基于 SVM 分类器的 XSS 攻击检测技术

赵 澄 陈君新 姚明海
(浙江工业大学信息工程学院 杭州 310023)

摘 要 Web 应用高速发展的同时产生了大量安全漏洞,跨站脚本攻击(XSS)就是危害最为严重的 Web 漏洞之一,而基于规则的传统 XSS 检测工具难以检测未知的和变形的 XSS。为了应对未知的和变形的 XSS,文中提出了一种基于支持向量机(SVM)分类器的 XSS 攻击检测方案。该方案在大量分析 XSS 攻击样本及其变形样本和正常样本的基础上,提取最具代表性的五维特征并将这些特征向量化,然后进行 SVM 算法的训练和测试。通过准确率、召回率和误报率 3 个指标来对分类器的检测效果进行评价,并优化特征提取方式。改进后的 SVM 分类器与传统工具和普通 SVM 相比性能均有所提升。

关键词 跨站脚本攻击,特征向量化,SVM 分类器
中图法分类号 TP393 **文献标识码** A

XSS Attack Detection Technology Based on SVM Classifier

ZHAO Cheng CHEN Jun-xin YAO Ming-hai
(College of Information Engineering, Zhejiang University of Technology, Hangzhou 310023, China)

Abstract A large number of security vulnerabilities appeare with the development of Web applications, XSS is one of the most harmful Web vulnerabilities. To deal with the unknown XSS, a XSS detection scheme based on support vector machine (SVM) classifier was proposed. The most representative five dimensional features are extracted to support the training of machine algorithms based on a large number of analysis of XSS attack samples. The feasibility of the SVM classifier was verified based on accuracy, recall and false alarm rate. In addition, the characteristics of deformed XSS samples were added to optimize the performance of the classifier. The improved SVM classifier has better performance compared with traditional tools and ordinary SVM.

Keywords XSS attack, Feature vectorization, SVM classifier

1 引言

与桌面软件相比,Web 应用具有轻量级、不需要安装等优势,同时 Web 应用采取的 B/S(浏览器/服务器)架构将软件维护转移到了服务器端,用户无需自己更新,这些优势使得 Web 应用深受互联网企业和用户的青睐。然而 Web 系统中大量运用 Ajax, JavaScript 等技术,大量交互产生在客户端,因此也产生了大量的 Web 漏洞,继而带来了危害严重的 Web 安全问题[1]。

跨站脚本攻击(Cross Site Scripting, XSS),是一种危害严重的 Web 漏洞,常年位居开放 Web 应用安全项目组 Top10 漏洞的前三。XSS 攻击的危害主要有盗取用户 Cookie、会话劫持、网络钓鱼、引发拒绝服务攻击等。

在防御 XSS 攻击时,传统方法使用跨站脚本过滤器 XSS-Filter 来对用户提交的输入进行过滤,XSS-Filter 使用黑名单策略,如果检测到黑名单中的数据就进行拦截。由于安全攻击的方法与手段都是动态的,因此基于黑名单策略的 XSS-Filter 容易被黑客绕过。针对 XSS 攻击的检测,已经有相关工作者研究并设计了 XSS 检测方案,Shashank 等[2]提出在线和离线相结合的方法检测 DOM-based XSS 攻击,对移动云上的 DOM-based XSS 有良好效果,但是没有涉及到反射型 XSS 的检测。Wang 等[3]提出将机器学习算法用于入侵检测,并将 k-NN、PCA 和支持向量机(Support Vector Machine, SVM)算法进行比较,对常见 Web 入侵都能检测。吴少华等[4]将 SVM 算法用于 SQL 注入攻击和 XSS 攻击检测,二者对于变形的 XSS 攻击都没有进行深入研究。Mahmood 等[5]提出了一种新的基于规则的威胁检测方法,将 SVM 算法运用于金融领域的威胁检测,并能对零日漏洞进行识别,但是样本限于金融领域,无法直接复制到其他领域。Salas 等[6]提出使用渗透测试的方法检测 XSS 漏洞,对于 XML 格式的跨站脚本攻击有较好的检测效果,但是其他格式的跨站脚本攻击设计较少。

