非结构去中心化的 P2P 网络 DDoS 攻击的防御研究*

许晓东[a], 李 刚[b], 杨 燕[b]
(江苏大学 a. 信息化中心; b. 计算机与通信工程学院, 江苏 镇江 212013)

摘 要: 针对非结构去中心化的 P2P 网络可能作为 DDoS 引擎而产生大规模的网络攻击,提出了一种基于人工免疫(AIS)的方法来对非结构去中心化的 P2P 网络中的恶意节点进行免疫处理。通过在非结构去中心化的 P2P 网络中的节点上构建人工免疫系统,利用抗体和抗原之间天然的亲和关系,以及抗体不断进化的特点,实时计算由返回查询消息的节点提供的资源信息而进行请求得到的请求结果状态序列与检测器中的对应节点的请求状态序列特征之间的亲和力,并检测出恶意节点。在 NS2 仿真平台上通过修改 GnuSim 插件,对非结构去中心化的 P2P 网络中节点的人工免疫系统进行模拟仿真,实验仿真验证了该方法的可行性,且能够有效地降低非结构去中心化 P2P 网络中恶意节点产生的 DDoS 攻击程度。

关键词: 非结构; 去中心化; 对等网络; 分布式拒绝服务; 人工免疫; 网络安全
中图分类号: TP311.135.4 **文献标志码**: A **文章编号**: 1001-3695(2012)12-4618-04
doi:10.3969/j.issn.1001-3695.2012.12.055

Study on defense of unstructured and uncentralized P2P network DDoS attacks

XU Xiao-dong[a], LI Gang[b], YANG Yan[b]
(*a. Information Center, b. College of Computer & Communication Engineering, Jiangsu University, Zhenjiang Jiangsu* 212013, *China*)

Abstract: As unstructrured and uncentralized P2P network might be the engine of DDoS attacks, this paper proposed a theory of using AIS to isolate the malicious node from the P2P network. With AIS in a node and the nature relationship between antigens and antibodies and the continue evolution of antibodies, the node could detect malicious node by calculating the appetency of request result cycle queue of the node that returned resource information and the node's detector in real time in the unstructured and uncentralized P2P network. It did the experiment on the NS2 simulation platform by modifying the GnuSim plugin with AIS in the node of unstructured and uncentralized P2P network, and verified the model's feasibility. And the experiment indicates that the method can effectively reduce the degree of DDoS caused by malicious node in the unstructured and uncentralized P2P network.

Key words: unstructured; uncentralized; P2P network; DDoS; AIS; network security

在 Internet 快速发展的过程中,P2P 网络结构也随之不断变化。从传统的有结构有中心到有结构非中心,再到现在的非结构去中心化,P2P 网络的参与者散布在网络中的每一个角落。然而,隐藏在这种非结构去中心化的 P2P 网络中的恶意节点可以利用 P2P 协议本身的漏洞,将整个该 P2P 网络作为 DDoS 攻击的引擎[1],由此引发的非结构去中心化的 P2P 网络 DDoS 攻击将对互联网构成一个巨大隐患。传统防范 P2P 网络的 DDoS 攻击主要是针对具有结构化或者具有中心化的 P2P 网络,且大多数都是基于一种对 P2P 网络流量[2~4]的异常检测或者是对其中的参与者之间的信任度[5,6]计算来识别恶意节点和虚假的返回信息。

非结构去中心化的 P2P 网络产生的小规模 DDoS 攻击可以较快消除,但其一旦形成大规模的 DDoS 攻击,网络再进行正常恢复,则需要很长的时间。人工免疫算法主要针对于一些难度随规模扩大而迅速增大的问题, 如 NP 问题等,这类问题的特点是在规模较小时,问题一般易于求解或者说易于发现其局部条件下的求解规律,而在规模较大时,问题很难解决。针对这种规律,本文提出了利用人工免疫的方法对非结构去中心化的 P2P 网络中的恶意节点进行免疫处理。

1 攻击原理和系统实现

1.1 非结构去中心化 P2P 网络中的 DDoS 攻击原理

在非结构去中心化的 P2P 网络中,恶意节点收到来自邻居节点发送(或者转发)的查询消息后,便会给查询者返回一个含有指向非本 P2P 网络中的受害者主机地址的虚假消息,查询者利用此虚假消息向受害主机发起连接。与此同时,其他的节点向其查询同样的资源时,就会进一步扩散该虚假信息。最后,会有大量的节点向受害主机发起连接,这样便会占用受害主机的大量连接带宽,如图 1 所示。

