基于 FPE 技术的企业安全邮件解决方案

张 蕾[1],高永兵[1],马占飞[2]
(1. 内蒙古科技大学 信息工程学院,内蒙古 包头 014010;
2. 内蒙古科技大学 包头师范学院,内蒙古 包头 014030)

摘 要:由于域内大量敏感信息的存在,企业内部电子邮件系统的安全性受到大量企业管理者的重视。在对现有各种安全电子邮件解决方案进行分析的基础上,指出了现有方案的不足之处。针对存在的问题,充分利用保留格式加密(FPE)技术加密后数据格式和长度不变的特点,在保证邮件协议能正常使用的前提下,对邮件头部信息进行了有效的安全保护,提出了一种基于 Feistel 网络 FPE 算法的安全邮件解决方案,使得在保障企业内部电子邮件服务器端和客户端安全性的同时,传输邮件的效率和安全同样获得了保证。

关键词:保留格式加密;安全;电子邮件;Feistel 网络;加密
中图分类号:TP393 **文献标识码**:A **文章编号**:1673-629X(2014)03-0138-05
doi:10.3969/j.issn.1673-629X.2014.03.035

Solution of Security Enterprise E-mail Based on FPE Technology

ZHANG Lei[1], GAO Yong-bing[1], MA Zhan-fei[2]
(1. School of Information Engineering, Inner Mongolia University of Science and Technology, Baotou 014010, China;
2. Baotou Teachers College, Inner Mongolia University of Science and Technology, Baotou 014030, China)

Abstract: Because there are a lot of secret information in Intranet, electronic mail system security has gained a lot of attention to enterprise managers. Based on analysis of the existing solutions of security e-mail, point out the deficiencies of the existing scheme. Aiming at these problems, make full use of the format preserving encryption characteristics, which the enciphered data format and length unchanged. Under the premise of ensuring mail protocol to proper use, mail header information is get for effective protection, and a security mail solution is put forward based on the Feistel networks FPE algorithm. While it ensures the security of enterprise internal e-mail server and client, the efficiency and safety of transmission mail is also received assurance.

Key words: format-preserving encryption; security; e-mail; Feistel network; encryption

0 引 言

随着网络技术的迅速发展,电子邮件已经成为办公自动化的一个重要组成部分。建立企业自己的邮件系统,有一个和自己企业相符合的企业邮箱,已成为互联网时代许多企业的一个基本需求。而近年来,由于企业信息的泄露,更多的研究者开始关注企业内网电子邮件的安全问题。

1 现有安全邮件解决方案的研究

目前保证电子邮件的安全常用到两种端到端的安全技术:S/MIME[1](Secure/Multipurpose Internet Mail Extension)和 PGP[2](Pretty Good Privacy)。两种技术的主要功能就是身份的认证和传输数据的加密,都是利用单向散列算法完成对电子邮件的信息摘要,来确保邮件内容信息的唯一性,通过对称算法和非对称算法一起使用,保护私钥以及加密密钥,达到加密的可靠性和不能抵赖的功能[3]。这两种方案的不同主要是认证的方式。

但是它们都存在着同样的一个安全隐患问题,就是只对邮件体进行加密和签名,而对于邮件头没有实施保护措施。这主要是因为邮件头主要包括邮件发送者和接收者等基本信息,这些信息为邮件在网络中的

收稿日期:2013-05-21 **修回日期**:2013-08-25 **网络出版时间**:2014-01-07
基金项目:国家自然科学基金资助项目(61163025)
作者简介:张 蕾(1984-),女,硕士研究生,研究方向为网络安全;高永兵,副教授,硕士,CCF 会员,研究方向为信息检索与社会网络研究;马占飞,教授,博士,研究方向为信息安全。
网络出版地址:http://www.cnki.net/kcms/detail/61.1450.TP.20140107.1721.041.html

