据控制的过程必须是自动化的,因为并不希望攻击者察觉到他所入侵的系统处于蜜网中[12]。

③数据分析则是对捕获到的攻击数据进行整理和融合,以辅助安全专家从中分析出这些数据背后蕴涵的攻击工具、方法、技术和动机,在分布式部署的蜜网体系中,存在着将多个蜜网中捕获数据进行安全地传输到一台中央服务器,并进行集中化分析的分布式数据收集需求。

2.2　搭建蜜网系统

当前有两种类型的蜜网系统能够在网络中使用,它们是 GEN I(第一代蜜网系统)和 GEN II(第二代蜜网系统)。选择哪一类蜜网系统取决于资源的可用性、需要检测的攻击者攻击类型和使用者对蜜网的整体使用经验等。

开始在本地网络安装的是第一代蜜网系统,为的是检测本地网络中遭受自动脚本类型攻击的机器,而不是收集 Rootkit 信息。之后,选择在本地网络中安装第二代蜜网系统,所用到的软件均为开源软件。蜜网系统的结构如图 2 所示。

3　数据分析

蜜网系统收集到的数据分别存储于监控系统两个不同位置,而 SNORT 的特征数据库存于一个 SQL 数据库中。这些警报特征可通过由计算机紧急响应组(CERT)开发的入侵检测分析控制台 ACID 获得。

SN-ORT 的入侵检测分析控制台的 Web 警报输出,结果如图 3 所示。

图中的数据是由 SNORT 的数据捕捉完成的,并存储在监视系统的日志文件中,SNORT 每天为该数据创建一个新目录。使用数据包分析器 Ethereal 来分析该数据,它是基于 libpcap 库的开源软件,可安装于大部分 Linux 操作系统中。通过分析数据,显示出蜜网中的所有数据报的发送和接受过程,它可以分析出一个数据报的源地址和目标地址、使用的协议、源端口和目标端口及数据报内容,它也可以分析出攻击者和蜜网中目标机器的某个 TCP 会话对应的所有数据报的内容。还可使用 Ethereal 分析蜜网捕获的数据来检测自动传播的蠕虫病毒。

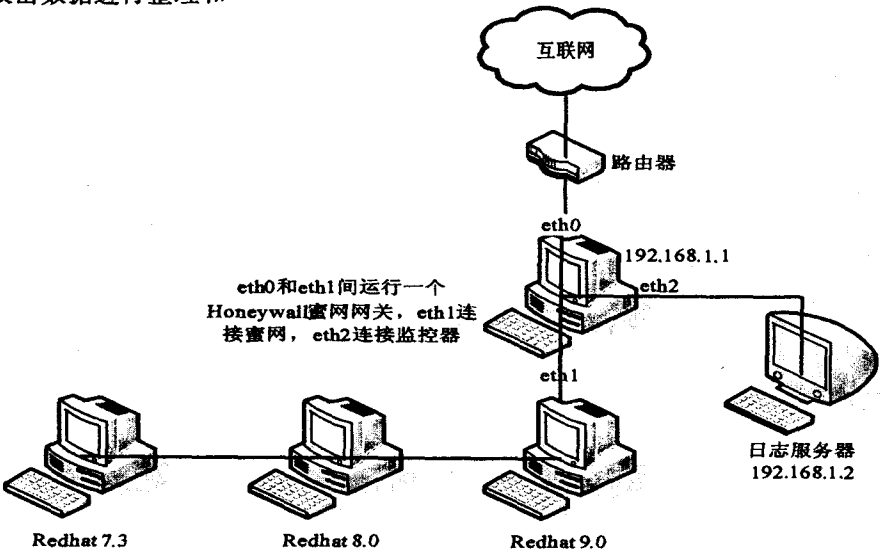

图 2　蜜网系统的结构图

Ethereal 的分析蜜网数据包的输出显示,如图 4 所示。

分析 SNORT 提供的数据是十分耗时的,每天至少花费 1 个小时来分析蜜网中三台计算机的数据。当蜜网被攻击或被攻击者入侵时,将花费更长时间分析数据,在目标系统上完成计算机入侵的取证工作。一小时的攻击过程需要四小时的分析工作,之后使用开源软件 X－CD－Roast[13]存储分析数据。