1.2 人工免疫系统在非结构去中心化 P2P 网络中的实现

非结构去中心化 P2P 网络中的每个节点都可以看做是一个独立的人体免疫系统。因此,当一个独立的节点 a 从某个节点 b 获得其请求的的资源信息时,它根据资源信息里所提供的 url 地址去相应的主机进行资源请求。一旦资源请求出现异常的情况,则可以认为是外来的抗原入侵。当从节点 b 获得的资源 url 表现出抗原入侵的程度超过一定阈值时,可以将其对应的请求结果队列加入到记忆库(记忆细胞)中。在节点上构建如

收稿日期: 2012-04-12; **修回日期**: 2012-05-14 **基金项目**: 国家自然科学基金资助项目(61005017)

作者简介: 许晓东(1965-),男,福建漳州人,主要研究方向为网络安全和网络管理;李刚(1987-),男,宁夏银川人,硕士研究生,主要研究方向为网络安全(aiwenlg007@163.com);杨燕(1988-),女,江苏南通人,硕士研究生,主要研究方向为网络安全.

图 2 所示的人工免疫系统,系统中的各个模块功能说明如下:

路由表:节点的邻居路由信息。

路由处理模块:a)根据资源信息查询模块的命令来查询路由表;b)根据记忆库(细胞)清除路由表中的恶意节点的路由信息。

资源信息查询器:向邻居节点进行资源信息的查询,并将返回的资源信息呈递给资源请求模块。

资源请求模块:a)接收资源信息查询器呈递的资源信息,并向相应的主机进行资源请求;b)提交请求状态给请求结果采集器模块。

请求结果采集器:a)采集资源请求的状态,并将状态加入到返回查询信息节点对应的请求状态队列;b)激活状态检测器来将返回信息的节点对应的检测器和其对应的循环队列进行亲和力计算。

状态检测器模块:将返回信息的节点对应的检测器和其对应的循环队列进行亲和力计算,根据计算的结果判断是否提交到记忆库(细胞)并对路由表中的相应路由进行处理,对检测器进行进化。

记忆库(细胞):存放恶意节点的信息。

检测器:存放返回查询信息的节点对应的资源请求状态特征序列。

状态循环队列:存放返回查询信息的节点所对应的资源请求状态。

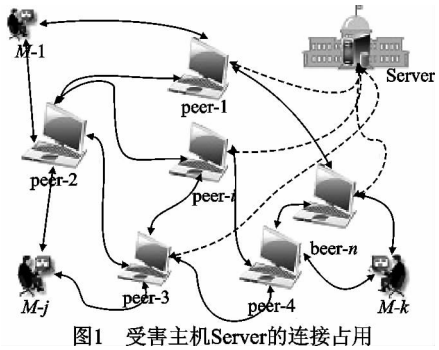

图1　受害主机Server的连接占用

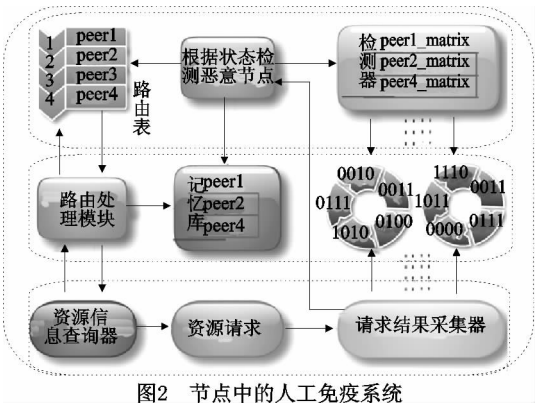

图2　节点中的人工免疫系统

1.3　非结构去中心化 P2P 网络中的人工免疫算法

在已经建立的人工免疫系统模型中,需要将如下内容抽象为数学模型来实现免疫系统:

a)检测器生成算法的数学模型;

b)亲和力计算的数学模型;

c)检测器进化的数学模型。

1.3.1　检测器的生成

为了简化算法的复杂程度,在检测器生成中将采用简单的生成方法,即对每个节点中的检测器的资源请求状态特征序列集合都初始化为成功的请求状态序列。重点将放在亲和力计算与检测器进化算法上。

1.3.2　亲和力计算

给定抗原 $x=x_1x_2\cdots x_{n-1}x_n$ 和抗体 $y=y_1y_2\cdots y_{n-1}y_n$,亲和力计算的数学模型主要是利用阴性选择算法中的匹配规则,本文将给出两种不同的方法来进行其亲和力的度量。