传输以及邮件的处理提供了必要的信息,若是对它用现有的加密技术进行保护,邮件就不能按正常的邮件协议被发送和接收。但是邮件头的安全又是不容忽视的,比如黑客可以给寄件人和收件人发送大量的垃圾邮件甚至是病毒邮件;可以在窃听邮件头的过程中,获知重要的邮件人位置,通过攻击一台重要用户的桌面达到窃取重要信息的目的。在这种情况下,人们就提出了使用 SSL 技术[4]对整个传输过程加密的解决方案。

随着电子商务的迅速发展,作为 SSL VPN 基础的 SSL 协议被 Netscape 公司提出,用作保护 HTTP 通信协议,之后得到了广大安全厂商的支持。而后由 HTTPS 的兴起以及人们对未加密的邮件头的担心,产生了 SSL SMTP 和 SSL POP3。它们是指通过在 SSL 协议所建立的安全传输通道上运行 SMTP 和 POP 协议,即在客户端向服务器发送邮件以及客户端从服务器接收邮件时,双方会利用 SSL 协议专用的通信端口,在双方验证过身份之后,由服务器端发送加密密钥给客户端,之后双方在进行 SMTP 和 POP 协议时,所有的信息都是加密后发送的,在到达后再解密交给相应的模块处理,以此实现电子邮件整体在传输过程中的安全。

但是该方案也存在一些不足之处。首先由于加密的邮件在到达服务器后是要先被解密后才送到相应模块处理的,这使得邮件在服务器上以明文形式保存。这样,一旦用户的用户名及密码泄露,用户的所有邮件都可以被第三者看到。即使邮件服务器没有被黑客入侵,邮件服务器管理员也可能看到服务器中保存的邮件内容。还有一个问题就是,因为原有使用 S/MIME 或 PGP 加密邮件体时,邮件服务器本身是不知道存储了什么样的邮件,也不需要对加密的邮件做什么额外的处理,邮件的加密和解密工作都是由客户端完成的,邮件服务器不需要增加过多的其他功能。而在 SSL 安全邮件方案中,邮件服务器首先要支持 SSL 协议,而且邮件服务器还要负担起用 SSL 协议加解密邮件的工作,这样就增加了服务器的负担,降低了系统的处理效率。

目前采用 SSL 技术部署的安全邮件系统中,解决方案可分为两种:其一是仅使用 SSL,但是在邮件服务器上就是明文;其二则是先用 S/MIME 或 PGP 加密邮件体后,再使用 SSL 加密整个传输过程,优点是保证了安全,缺点是消耗了资源,尤其是面临大邮件或者是邮件量高峰期的时候,邮件服务器的运行会受到严重的影响。

文中提出采用 FPE 加密算法来解决对邮件头进行保护的问题,实现安全而又完整保留原有数据格式,在降低服务端集群加解密压力的情况下,达到 SSL、S/MIME 结合的邮件安全系统作用的体系解决方案。

2　FPE 技术

2.1　FPE 技术简介

FPE (Format Preserving Encryption) 即保留格式加密是一种全新的密码学技术,它将一种特定格式的明文加密成相同格式的密文,即密文的类型和长度与明文相同[5]。

早在 1987 年,国外就开始思考保留格式加密的问题了。只是那时还没提出保留格式加密的概念,而先是有了一种算法,这种算法可以将字母组合加密后仍映射回字母域内,加密基于 DES 算法。到了 1997 年,有人提出了不改变数据类型为前提的数据加密想法,但那时的方案还不够合理。一直到了 2002 年,Black 和 Rogaway 首次从密码学角度研究了 FPE 问题,才提出了适用于整数集上的几种基本的保留格式算法思想:prefix、cycle-walking 和 generalized-feistel[6]。这些基本方法在一定范围内可以处理整数域内的保留格式加密问题,他们也为以后所要研发的加密模型提供了主要参照。真正的保留格式加密应用是在 2008 年 Voltage 公司发布的安全产品中对 FPE 技术的使用。近年来随着网络商务的迅速发展,FPE 技术凭借其独有的加密理念,逐渐成为网络应用和加密处理领域的一个新热点。