针对现有 XSS 攻击检测技术只能集中在特定领域或常见类型的不足,本文改进了基于 SVM 分类器的 XSS 攻击检测技术,全面提取大量 XSS 样本特征,尤其是变形 XSS 攻击的特征,通过机器学习的方法形成分类模型,对 XSS 样本进行预测,能够改善传统检测方法的不足。

本文受国家自然科学基金(61379123,61402414),浙江省教育厅资助项目(Y201431815)资助。

赵 澄(1985—),男,博士,高级工程师,主要研究方向为无线网络、数据安全、数据挖掘;**陈君新**(1992—),男,硕士,主要研究方向为网络安全与 Web 安全;**姚明海**(1963—),男,博士,教授,CCF 会员,主要研究方向为智能控制、模式识别、网络控制,E-mail:ymh@zjut.edu.cn。

2　XSS 的分类和特点

XSS 根据其特点和攻击手法的不同，主要可以分为 3 类：反射型 XSS、存储型 XSS 和 DOM-based XSS。

反射型 XSS 也称作非持久型 XSS，攻击者构造一个含有恶意代码的 URL，然后诱骗用户点击此 URL，用户点击 URL 后，恶意 JavaScript 代码就会在用户的客户端执行，恶意 JavaScript 代码只在用户点击 URL 链接时触发，只执行一次，因此又被称作反射型跨站脚本[7]。

存储型 XSS 也称作持久型 XSS，存储型 XSS 不需要用户点击特定 URL 就能进行攻击，攻击者将含有恶意代码的页面上传到服务器上，然后用户在浏览包含恶意代码的网站时就会执行 JavaScript 代码，一般出现在网站评论和转发处。由于恶意代码是上传到服务端的，因此存储型 XSS 比反射型 XSS 危害更大。

DOM-Based XSS 是基于 DOM 文档对象模型的一种漏洞，反射型 XSS 和存储型 XSS 一般存在于服务器端，而 DOM-Based XSS 受客户端浏览器的脚本代码所影响[8]。在使用到 document. referer，window. name 和 window. location 等属性时，尤其要注意防范 DOM-Based XSS。

在这 3 种 XSS 类型中，以反射型 XSS 攻击最为普遍，反射型 XSS 构造简便，能够直接在 URL 的参数中构造，且变化形式较为丰富，多用于获取客户端信息。

3　XSS 攻击检测 SVM 分类器设计

SVM 在二分类尤其是小样本非线性分类问题中效果显著，而且具有很好的泛化能力，可用于多个领域。SVM 的优势主要是通过一个非线性映射，将样本空间映射到高维空间中，使得原来样本空间中非线性可分问题转化为线性可分问题，而 SVM 又通过核函数解决了升维导致的计算复杂性问题，利用核函数展开定理不需要知道非线性映射的显性表达式，因此 SVM 非常适合 XSS 这样的非线性样本。

SVM 分类器的数据处理流程如图 1，将收集的 XSS 攻击样本与正常样本进行数据清洗，数据清洗后进行特征提取与向量化，由于样本分两类，需要对两种样本进行标记，标记后进行 SVM 算法模型训练与测试，如果评价指标达不到要求，就调整模型参数直到达到预期效果。

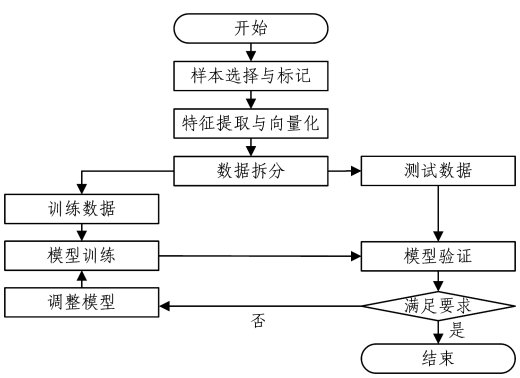


图 1　SVM 分类器的数据处理流程图

3.1　XSS 攻击检测方案设计

XSS 攻击的主要载体就是含有恶意代码的 URL 请求，XSS 攻击样本基本都含有危险函数或敏感关键词，并通过这些危险函数实现攻击。

为了检测 XSS 攻击代码，本文设计了一套基于 SVM 的检测方案，流程如图 1 所示。

一个完整的 URL 请求包括协议、域名、端口、虚拟目录、文件名和参数，实际上 XSS 攻击样本和正常样本的区别主要在于虚拟目录、文件名和参数等部分，因此，为了减少特征提取的工作量，将非关键元素剔除掉，包括协议、域名和端口[9]。数据清洗后的正常样本和 XSS 攻击样本分别如表 1 和表 2 所列。

表 1　数据清洗后的正常样本

序号	示例
1	/en-us/api/search/jobs?s=24&s=56
2	/lib/exe/indexer. php?id=dns&1331
3	/includes/functions_kb. php?phpbb_root_path=http://cirt. net/rfiinc. txt?