1)方法 1[7]

$$(A_g)_k=\frac{1}{1+t_k}$$

其中:$(A_g)_k$ 是抗原和抗体之间的亲和力,t_k 是抗原和抗体 k 的结合强度。$(A_g)_k$ 的取值在[0,1]之间。$(A_g)_k=0$ 时,表示抗体与抗原完全结合,也就是这里的完全匹配。

实数型的 t_k 结合强度的计算利用 Euclidean 形态空间的 Euclidean 距离:

$$D=\sqrt{\sum_{i=1}^{L}(x_i-y_i)^2}$$

2)方法 2

二进制表示的匹配算法——利用海明匹配与海明距离。给定抗原 $x=x_1x_2\cdots x_{n-1}x_n$ 和抗体 $y=y_1y_2\cdots y_{n-1}y_n$,有一般形式的匹配函数:

$$dMx=\sum_i\overline{x_i\oplus y_i}\geqslant r\quad 0\leqslant r\leqslant n$$

通过上述改进后得到如下匹配函数[8]:

$$dMx=\frac{\sum_i\overline{x_i\oplus y_i}}{\sum_i\overline{x_i\oplus y_i}+2\sum_i x_i\oplus y_i}\geqslant r\quad 0\leqslant r\leqslant 1$$

其中:r 是阈值,dMx 是在阈值内度量 y 和 x 之间的亲和力。

1.3.3　检测器(抗体)的进化算法

检测器的进化对于检测恶意节点至关重要,本文使用了标准的遗传算法来完成检测器进化。在抗原入侵时,系统将抗原 $x=x_1x_2\cdots x_{n-1}x_n$ 和抗体 $y=y_1y_2\cdots y_{n-1}y_n$ 选择为两个交叉遗传的串,根据一致交叉的原则,在染色体位串上的每一位按照相同的概率进行随机均匀交叉[9]:

$$O(p_c,r)\quad z'=\begin{cases}x_i & r>1/2\\ y_i & r\leqslant 1/2\end{cases}\qquad z''=\begin{cases}y_i & r>1/2\\ x_i & r\leqslant 1/2\end{cases}$$

其中:r 是[0,1]上符合均匀分布的随机变量;$p_c=0.60\sim 1.00$[9];生成的新个体为 $z'=z'_1z'_2\cdots z'_{n-1}z_n'$ 和 $z''=z''_1z''_2\cdots z''_{n-1}z''_n$,对 z' 和 z'' 进行变异操作,变异算子按照变异概率 $p_m=0.005\sim 0.01$[9] 随机反转 z' 和 z'' 上的等位基因的二进制字符:

$$O(p_m,r)\quad x'=\begin{cases}1-z_i' & r_i\leqslant p_m\\ z_i' & r_i>p_m\end{cases}\qquad x''=\begin{cases}1-z_i'' & r_i\leqslant p_m\\ z_i'' & r_i>p_m\end{cases}$$

由此可以得到 x' 和 x'',最后分别计算 x' 与 y 之间的亲和力和 x'' 与 y 之间的亲和力,并取亲和力适合者作为检测器的进化结果。

2　在 NS2 上的实验与分析

2.1　NS2 上 GnuSim 的仿真实验

GnuSim 是运行于 NS2 网络仿真平台上的 P2P 网络的插件,它使用的是 Gnutella 协议。Gnutella 协议是非结构去中心

化 P2P 网络的最典型代表。为了数据模拟的真实性,本文以 GnuSim 插件中的 Gnutella 协议为原型,在此基础上进行相应功能的修改,并将人工免疫系统与 Gnutella 协议结合来完成实验。

为 GnuSim 增加如下监测变量和功能函数模块,并对其他相应代码进行修改。

```
// 总共的请求数目
int m_total_url_request;
// 请求失败的数目
int m_failed_url_request;
// 检测器进化的阈值
double m_evolution_threshold;
// 检测器进化模块
double detector_evolution(NodeAddr_t mal_peer);
// 资源请求处理模块
bool push_files(int res_id);
// 请求结果状态循环队列处理模块
bool add_rqst_result(NodeAddr_t addr,bool rqst_state);
// 恶意节点处理模块
bool add_mal_to_memory(NodeAddr_t mal_addr);
// 检测器执行模块
bool exec_detector(NodeAddr_t addr);
// 资源获取模块
NodeAddr_t get_res_addr(int res_id);
// 路由处理模块
bool control_route_table();
```