随着 FPE 探讨的深入研究,对于 FPE 加密模型的研究在一些领域内得到了比较好的解决,特别是在整数范围里的问题目前已经有了安全、有效的解决方案;而面临较为繁杂的字符集上的保留格式问题,一些研究者们也提出了多个可行的加密模型,虽然解决的方法各有不同,但是多数都使用了 Feistel 网络来构建模型。伴随需要解决的问题域的复杂度越来越高,想要保留格式的问题也就越不好解决。现在解决的思路是不能单因复杂度而增加模型的复杂程度,而是从简单的模型入手,从简单的模型中思考如何与想要解决的复杂模型相关联,将复杂性化整为零,找到等价的整数域上的相关模型[7]。

2.2　FPE 技术的应用

FPE 是一种对称密码,要求密文与明文具有相同的格式,它的初衷是为了加密数据库或者应用系统中的个人识别信息(Personally Identifiable Information, PII),确保信息的密文与明文具有相同的数据类型和长度,进而可以在不修改数据库结构或者应用程序的前提下达到加密的目的,降低成本。这种好的加密思想并没有止步于上面的几个应用,而是不断地被人们挖掘着。现有的一种应用是在测试领域里的使用。因

为原始数据是一些真实的敏感信息(比如银行卡号等),却需要对刚开发出来的新系统进行测试,为了防止数据泄露,使用 FPE 技术加密原始信息得到格式和长度完全相同的测试数据信息,既保证了测试的有效性,又保护了信息的安全。另一种是在需要遵守原有数据格式或协议的加密领域。比如 Stütz[8] 在 2010 年提出的多媒体领域 FPE 的应用。将图像在压缩过程中,使用正则语言的 FPE 方法进行加密处理。

2.3 基于 Feistel 网络的邮件头加密处理

Feistel 密码结构[9]是目前主流的分组密码中的一种对称结构。很多密码标准都使用了 Feistel 网络,其中包括 DES。由于它的对称结构,使得加解密极为相似,解密就是加密的逆运算过程。这就使得编码在开发的过程中节省了将近一半的量。Feistel 网络由于 DES 算法的公布而广为人知,已提出的 FPE 方案多数都采用了 Feistel 结构,比如 FFSEM[10]、FFX[11]、BPS[12]等。

文中结合 Feistel 网络在现有的 FPE 方案中的应用现状,提出对于邮件头的 FPE 方案。要说明的是此方案中是对邮件头中双方的邮件地址进行保留格式加密。

对于邮件地址来说,它的格式是字母加数字@ 域名的形式,其中@ 前面的是用户信息,后面的域名是邮件服务器信息。域名信息在网络传输过程中起路由的作用,用户信息起认证作用。两个信息中,前者是需要保护的,而后者往往是公开的,对它的保护是交给 DMZ 和防火墙来完成的。

此处的 FPE 模型主要通过算法:ΣFPE = (Gen, Enc, Dec)完成邮件头的加解密过程,其中:

1) 算法 Gen:对相关参数进行初始化:

(1) 字符集表 chars = {a, b, c, …, x, y, z, _, 0, 1, …, 9} 和相对应的基数 radix 是字符集表的长度;

(2) 选择要使用的 Feistel 网络的模式;

(3) 需要加密或者解密的消息格式的长度 n;

(4) 在轮函数中要用什么样的伪随机函数、轮函数的循环次数以及字符加法的类型等。

其中用户信息中的字母和数字构成了字母表中的消息空间。消息空间中元素的长度 n 在此次算法中以所要加密的所有用户信息的最大长度定义。使用截断基础分组密码 AES 输出的方式构造伪随机函数 f。运算类型使用字符加法,即 $a_1 \cdots a_n + b_1 \cdots b_n = c_1 \cdots c_n$,其中 $c_i = (a_i + b_i) \bmod \text{radix}$。