表 2　数据清洗后的 XSS 攻击样本

序号	示例
1	/0_1/api. php?op=map&maptype=1&city=test%3Cscript%3Ealert%28/42873/%29%3C/script%3E
2	/goods_list. php?type=1s'%20onmouseover=alert(/ed1e83f8d8d90aa943e4add2ce6a4cbf/)%20//
3	/include/dialog/templets. php?adminDireHand=%22/%3E%3C/script%3E%3Cscript%3Ealert(1);%3C/script%3E

3.2　特征提取与向量化

基于规则的 XSS 过滤器由于规则库或黑名单的限制，不能对未知的 XSS 攻击进行过滤，而采用机器学习的思想将大量样本进行训练，得出分类模型，能够对未知 XSS 攻击样本进行识别。在分类器的设计过程中，特征提取的质量直接影响到分类器的效果。

从权威 Web 漏洞提交平台 exploit-db 获取大量 XSS 攻击样本，针对 XSS 攻击样本中 URL 的特点，从 5 个维度进行样本特征提取。

(1)攻击关键词频率

攻击样本可能在 URL 中使用 JavaScript 代码加载远程脚本，或者通过 document 对象完成对客户端信息的窃取，通过 eval 等危险函数进行攻击。script，document 和 eval 等字符可归纳为攻击关键词维度，而普通样本的 URL 中一般不含有攻击关键词。

(2)特殊字符频率

特殊字符区别于攻击关键词，其为非英文字母，〈script〉的左右尖括号，转义字符\，转码字符 &# 等特殊字符都可以归为此类维度，而普通样本中不需要转义转码等行为，一般没有大量的特殊字符。

(3)数字字符频率

大部分变形 XSS 攻击不直接含有攻击关键词，而是将攻击关键词编码为特殊字符加数字的形式，XSS 攻击样本中的数字频率比普通样本高，因此数字字符频率可以作为一个特征维度。

(4)第三方域名频率

通过分析大量 XSS 攻击样本可知，有相当部分的攻击样本用第三方域名作为攻击者服务器，其作用是接收并存储盗取的客户端信息，而正常请求样本中出现第三方域名的频率低很多。

(5)URL 长度

反射型 XSS 攻击的漏洞利用代码放在 URL 请求中，因

此其 URL 长度更长，而正常 URL 请求不含漏洞利用代码，只有域名、路径和参数等基本部分，其 URL 长度比攻击样本的 URL 长度更短。

传统的基于黑名单的安全工具对于变形的 XSS 检测效果并不理想，普通 SVM 中如果不考虑变形 XSS 样本特征，那么理论上根据特征训练出的分类器对于变形 XSS 攻击的检测效果也是不理想的。本实验在普通 XSS 攻击样本特征的基础上，对变形 XSS 样本进行研究，并提取相关敏感词作为特征提取的重要补充，变形 XSS 特征提取主要有以下 6 种。

(1)使用 javascript:[code]伪协议的形式。由于 HTML 标记中的属性都支持此形式，因此可以利用部分 HTML 标记的属性值进行 XSS，例如：〈img src＝"javascript:alert('xss');"〉，可提取关键词 img 和 javascript。

(2)对标签属性值进行转码。直接使用 XSS 漏洞关键词会被过滤器识别，将关键词转码之后，如果过滤器没有转码后的黑名单，就会产生 XSS 漏洞利用。javascript:alert('xss')经 ASCII 码转换成 javascrip&#116&#58:alert('xss')，可提取特殊字符 &#。

(3)使用空格来分离敏感词。对于 javascript 而言，可以构造如下攻击载荷：〈img src＝"javascript:alert(/xss/)" width＝50〉，其中用空格键将 javascript 隔开，可以绕过 XSS-Filter，可提取特殊字符空格。