2.2 实验结果分析

实验中,为 P2P 系统分配 10 个文件、20 个节点,其中一个为恶意节点(编号 4,是修改协议后的节点),一个为受害节点(编号 3,是普通的节点类型);检测器和状态循环队列长度为 k。NS2 在时间 t 后结束,而恶意节点 4 一旦提供虚假信息,将指向受害节点 3。通过编写的 tcl 脚本构建的非结构去中心化 P2P 网络如图 3 所示。

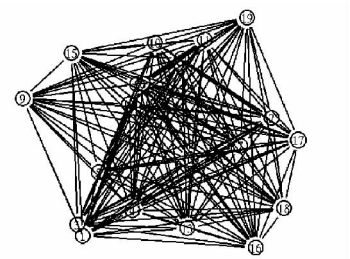

图3 非结构去中心化的P2P网络拓扑

在没有为节点添加人工免疫系统时,节点收到其他节点返回的资源 url 而进行请求结果如表 1 和 2 所示。其中:N-NUM 为节点编号;F4-NUM 为从节点 4 提供的资源信息而请求资源失败的数目;T-NUM 为节点进行的资源请求总数。

表 1 t = 30 000 s 结束

N-NUM	F4-NUM	T-NUM
5	18	75
6	15	100
7	19	141
8	19	82
11	25	177
13	1	11
15	1	4

表 2 t = 100 000 s 结束

N-NUM	F4-NUM	T-NUM
5	60	293
6	54	339
7	56	459
8	58	317
11	74	627
13	1	11
15	1	4

在加入人工免疫系统后,先对每个节点上由其他节点返回的资源信息而进行相应资源请求结果的状态序列计算亲和力(利用方法 1 中的度量标准,方法 2 暂不讨论),并对这些亲和力数据进行采集,如图 4 所示。

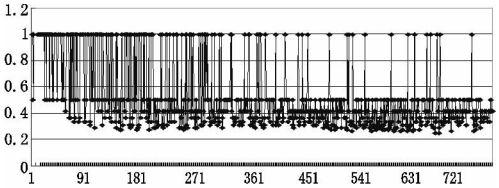

图4 按照节点提供的信息进行请求而得到所有节点的亲和力的序列

图 4 中的横坐标是所有节点按照节点所提供的资源信息而请求得到的请求序列,纵坐标是相应节点每次进行请求后计算出检测器集合中对应节点的请求状态序列特征与自己循环队列中对应的节点的请求状态序列的亲和力。从图中可见,在 0.3 左右,基本是正常节点与恶意节点 4 的亲和力。所以取得两个关键的值作为阈值,即 0.366 03 和 0.333 33(这两个值是正常节点同恶意节点 4 的亲和力)。

分别初始化阈值为 0.36603 和 0.33333,取请求结果状态循环队列和检测器的长度 k 为 5、8、10,系统运行时间 t 分别为 30 000 s 和 100 000 s,运行修改后的仿真系统得到表 3 ~ 5 实验数据。通过对表 3 ~ 5 的分析,得出在 k = 5 的情况下能够尽快地发现恶意节点 4,并能够进行隔离,此时的误报率为 1 个节点;在 k = 8 和 k = 10 的情况下,节点在发现恶意节点 4 时,虽然能够隔离,但是误报率为 3 ~ 5 个节点。

表 3 k = 5 时,不同时间长度、不同阈值的误报采集

时间/s	误报数	阈值
30 000	1	0.366 03
100 000	4	0.366 03
30 000	0	0.333 33
100 000	0	0.333 33

表 4 k = 8 时,不同时间长度、不同阈值的误报采集

时间/s	误报数	阈值
30 000	3	0.366 03
100 000	5	0.366 03
30 000	1	0.333 33
100 000	3	0.333 33

表 5 k = 10 时,不同时间长度、不同阈值的误报采集

时间/s	误报数	阈值
30 000	5	0.366 03
100 000	5	0.366 03
30 000	4	0.333 33
100 000	5	0.333 33