2) 算法 Enc:输入是与该邮箱地址相对应的密钥 k 和邮箱地址@ 前的字符串 x,输出是与原字符串格式和长度都一致的字符串 y。两个字符串的字符组成都是来源于前面定义的字符集表。

其中对于字符串 x 的长度,若是小于 n,则暂用固定某个字符填充。

加密的过程可以简单地描述为以下两个过程:

第一个过程是将原始的字符串映射为对应的整数集上的字符组合。每个字符对应的整数字符是其在整个字符集里的位置编码。比如 a 的对应整数字符就是 01,以此类推。当然需要注意的是,为了编码统一得到正确的结果,每个字符的编码均是两位,对于单个的数值位数,前面补零,零也算进编码。比如对 abc 的映射编码就是 010203。

第二个过程是对上面产生的新的字符组合进行事先确定好的 r 轮循环 Feistel 网络运算。首先需要将第一个过程中得到的整数字符串分割为左右两个部分,简称 L 和 R;然后将右半部分作为伪随机函数的输入,得到 R',将 L 和 R' 做字符加法运算得到 L'。最后将 L' 和原先的 R 调换位置后得到下一轮的新的输入。其运算过程如图 1 所示。

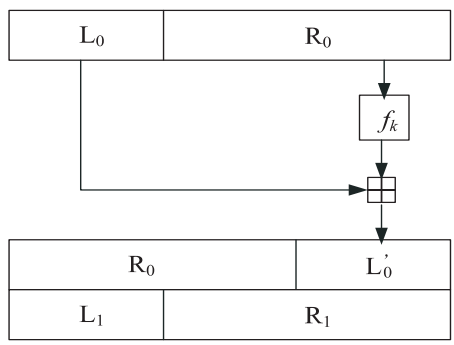

图 1 非平衡 Feistel 运算

对于最后得到的另一元素 j,将其重新替换为字母表中的字母而得到密文 y。

整个加密过程如图 2 所示。

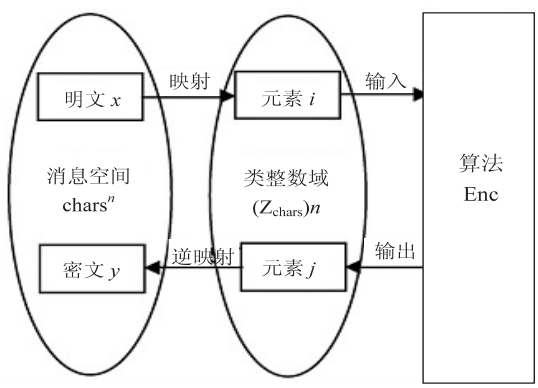

图 2 FPE 的加密过程

3)算法 Dec:输入为基础分组密码的密钥 k 和密文字符串 x,输出为明文字符串 y。该算法是算法 Enc 的逆运算。

2.4 基于 Feistel 网络的 FPE 算法的安全性

保留格式加密是一种特殊的对称密码,其标准的安全目标就是伪随机置换的安全,这种安全就是使攻

击者没有办法鉴别当前的加密是保留格式加密还是某种简单规则下的随机置换。现有 FPE 方案的 Feistel 网络中所用到的伪随机函数的构造方法都是具有可证明的安全性。

3　基于 FPE 技术的安全电子邮件系统的分析和设计

3.1　安全电子邮件系统总体设计

基于 FPE 技术的安全电子邮件系统主要由客户端部分和安全邮件服务端部分构成,另外还有配合邮件体加密的 CA 中心等部分,在邮件体的加密上遵从原有对邮件体加密的 S/MIME 方案,故对邮件体的加密不做重点说明。

客户端部分主要由两部分组成:邮件加解密模块(包括邮件头加解密和邮件体加解密两部分)以及用户的邮件收发客户端模块。邮件头是根据 FPE 技术对邮件头中邮箱地址的保留格式加密或解密;邮件体加解密是根据用户的私钥和收件人的公钥对原有明文邮件实现的类 S/MIME 算法的透明加解密;邮件收发模块一般为用户习惯用的 outlook 软件或者 foxmail 软件。