4　结束语

文中提出一种检测和分类 Rootkit 类型的新方法。提出的方法是提供给系统管理员和网络安全研究人员当系统遭受 Rootkit 感染时,及时分析出它属于已知

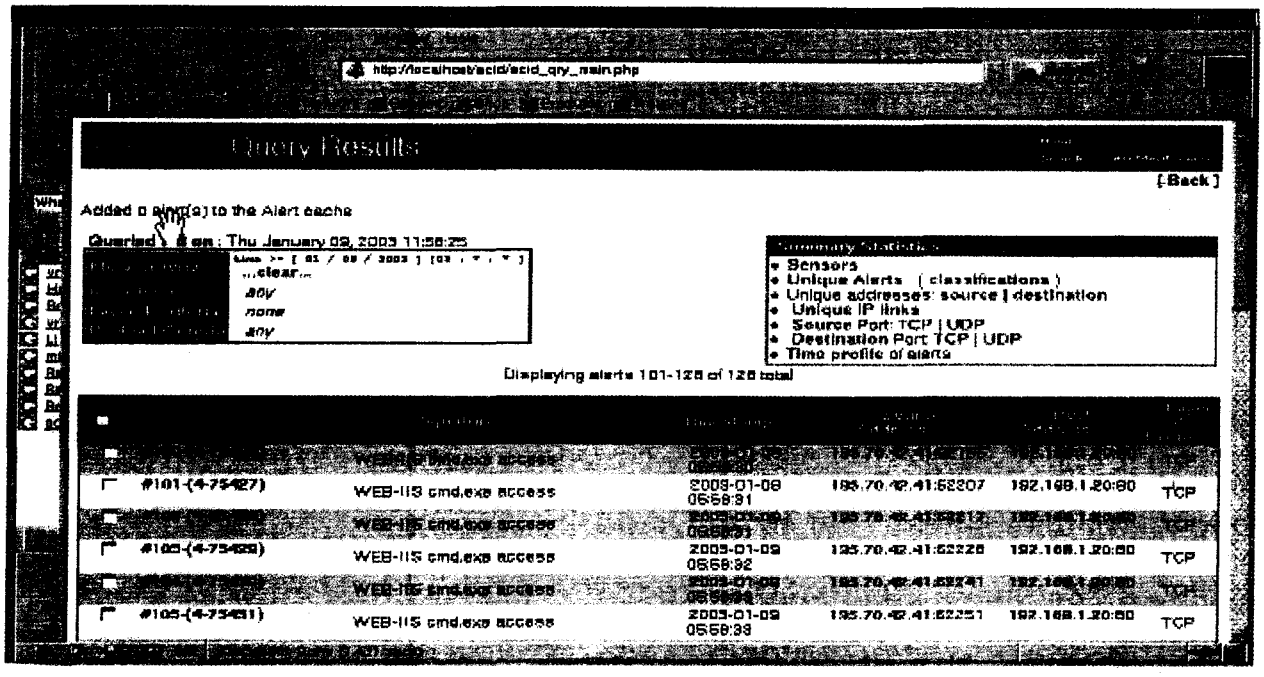

图 3 SNORT 的入侵检测分析控制台的 Web 警报输出

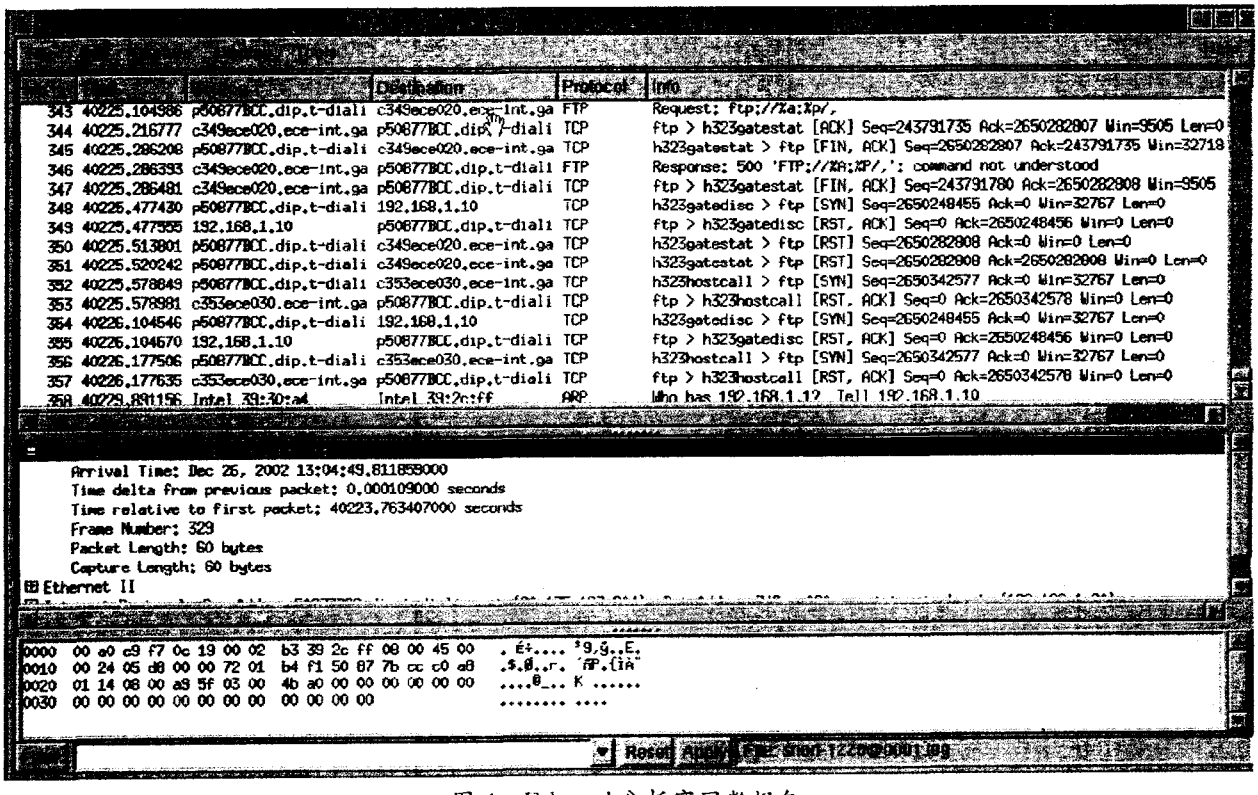

图 4 Ethereal 分析蜜网数据包

Rootkit 的修改版本还是新型 Rootkit。同时该方法提供给系统管理员和安全研究人员分析 Rootkit 特征的能力，使他们能采取最佳的防护和修复措施，也有助于检测和预防与 Rootkit 相关的安全问题。搭建蜜网系统用来收集攻击者入侵后的活动数据，能够捕获攻击者利用漏洞对目标系统进行的入侵活动并阻止攻击者使用蜜网中的系统攻击其他主机。

参考文献：

[1] O'Brien D. Recognizing and Recovering from Rootkit Attacks [J]. Sys Admin, 1996, 5(11): 8 - 20.

[2] Halflife. Abuse of the Linux Kernel for Fun and Profit[J]. Phrack Magazine, 1997, 7(50): 379 - 386.

（下转第 191 页）

```
/* 计算 TCP 校验和 */
libnet_do_checksum(buf,IPPROTO_TCP,TCP_H);
/* 发送包 */
libnet_write_ip(libnetsock,buf,TCP_H+IP_H)
```

4 结束语

使用协议分析技术,对 SMTP 协议进行解析,进而对邮件底层特性和邮件内容特性检测并发现邮件入侵,使邮件防护系统提高垃圾邮件的正确阻截率,解除邮件用户的烦恼,不受到有害邮件的攻击,对于维护网络的安全具有重要意义。就目前而言,对 SMTP 协议的分析的研究还比较少,从捕获到的邮件内容信息中找到敏感的信息,如果单纯采用简单的字符匹配,误判率高,所以对数据进行预处理、智能分词、快速索引等技术手段,将是以后研究的方向。

参考文献:

[1] 谢希仁. 计算机网络[M]. 大连:大连理工大学出版社,2004.