值得注意的是,在 k = 5、阈值为 0.333 33 时,误报的节点数目为 0 个,通过跟踪其中一个请求数据,如表 6 所示。通过表 4 和 6 的分析,虽然没有误报节点,但是要发现恶意节点需要收到很多失败的请求(即 F4-NUM 的值很大),也就是说正常请求的节点通过恶意节点返回的信息向受害主机 3 发起了多次连接。而在此期间,正常节点如果没有很快地发现它,恶意节点提供的虚假信息将很快通过正常节点在网络中蔓延传播。而在 k = 8、阈值为 0.333 33 时,通过跟踪其运行时的请求数据(表 4 和 7)可发现,相应节点的 F4-NUM 值都比较小,也就是正常节点能较早地发现恶意节点,并通过免疫对其进行隔离。但与此同时,其误报也有所提高,不过相信这个误报是可以容忍的,因为在有恶意节点传播虚假信息时,如果不尽快地切断传播,整个网络将成为一个 DDoS 攻击的巨大引擎,这样造成的危害远远大于误报所带来的后果。

表 6 k = 5 时,不同节点的资源请求总数与失败请求总数对比

N-NUM	F4-NUM	T-NUM
5	5	60
6	21	95
7	34	148
8	24	123
11	16	201
13	1	11
15	1	4

表 7 k = 8 时,不同节点的资源请求总数与失败请求总数对比

N-NUM	F4-NUM	T-NUM
5	5	181
6	7	231
7	8	307
8	5	205
11	6	415
13	1	11
15	0	1

通过以上实验说明,在非结构去中心化的 P2P 网络中的节点增加人工免疫系统后,正常节点抵抗恶意节点的能力显著增强,并且在一个可以容忍的误报范围里,能够尽快地将恶意节点隔离。

3　结束语

通过在节点中添加人工免疫系统,对于 20 个节点的非结构去中心化的 P2P 网络,当人工免疫系统中的请求状态循环队列的长度 k 为 5 时,正常节点能发现恶意节点,且误报率低,但是由于非常严格的阈值,使得节点要花费很长的时间才能真正发现恶意节点;当选择 k 为 8 时,节点能在较短的时间发现恶意节点,但误报节点有所增加;当选择 $k=10$ 时,虽然找到恶意节点,误报的节点直线上升。

对于非结构去中心化的 P2P 网络带来的 DDoS 攻击,取状态循环队列长度 $k=8$、阈值为 0.333 33 时,误报的节点数在一定的容忍范围内,可以有效地降低恶意节点带来 DDoS 攻击的风险。在选择请求状态队列的长度 k 时,可以适当放宽误报节点的数目;而在检测器进化时,需要权衡节点上检测器进化的时间是否能够为节点所容忍,这个进化的结果是否能够适应后期出现的恶意节点的检测,这有待继续研究。

参考文献:

[1] NAOUMOV N, ROSS K. Exploiting P2P systems for DDoS attacks [C]//Proc of the 1st International Conference on Scalable Information Systems. New York: ACM Press,2006.

[2] DASWANI N, GARCIA-MOLINA H. Query flood DoS attacks in Gnutella networks[C]//Proc of the 9th ACM Conference on Computer and Communications Security. New York: ACM Press,2002:181-192.

[3] 李俊青,潘全科,王文宏,等. 蚁群优化在 P2P 网络防范 DDoS 攻击中的应用研究[J]. 计算机应用研究,2009,26(1):339-341.

[4] 谭艳霞,吴灏. 基于免疫的对等网络 DoS 攻击防御系统[J]. 计算机工程与设计,2006,27(22):4204-4206.

[5] MA Xin-xin, ZHAO Yang, QIN Zhi-guang. Improving resilience against DDoS attack in unstructured P2P networks[J]. Journal of Electronic Science and Technology of China,2007,5(1):18-22.

[6] ATHANASOPOULOS E, ANAGNOSTAKIS K G, MARKATOS E P. Misusing unstructured P2P systems to perform DoS attacks the network that never forgets[C]//Proc of the 4th International Conference on Applied Cryptography and Network Security. 2006:130-145.

[7] 莫宏为. 人工免疫系统原理与应用[M]. 哈尔滨:哈尔滨工业大学出版社,2003.

[8] 莫宏为,左兴权. 人工免疫系统[M]. 北京:科学出版社,2009.

[9] 李敏强,寇纪淞,林丹,等. 遗传算法的基本理论与应用[M]. 北京:科学出版社,2009.

[10] ZEINALIPOUR-YAZTI D. Exploiting the security weaknesses of the Gnutella protocol[D]. Riverside: University of California,2002.

[11] LIU Yun-hao, LIU Xiao-mei, WANG Chen, *et al*. Defending P2Ps from overlay flooding-based DDoS[C]//Proc of International Conference on Parallel Processing. 2007.