安全邮件服务端部分也由两部分构成,FPE 加解密组件以及邮件服务器。FPE 加解密组件主要负责对收到的邮件的邮件头进行解密和对要发出的邮件头进行加密的工作;而邮件服务器则不需要进行大的改动,它主要负责存储接收和转发客户端的邮件。结构如图 3 所示。

3.2　发送邮件前邮件数据的处理

发送者的客户端在邮件发送前需对邮件数据进行安全处理。

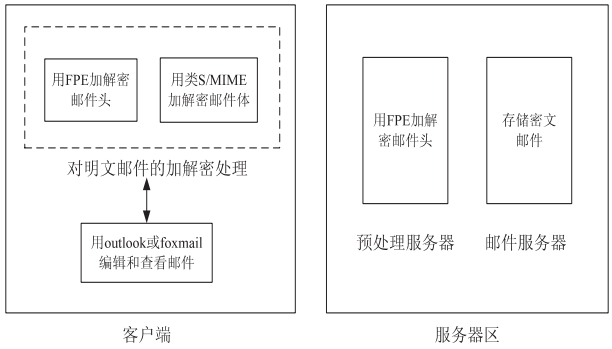

图 3　安全电子邮件系统结构图

(1)先对邮件体进行加密:先对邮件用散列函数进行摘要提取,使用用户的私钥加密摘要生成签名;然后进行邮件加密,先用随机函数产生对称密钥,用其对邮件体进行加密;接下来是用收件人的公钥对随机密钥进行加密。收件人若是单个域内用户,则产生一个解密密钥;若是多个域内用户,则需用每个用户的公钥对随机密钥进行一次非对称加密,产生多个解密密钥。最后是生成密文邮件体,先将签名信息和加密的随机密钥写到前面,再将加密后的整个邮件体写到邮件体的后面部分。

(2) 接下来是对邮件头的加密:主要是用已协商好的密钥,先后对发件人邮箱地址和收件人邮箱地址进行基于 Feistel 网络的保留格式加密,加密后将生成同样格式的邮箱地址,也是由字母和数字构成。