[2] Comer D E, Stevens D L. 用 TCP/IP 进行网际互连[M]. 林瑶,蒋慧轩译. 北京:电子工业出版社,1998.

[3] 周　婕. 协议分析在入侵监测系统中的应用[J]. 计算机与网络,2003(6):137－140.

[4] 蔡伟鸿,汤立浩. 电子邮件分析系统的设计[J]. 汕头大学学报,2004(2):75－78.

[5] Jonathan. Simple mail transfer protocol[S]. RFC821.1982.

[6] 胡吉明,刘少君. 状态协议分析技术在 TCP 中的应用[J]. 计算机技术与发展,2006,16(3):212－216.

(上接第 184 页)

[3] Hoglund G. A Real NT Rootkit, Patching the NT Kernel[J]. Phrack Magazine,1999,9(55):55－65.

[4] Warrender C, Forrest S, Pearlmutter B. Detecting intrusions using system calls alternative data models[C]//IEEE Symposium on Security and Privacy. Oakland: IEEE Computer Society,1999:133－145.

[5] 杨风召,朱扬勇,施伯乐. IncLOF:动态环境下局部异常的增量挖掘算法[J]. 计算机研究与发展,2004,41(3):477－484.

[6] Samhain Labs. The Basics－ Subverting the Kernel[EB/OL]. 2003－01. http://la－samha. de/library/rootkits /basics. html.

[7] Samhain Labs. Detecting Kernel Rootkits[EB/OL]. 2003－01. http://la－samha. de/library/rootkits/detect. html.

[8] 蒋盛益,李庆华. 基于引力的入侵检测方法[J]. 系统仿真学报,2005,17(9):2202－2206.

[9] Huang Zhengxue. Extensions to the k－Means Algorithm for Clustering Large Data Sets with Categorical Values[J]. Data Mining and Knowledge Discovery,1998,2(9):283－304.

[10] 伊胜伟,刘　旸,魏红芳. 基于数据挖掘的入侵检测系统智能结构模型[J]. 计算机工程与设计,2005,26(29):2464－2466.

[11] 黄　锦,李家滨. 防火墙日志信息的入侵检测研究[J]. 计算机工程,2001,26(9):115－117.

[12] 苏瑜睿,冯登国. 基于非层次聚类的异常检测模型[C]//中国计算机大会论文集. 北京:清华大学出版社,2005.

[13] 严晓光,锗学征. 聚类在网络入侵的异常检测中的应用[J]. 计算机系统应用,2005(10):78－80.

(上接第 187 页)

表 3　文中算法与其它算法的比较

	隐藏率(bits/Byte)(统计平均值)	信噪比(dB)(统计平均值)
文中算法	0.160	42.276
Thodi 算法	0.182	40.754
JPEG－LS 预测算法	0.364	31.270

7 结束语

文中结合线性预测和位操作,提出了一种新的简单易于实现的信息隐藏算法,具有较高的嵌入量和信噪比,能够无损提取隐藏信息。但图像不能无损提取,在传输的安全性和抗干扰,以及提取预测算法的预测准确度等方面是今后的研究重点。

参考文献:

[1] 付　兵. 一种增加 LSB 信息隐藏量的方法[J]. 长江大学学报:自然版,2006,3(4):73－75.

[2] Fridrich J, Goldjan M, Du R. Invertible authentication[C]// Proceedings of SPIE. San Jos, California:[s.n.],2001:197－208.

[3] Goldjan M, Fridrich J, Du R. Distortion－free data embedding[C]//Proceedings of the 4th Information Hiding Workshop. Pittsburg, PA:[s.n.], 2001:27－41.

[4] Thodi D M, Rodrfguez J J. Reversible watermarking by prediction－error expansion[C]//Proceedings of the 6th IEEE Southwest Symposium on Image Analysis and Interpretation. Lake Tahoe, Nevada:[s.n.],2004:21－25.

[5] 谢于明,程义民,王以孝,等. 基于线性预测的图像无损信息隐藏方法[J]. 计算机辅助设计与图形学学报,2006,18(4):585－591.