[12] WEI Dong, YANG Shou-bao, LIU Xiao-qian. Artificial immunology based anti-pollution P2P file sharing system grid and cloud computing [C]//Proc of the 6th International Conference on Grid and Cooperative Computing. 2007:82-87.

[13] SUN Xin, TORRES R, RAO S G. On the feasibility of exploiting P2P systems to launch DDoS attacks[J]. Peer-to-Peer Networking and Applications,2010,3(1):36-51.

[14] CHOLEZ T, HENARD C, CHRISMENT I, *et al*. A first approach to detect suspicious peers in the KAD P2P network[C]//Proc of Network and Information Systems Security. 2011:1-8.

[15] 刘丹,李毅超,余三超,等. 面向 P2P 网络的 DDoS 攻击抑制方法[J]. 电子科技大学学报,2011,40(1):85-89.

[16] QWASMI N, AHMED F, LISCANO R. Simulation of DDoS attacks on P2P networks[C]//Proc of the 13th IEEE International Conference on High Performance Computing and Communications. 2011: 610-614.

(上接第 4617 页)

表 1 证明了 Krawtchouk 不变矩的差值只有十分微小的变化,可见它们对平移、旋转、镜面以及尺度变换具有不变性。从表 2 中可以看出,在椒盐噪声、高斯噪声、JPEG 压缩、旋转和剪切的攻击下,本文算法比文献[7,8]的算法提取出的水印图像更清晰,*NC* 值略大。本文算法采用双水印系统,在透明性、鲁棒性、稳定性和抗攻击能力上与其他两个文献算法相比都略胜一筹。

6　结束语

本文算法充分利用了 Krawtchouk 不变矩、提升小波变换和奇异值分解的优势,通过两级提升小波变换后提取其奇异值,再将水印奇异值有效加入。考虑到水印嵌入低频分量,其不可见性好,鲁棒性较差;嵌入到高频分量,其不可见性较差。因此,本文选取其中频分量,兼顾了不可见性和鲁棒性。另外,通过计算 Krawtchouk 不变矩作为另一验证标志,双重水印保证了其鲁棒性。通过实验证明,该算法不可见性好,对常见攻击和几何攻击都具有较好的鲁棒性,具有一定的应用价值。

参考文献:

[1] ZHOU Bo, CHEN Jian. A geometric distortion resilient image watermarking algorithm based on SVD[J]. Chinese Journal of Image and Graphics,2004,9(4):506-512.

[2] 王丽娜,于戈,王国仁. 基于混沌特性改进的小波数字水印算法[J]. 电子学报,2001,29(10):1424-1426.

[3] 刘瑞祯,谭铁牛. 基于奇异值分解的数字图像水印方法[J]. 电子学报,2001,29(2):168-171.

[4] 刘连山,李人厚,高琦. 一种基于彩色图像绿色分量的数字水印嵌入方法[J]. 西安交通大学学报,2004,38(12):1256-1259.

[5] SWELDENS W. The lifting scheme: a new philosophy in biorthogonal wavelet constructions[C]//Proc of SPIE on Wavelet Applications in Signal and Image Processing Ⅲ. [S.l.]: SPIE, 1995: 68-79.

[6] FRIDRICH J, GOLJAN M, HOGEA D. Attacking the outguess[C]// Proc of ACM MULTIMEDIA'02 Workshop on Multimedia and Secrecy, and Steganalysis. New York: ACM Press,2002:3-6.

[7] 徐国荣,王礼平. 基于奇异值与提升小波的彩色图像水印算法[J]. 计算机应用研究,2011,28(5):1982-1986.

[8] 赵玉霞,康宝生. 基于混沌系统与提升小波的彩色图像盲水印算法[J]. 计算机应用研究,2010,27(1):247-250.

[9] 张力,肖薇薇,钱恭斌,等. 基于 Krawtchouk 不变矩的仿射攻击不变性局部水印算法[J]. 电子学报,2007,7(7):1403-1408.

[10] 吴一全,谢静,庞磊. 基于 Krawtchouk 矩和 Contourlet 变换的多目的水印[J]. 光子学报,2009,38(8):2160-2164.

[11] 王春桃,倪江群,卓华硕,等. 基于可变形多尺度变换的几何不变鲁棒图像水印算法[J]. 自动化学报,2011,37(11):1368-1380.

[12] 夏嵬,鲁宏伟,赵小厦. 鲁棒性数字图像水印技术[J]. 小型微型计算机系统,2011,2(2):356-360.