(3)将完成加密的邮件重新交给发送模块,发送模块就会从邮件头部分分离出加过密的发件人和收件人邮箱地址,利用 SMTP 联系邮件服务器,完成发信过程。

整个加密过程如图 4 所示。

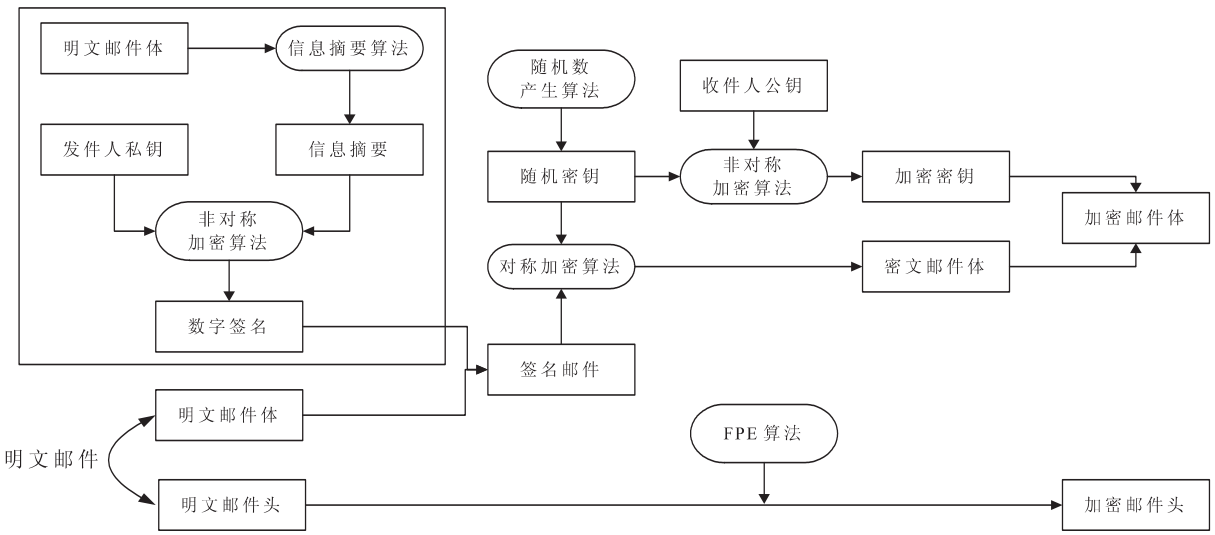

图 4　邮件加密过程

3.3　邮件到达服务区过程中的处理

邮件到达服务区后会先进入预处理服务器,预处理服务器监听着 SMTP 的 25 端口,当有邮件到来后,接收到发件人和收件人信息后,预处理服务器会用事

先统一的密钥对邮箱地址进行解密,然后用解密后的邮箱地址来重新书写邮件头,在和邮件服务器确认收发邮件地址都存在后,会将邮件传递给邮件服务器;否则,会认为是非法的邮件,自动写退信给发件人,退回信件。

当邮件要从邮件服务器传递给收件人时,预处理服务器会先将收件人的 IP 信息等保存起来,然后对邮件头用统一的密钥对邮箱地址进行加密,接着再联系收件人,将已被加密的邮件(邮件头和邮件体)发送过去。

3.4 接收到邮件后邮件数据的处理

接收者在邮件到达后,加解密模块需先对邮件数据进行解密后再交由邮件客户端软件处理。对邮件的解密包括邮件头部分和邮件体部分。对于邮件头里的邮件地址要用实现统一的密钥进行 FPE 对称解密,将解密后正常的邮件地址重新写回邮件头部分。解密邮件体时使用的是用户的私钥对邮件体前面的随机密钥解密。若收件人为多个,则会用收件用户的私钥去一一解密每个加密的随机密钥,直到正确解出密钥为止。在用密钥解密了整个邮件体后,还要对明文邮件体用统一的随机函数进行摘要处理;然后用发件人的公钥解密原邮件的摘要信息,比对无误后,这封邮件才算完全加密并认证完毕。邮件才交由邮件客户端软件(outlook 或者 foxmail)处理。

3.5 新方案的安全评估

结合了 FPE 技术的企业电子邮件系统,使用了恰当的加密算法进行封装,封装后的邮件信息仍然符合 SMTP 对邮件头和邮件体的描述要求,有效地保证了邮件在传输过程和邮件服务器上的安全。具体的安全性能将从以下几个方面进行讨论:

(1) 防止邮件被泄露。

邮件头和邮件体都是可以利用的目标。邮件体用对称和非对称加密算法进行处理,然后邮件头也要进行 FPE,合成一封完整的加密邮件后再进行传输。保证了邮件只能被希望的接收者阅读。由于邮件头是在进行了 FPE 后才进行的传输,利用保留格式加密技术防止了邮件头部信息被窥视。

(2) 防止邮件被篡改。

对于邮件体的完整性,可以通过现有比较成熟的摘要算法来保证。而对于邮件头来说,若是随意伪造的地址,将会在服务器端自动解密邮件头的过程中被发现而引起退信,若是用了其他加密的邮件地址,此邮件将会被邮件服务器错误投递,在接收端解密邮件体时失败而产生错误投递的退信。因此不管哪种篡改都是会被发现的。

(3) 防止冒名顶替的邮件。

从邮件体的角度来说,数字签名技术可以使接收者对发送者的真实性进行有效地鉴别。除了对邮件体使用数字签名防止了冒名顶替的风险外,邮件头的 FPE 也可以防范这样的冒充。如果冒充者以全明文的方式冒充发信时,其发信邮箱地址的不正确加密就会在邮件到达服务器端时被察觉。