(4)利用大小写混淆的 XSS，〈iMg Src＝"javAsCript:alert('xss');"〉，如果黑名单中没有对大小写过滤，那么这种方式就可以绕过 XSS-Filter，可提取关键词 javAsCript。

(5)利用字符编码，可以将敏感词转化为十进制或十六进制。例如，利用攻击词汇 javascript 进行十进制编码得到：&#106&#97&#118&#97&#115&#99&#114&#105&#112&#116，javascript 转化为十进制编码后可能绕过防御[10]。此外，还可以将 URL 中的关键词转化为 URL 编码，"对应%22，＞对应%3E，可提取特殊字符 &#和%。

(6)利用层叠样式表(Cascading Style Sheets，CSS)绕过检测，如果用户浏览器不过滤 style 属性，那么攻击者就可以利用 style＝x:expression(alert(42873))进行 XSS 攻击，因此可提取 expression 和 import 等属性。

5 种特征分类和说明如表 3 所列。

表 3 特征分类和说明

特征分类	特征说明
攻击关键词频率	script，alert，eval，iframe，expression 等字符数量
特殊字符频率	%，\，&，<，>，$，"等字符数量
数字字符频率	阿拉伯数字 0-9 的数量
第三方域名频率	URL 中第三方域名的数量
URL 长度	用户 URL 请求的字符数

特征提取后进行特征向量化，计算机无法直接对 script 等字符进行处理，需要向量化之后才能处理。如果一个 XSS 攻击样本中，攻击关键词字符有 a 个，特殊字符频率有 b 个，数字字符频率有 c 个，第三方域名有 d 个，URL 请求的字符数为 e 个，则此样本可向量化为：$[a,b,c,d,e]$，海量样本的特征经过向量化之后就形成了一个巨大的五维阵列，作为 SVM 分类器的输入数据。

3.3 SVM 分类器设计

SVM 分类算法处理的数据集分为线性可分和非线性可分，如果数据集是线性可分的，那么可以用一条直线或一个平面将两类分开，如图 2 所示。这样的直线或平面有无数个，其中有一个使得决策边界的边缘最大，这一条直线或这个平面就叫作最大边缘超平面，即直线 $\omega \cdot x+b=0$。其中 ω 是超平面的法向量，b 为模型的参数。如果数据集在空间里不是线性可分的，则需要使用非线性映射将它们转化为更高维空间中的数据集，使决策边界在这个空间下变成线性的。

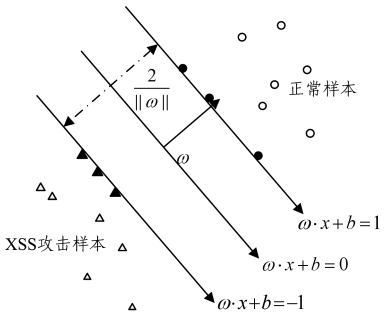


图 2 支持向量机超平面与决策边界

求解决策边界的边缘的最大值，可以转化为最优化问题

$$\min_{w,b,\xi_i} \frac{1}{2}\|\omega\|^2+C\sum_{i=1}^{N}\xi_i \quad (1)$$

$$\text{s.t. } y_i(\omega\cdot\phi(x_i)+b)\geqslant 1-\xi_i,\xi_i\geqslant 0,i=1,2,\cdots,N$$

其中，C 为惩罚因子，表示对误分类的惩罚。ξ_i 为松弛变量，用来放宽不等式约束，以适应非线性可分数据。$\phi(x_i)$为映射函数，用于将数据集映射到更高维的空间。对于不可分样本，需要引入惩罚因子、松弛变量和核函数。

将其转化为对偶拉格朗日函数问题：

$$\max \sum_{i=1}^{N}\lambda_i-\frac{1}{2}\sum_{i,j=1}^{N}\lambda_i\lambda_j y_i y_j \phi(x_i)\cdot\phi(x_j) \quad (2)$$

$$\text{s.t. } \sum_{i=1}^{N}\lambda_i y_i=0,0\leqslant\lambda_i\leqslant C,i=1,2,\cdots,N$$