(4) 防止发信者或收件者的抵赖行为。

邮件体的数字签名说明只有发件者自己的私钥可以加密,只有收件者自己的私钥可以解密,而且邮件头的加密密钥也只有本人和邮件预处理服务器所有,故不管是发信者还是收件者都不能否认邮件发送或接收的环节。

4 结束语

FPE 技术在国内外使用尚处在探索阶段,现在主要的应用是数据库的加密。而保留格式这样的加密本身对于网络传输的安全性来说,不仅可以保护数据的安全,还能保证原有通信协议的可用性,对网络通信的发展有很大的帮助。对于邮件的加密,达到了效率和安全都提升的作用。而且此次实验只是一个尝试,未来的研究还会考虑如何更灵活地运用 FPE 技术加密邮件头,达到更安全、更高效的目的。

SSL 加密的缺陷除了需要客户端和服务器端都必须支持 SSL 协议外,对数据信息的再次加密也是资源的浪费。

若是 FPE 在邮件的安全上得以广泛应用的话,受益的将不止是 SMTP 和 POP3 协议,可以想象,将会有更多的网络协议因为 FPE 的方便性和隐秘性而获益。

参考文献:

[1] Galvin J, Murphy S, Crocker S. Security multipart for MIME: Multipart/signed and multipart/encrypted[DB/OL]. 1995-10. http://www.ietf.org/rfc/rfc1847.txt.

[2] Elkins M. MIME security with Pretty Good Privacy (PGP)[DB/OL]. 1996-10. http://www.ietf.org/rfc/rfc2015.txt.

[3] 张啸农,徐向阳. 一种企业安全电子邮件系统的设计与实现[J]. 计算机技术与发展,2006,16(10):131-133.

[4] 费巧玲,徐向阳,蒋国清,等. 基于 SSL 的安全邮件解决方案[J]. 计算机工程,2007,33(5):114-116.

[5] 刘哲理,贾春福,李经纬. 保留格式加密技术研究[J]. 软件学报,2012,23(1):152-170.

[6] Black J, Rogaway P. Ciphers with arbitrary finite domains[C]//Proc of the CT-RSA 2002. San Jose: Springer-Verlag, 2002:114-130.

[7] 刘哲理,贾春福,李经纬. 保留格式加密模型研究[J]. 通信学报,2011,32(6):184-190.

(下转第 146 页)

相似,从而对数据区域进行过滤;第 10 ~ 13 行表示发现了一个新的候选目标数据区域;第 14 ~ 17 行是把一条新的数据记录添加到已有数据区域,并更新该区域至区域集合。

从视觉上看,一般页面中所占的版面面积最大的即为目标数据区域,假设由前述 SDRs 算法得到 n 个候选目标数据区域 $DR_1, DR_2, \cdots, DR_n$,根据各区域的长、宽计算区域面积分别为 $S_1, S_2, \cdots, S_n$,排序得最大面积为 $S_t = \mathrm{Max}\{S_1, S_2, \cdots, S_n\}$, $1 \leqslant t \leqslant n$, 则对应的数据区域 DR_t 即为目标数据区域,其余视为噪音。

2.4 用户搜索

考虑到用户常常无法全面地描述自己想要的资料,当用户利用该系统进行检索的时候,查询接口模块应根据用户输入的关键词,采用关键词工具进行扩展得到一组相关的关键词集合,再通过索引库进行查找。采用此方法,用户仅需要输入少数几个关键词,基本上就能得到全部信息,大大提高了信息覆盖率,减少了用户检索次数,从而提高效率。