其中，λ_i 和 λ_j 为拉格朗日乘子，$\phi(x_i)$和 $\phi(x_j)$为映射函数。$\phi(x_i)$与 $\phi(x_j)$的乘积为点积，由于点积计算复杂，根据 Mercer 定理[11]，采用核函数将问题转化为：

$$\max \sum_{i=1}^{N}\lambda_i-\frac{1}{2}\sum_{i,j=1}^{N}\lambda_i\lambda_j y_i y_j k(x_i,x_j) \quad (3)$$

$$\text{s.t. } \sum_{i=1}^{N}\lambda_i y_i=0,0\leqslant\lambda_i\leqslant C,i=1,2,\cdots,N$$

其中，$k(x_i,x_j)$是核函数，进而可求得分类函数 $f(x)$为：

$$f(x)=\text{sign}(\sum\lambda_i y_i k(x_i,x_y)+b),i=1,2,\cdots,N \quad (4)$$

XSS 样本集是非线性的，需要通过核函数将样本映射到高维空间中，SVM 主要有 4 种核函数，即线性核函数、径向基核函数、sigmoid 核函数和多项式核函数。本实验中样本特征维度只有五维，根据适用条件，采用性能良好的径向基核函数。

4 实验与结果分析

实验环境包括操作系统 64 位 Ubuntu16.04，处理器英特尔酷睿 i5 2467M，内存 8GB，编程语言 Python3.5，预装机器学习模块 sklearn。

作为一个良好的 SVM 分类器，其特征应具有可区分性，对应本模型，则要求正常样本和 XSS 样本的特征有一定的差别。表 4 和表 5 分别给出了表 1 中正常样本和表 2 中 XSS 样本的特征分布情况。其中特征 1－特征 5 依次对应攻击关键词频率、特殊字符频率、数字字符频率、第三方域名频率和 URL 长度。从中可以看出正常样本的特征值和 XSS 样本的特征值区别较大，特征 1 和特征 5 区别最明显，因此从文中 5

个维度进行特征提取具有合理性。

表 4　正常样本特征分布情况

正常样本	特征 1	特征 2	特征 3	特征 4	特征 5
1	0	0.0313	0.1250	0	0.0596
2	0	0.0322	0.0967	0	0.0561
3	0	0.0143	0	0.2500	0.1930

表 5　XSS 样本特征分布情况

XSS 样本	特征 1	特征 2	特征 3	特征 4	特征 5
1	0.2073	0.0313	0.0732	0	0.2350
2	0.0543	0.0217	0.1848	0	0.2702
3	0.2421	0.0842	0.0947	0	0.2807

实验一选取 XSS 攻击样本集和正常样本各 1000 个，XSS 攻击样本从漏洞提交网站 exploit-db[1)] 和 XSS 漏洞提交网站 XSSed[2)] 中获取，正常样本从 Web 服务器日志中提取。将 XSS 攻击样本标记为正样本，将正常样本标记为负样本，并将 XSS 攻击样本和正常样本各取出 60% 作为训练样本，剩余 40% 作为测试样本。为了全面评价 SVM 分类器的效果，本实验引入准确率、召回率和误报率 3 个评价指标[9]。

准确率表示分类的准确度，即：

$$ACC=\frac{TP+TN}{TP+TN+FP+FN} \tag{5}$$

召回率表示被预测为正的正样本占总的正样本的比例，即：

$$REC=\frac{TP}{TP+FN} \tag{6}$$

误报率表示错判为正的负样本占总的负样本的比例，即：

$$FAL=\frac{FP}{FP+TN} \tag{7}$$

其中，FN 是被错误判定为负样本的正样本的数量；FP 是被错误判定为正样本的负样本数量；TN 是被正确判定为负样本的负样本数量，TP 是被正确判定为正样本的正样本数量。

为了直观比较 3 种检测工具在准确率、召回率和误报率指标的不同表现，根据实验结果分别绘制了图 3 和图 4，由于误报率远远小于其他两个指标，单独绘制柱状图以清晰对比误报率。从图 3 的准确率比较可以看出，由于加入变形 XSS 攻击样本的特征提取，改进后的 SVM 分类器的准确率比普通 SVM 分类器和 XSS-Filter 的准确率高。从召回率比较可以看出，两种 SVM 分类器的召回率都比 XSS-Filter 要高，而改进后的 SVM 分类器的召回率的提升不如准确率明显，这是因为优化特征提取后，负样本被正确分类的比例提升更多。从图 4 的误报率比较可以看出，改进后的 SVM 分类器比另外两种检测器的误报率少很多，基于同样的原因，优化特征提取后，负样本被正确分类的比例提升更多。

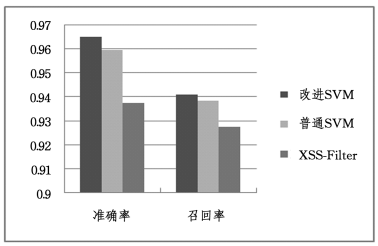


图 3　3 种检测器准确率和召回率的比较

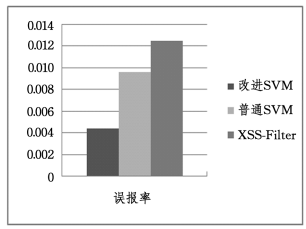


图 4　3 种检测器误报率的比较

实验 1 只是计算出 3 种检测器的准确率等指标，并验证了加入变形 XSS 攻击样本后的 SVM 分类器的效果更好，但是没有具体显示对 3 种 XSS 攻击的检测效果。实验 2 是将 3 种检测器对 3 种不同的 XSS 攻击的检测效果分别进行对比。

从漏洞提交平台 exploit-db 和 XSSed 中收集 3 种 XSS 攻击样本各 100 个，不同于实验 1 中的 XSS 攻击样本，为了评价 3 种检测器的效果，分别统计 3 种检测器检测出的不同类型的 XSS 攻击数量。

图 5 结果显示，3 种 XSS 攻击中反射型 XSS 攻击最容易被检测出，与大部分反射型 XSS 攻击代码直接在 URL 中构造的特点有关，SVM 分类器的特征提取是对 URL 请求中的关键词进行提取，因此反射型 XSS 的特征能够更全面地被提取出来，也就更容易被检测出。对于 DOM-Based XSS 攻击，3 种检测器的效果差别不大，这是因为 DOM-Based XSS 现有的统计特征不明显，只通过 URL 请求难以检测。

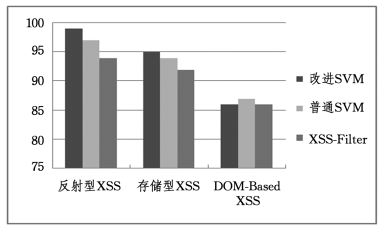


图 5　3 种 XSS 检测器检测出的攻击数

结束语　传统的基于规则的 XSS 检测器难以防御变形的和未知的 XSS 攻击载荷，因此提出使用 SVM 算法进行 XSS 攻击检测，将攻击样本和正常样本清洗标记，并经过训练和测试，达到了良好的准确率和召回率，验证了 SVM 分类器在 XSS 攻击检测领域的可行性。针对变形的 XSS 攻击样本，优化了特征提取的方法，进一步降低了分类器的误报率。相对于基于规则的 XSS-Filter 和普通 SVM 分类器，改进后的 SVM 分类器对 XSS 攻击样本的识别能力更强。实验后续需要完善的地方是将最新的变形 XSS 攻击样本加入特征提取之中，以进一步提高 SVM 分类器的性能。

参 考 文 献

[1]　张伟，吴灏，邹郅路. 针对基于编码的跨站脚本攻击分析及防范方法[J]. 小型微型计算机系统，2013，34(7)：1615-1619.

[2]　SHASHANK G，GUPTA B B，POOJA C. Hunting for DOM-Based XSS vulnerabilities in mobile cloud-based online social network[J]. Future Generation Computer Systems，2018，79(1)：319-336.

[3]　WANG W，LIU J Q，PITSILIS G，et al. Abstracting massive data for lightweight intrusion detection in computer networks[J].