图 2 为用户检索数据流图。

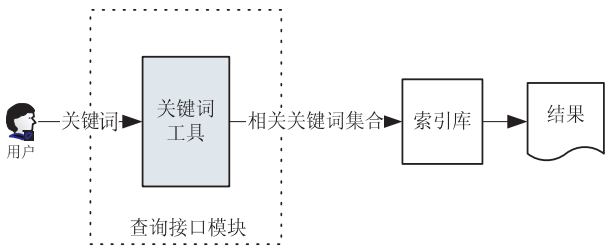

图 2 用户检索数据流图

3 结束语

传统的爬虫搜索方法不考虑搜索关键词的相关性问题,搜索结果常带有垃圾文档,而用户关心的文档却未找到,信息覆盖率、准确性都有待提高。文中对传统元索引进行扩展,引入关键词相关性技术,采用关键词扩充工具,从原始关键词关联出更大的一组关键词库,利用这些关键词库进行爬虫搜索,不仅提高了信息的覆盖率和精度,还大大节省网络、硬件等资源,而且很容易通过扩展应用到其他主题搜索领域。

参考文献:

[1] 马民虎. 互联网信息内容安全管理教程[M]. 北京:中国人民公安大学出版社,2008.

[2] Metasearch engine [EB/OL]. 2010. http://en. wikipedia. org/ wiki/Metasearch_engine.

[3] 刘 耕,方 勇,刘嘉勇. 基于关联词和扩展规则的敏感词库设计[J]. 四川大学学报(自然科学版),2009,46(3):667-671.

[4] Deitel H M. Java Web services for experienced programmers [M]. 北京:机械工业出版社,2003.

[5] Google AdWords [EB/OL]. 2013. https://adwords. google. cn/o/KeywordTool.

[6] Html Parser 2.0 [EB/OL]. 2010. http://htmlparser. sourceforge. net/.

[7] XML Path Language (XPath) 2.0 (Second Edition) [EB/OL]. 2010 - 12 - 14. http://www. w3. org/TR/2010/REC - xpath20-20101214/.

[8] Apache Lucene[EB/OL]. 2013. http://lucene. apache. org/.

[9] Focused crawler [EB/OL]. 2013. http://en. wikipedia. org/wiki/Focused_crawler.

[10] 王能斌. 数据库系统教程[M]. 北京:电子工业出版社,2002.

[11] 关毅璋,郝志峰. 随机变点统计的 MDR 边缘检测算法[J]. 计算机应用研究,2009,26(1):384-386.

[12] 安增文,徐杰锋. 基于视觉特征的网页正文提取方法研究[J]. 微型机与应用,2010(3):38-41.

(上接第 142 页)

[8] Stütz T, Uhl A. Efficient format-compliant encryption of regular languages: Block-based cycle-walking [C]//Proc of the 11th IFIP TC 6/TC 11 Int'l Conf. Linz: Springer-Verlag, 2010:81-92.

[9] Schneier B, Kelsey J. Unbalanced Feistel networks and block cipher design[C]//Proc of the fast software encryption'96. Cambridge: Springer-Verlag, 1996:121-144.

[10] Spies T. Feistel finite set encryption mode[EB/OL]. 2008. http://csrc. nist. gov/groups/ST/toolkit/BCM/documents/proposedmodes/ffsem/ffsem-spec. pdf.

[11] Bellare M, Rogaway P, Spies T. The FFX mode of operation for format-preserving encryption [EB/OL]. 2010. http://csrc. nist. gov/groups/ST/toolkit/BCM/documents/proposedmodes/ffx/ffx-spec. pdf.

[12] Eric B, Thomas P, Jacques S. BPS: A format-preserving encryption proposal [EB/OL]. 2010. http://brutus. ncsl. nist. gov/groups/ST/toolkit/BCM/documents/proposedmodes/bps/bps-spec. pdf.

基于FPE技术的企业安全邮件解决方案

作者： 张蕾， 高永兵， 马占飞， ZHANG Lei， GAO Yong-bing， MA Zhan-fei

作者单位： 张蕾,高永兵,ZHANG Lei,GAO Yong-bing(内蒙古科技大学 信息工程学院,内蒙古 包头,014010)， 马占飞,MA Zhan-fei(内蒙古科技大学 包头师范学院,内蒙古 包头,014030)

刊名： 计算机技术与发展

ISTIC

英文刊名： Computer Technology and Development

年，卷(期)： 2014(3)