1) https://www.exploit-db.com/webapps

2) http://www.xssed.com

Information Sciences,2018,433:417-430.
[4] 吴少华,程书宝,胡勇.基于 SVM 的 Web 攻击检测技术[J].计算机科学,2015,42(6A):362-364.
[5] MAHMOOD M,ALI Y V. New rule-based phishing detection method[J]. Expert Systems With Applications,2016,53:231-242.
[6] SALAS M I P,MARTINS E. Security Testing Methodology for Vulnerabilities Detection of XSS in Web Services and WS-Security[J]. Electronic Notes in Theoretical Computer Science,2014,302(302):133-154.
[7] ADEVA J J G,ATXA J M P. Inrusion detection in web application using text mining[J]. Engineering Applications of Artificial Intelligence,2007,20(4):555-566.
[8] ROCHA T S,SOUTO E. ETSSDetector:A Tool to Automatically Detect Cross-Site Scripting Vulnerabilities[C]// NetWork Computing and Applications. IEEE Computer Society,2014:306-309.
[9] BISHT P,VENKATAKRISHNAN V N. XSS-GUARD:Precise Dynamic Prevention of Cross-Site Scripting Attacks[C]// In Proceeding of Conference on Detection of Intrusions and Malware & Vulnerability Assessment. 2008:23-43.
[10] 邱永华. XSS 跨站脚本攻击剖析与防御[M].北京:人民邮电出版社,2013.
[11] AHUSBORDE E,AZAIEZ M,BELGACEM F B,et al. Mercer's spectral decomposition for the characterization of thermal parameters[J]. Journal of Computational Physics,2015,294(C):1-19.

(上接第 343 页)

中,此外又加了一定强度的噪声,得到新图像(见图 8),此时我们无法读出嵌入的二维码。

图 7 原图像

图 8 嵌入二维码的图像

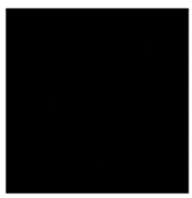
(2)解密

如果要读出二维码,那么只需对含有水印的图像进行奇异值分解,提取水印即可。

4 实验及分析

本文采用原文为"南京邮电大学"的二维码(见图 9(a))。图 9(a)未加密,能够使用普通识别软件读取,而图 9(b)和图 9(c)分别采用奇异值分解直接对二维码加密、将二维码嵌入其他图片的水印中,加密 QR 码,因此必须采用专用识别软件才能正确识读。

(a)原二维码



(b)加密后的二维码

原图像

嵌入了水印后图像

(c)原图像和加入二维码后的图像

图 9 几种图像的对比

对二维码进行加解密测试时,对于加密和未加密二维码,加解密软件可正确识读,而普通的识读软件对于加密二维码的正确识别率为 0%。进行重复实验,设定次数为 1000,记录实验结果。实验结果显示:该二维码的识别正确率为 99%,嵌入和提取水印的正确率为 98%。对加密前后的二维码符进行对比,发现加密不影响二维码的识别。

该实验表明,奇异值加密方法可以很好地完成加密,具有加密稳定、效率更高、简单方便、安全性更强等优点。

结束语 针对二维码信息安全性差的缺陷,本文研究了基于奇异值的加密和解密二维码。通过研究二维码编码规则及加密算法,提出一种基于奇异值分解的改进算法来对编码数据信息加密,在保证信息安全性的前提下,提高了加密效率,使其应用广泛。

参 考 文 献

[1] FU M S,AU O C. Self-conjugate watermarking technique for halftone image[J]. Electronics Letters,2003,39(4):356-358.
[2] 郑东,李祥学,黄征.密码学:密码算法与协议[M].北京:电子工业出版社,2009.
[3] 任勇金.基于 Rijndeal 和异或运算的 QR 二维码双重加密研究[J].华章,2012(29):338.
[4] 刘彦伟,王根英,刘云. QR 码信息加密的研究与实现[J].推广与应用,2012,21(11):37-41.
[5] 李东.基于加密和解密的二维条形码的实现[J].科学传播,2010(7):114-115.
[6] FU M S,AU O C. Self-conjugate watermarking technique for halftoneimages[J]. Electronics Letters,2003,39(4):356-358.
[7] 杨康,袁海东,郭渊博.基于属性加密的二维码分级加密研究[J].计算机工程,2018,44(6):136-140.
[8] 张新文,李华康,杨一涛,等.基于二维码技术的个人信息隐私保护物流系统[J].计算机应用研究,2016,33(11):3455-3459.
[9] 龙强,刘小华.基于非对称密码体制的二维码加密算法[J].重庆师范大学学报(自然科学版),2017,34(3):91-95.
[10] 肖本海,郑莹娜,龙建明,等.基于 SHA512 哈希函数和 Rijndael 加密算法 QR 二维码信息安全设计[J].计算机系统应用,2015,24(7):149-154.
[11] 王尧哲.基于奇异值分解的水印算法与 RSA 公钥密码的结合应用[D].长沙:湖南师范大学,2008.