文章编号:1001 - 9081(2009)05 - 1297 - 04

基于无可信第三方 IBS 的 XML 数字签名

叶晓彤[1], 彭 龚[2], 简清明[1]
(1. 四川理工学院 网络管理中心, 四川 自贡 643000; 2. 四川理工学院 计算机学院, 四川 自贡 643000)
(yxt_ok@suse.edu.cn)

摘 要:传统 XML 数字签名基于公共密钥基础设施(PKI)体系和非对称算法,存在管理复杂、计算量大等缺陷。通过对 XML 数字签名规范和无可信第三方基于身份的签名(IBS)方案的研究,采用无可信第三方 IBS 的密钥管理机制和对应椭圆曲线双线性映射算法实现 XML 数字签名,按照 XML 数字签名规范的要求,对相应 XML 数字签名实现过程和 XML 数字签名文件结构进行了设计,并分析了具体实现方式。该 XML 数字签名方案在保证安全性的同时,克服了传统基于 PKI 的 XML 数字签名的缺陷,具有更高的效率。

关键词:XML 数字签名;基于身份的签名;CZK 方案;双线性映射;密钥
中图分类号: TP309.7 **文献标志码**:A

XML signature based on IBS without trusted third-party

YE Xiao-tong[1], PENG Yan[2], JIAN Qing-ming[1]
(1. *Network Administration Center, Sichuan University of Science and Engineering, Zigong Sichuan* 643000, *China*;
2. *School of Computer, Sichuan University of Science and Engineering, Zigong Sichuan* 643000, *China*)

Abstract: Based on the Public-Key Infrastructure (PKI) system and asymmetric encryption algorithm, the traditional XML signature has many drawbacks such as complex management process and high computational cost. By the research of XML signature syntax and Identity Based Signature (IBS) scheme without a trusted third-party, the author realized a new XML signature based on the above IBS system and Weil pairing correspondingly, and designed the corresponding XML signature process and structure of XML signature according to the XML signature syntax. The new XML signature overcomes the drawbacks of traditional signature based on the PKI with good security and high efficiency.

Key words: XML digital signature; Identity Based Signature (IBS); CZK scheme; Weil pairing; key

0 引言

随着 XML 技术的发展与应用,XML 正在成为互联网上数据交换的标准。针对 XML 数据存储和传输的安全性需求,尤其是数据的完整性、可验证性和不可抵赖性的要求,W3C 和 IETF 联合发布了 XML 数字签名规范。XML 数字签名是对传统数字签名技术的发展,它基于目前被广泛使用的公共密钥体系(Public-Key Infrastructure, PKI)[1]。PKI 体系需要维护复杂的证书库,或者在客户端需要较大的运算和存储开销[2],因此,受此限制,目前基于 PKI 的 XML 数字签名存在运算量大、管理复杂等缺陷。

基于身份的签名(Identity Based Signature, IBS)方案直接将身份作为公钥,简化了公钥认证机制[3],同时采用了椭圆曲线双线性映射(Weil pairing)等强大的数学算法实现数字签名,在确保安全性的同时,比基于 PKI 的传统签名机制更方便和高效。特别是近年提出的无可信第三方的 IBS 方案[4],具有不需要证书、签名与验证速度快和系统开销小的优点,并且签名密钥由私钥管理中心(Private Key Generator, PKG)和用户共同产生,更进一步保证了签名的不可伪造性,这些特点尤其适合 XML 数字签名使用,能克服现有 XML 数字签名的缺陷,促进 XML 数字签名在数据安全交换领域的应用和发展。

1 XML 数字签名规范

目前,传统 XML 数字签名实现的基础是非对称加密技术,使用的是公钥加密算法与散列函数。在 2001 年 8 月 20 日,由 IETF 和 W3C 共同公布了 XML 数字签名规范[5],在这一规范中将 XML 数字签名解释为:定义一种与 XML 语法兼容的数字签名语法描述规范,描述数字签名本身和签名的生成与验证过程。该规范具体描述了采用 RSA 等算法实现签名和验证的过程,并将 XML 数字签名相匹配的 XML Schema 定义如下:

```
<elementname = "Signature" type = "ds: SignatureType"/>
<complexType name = "SignatureType" >
  <sequence >
    <element ref = "ds: SignedInfo"/>
    <element ref = "ds: Signaturevalue"/>
    <element ref = "ds: KeyInfo" minOccurs = "0"/>
    <element ref = "ds: Object" minOccurs = "0"
      maxOccurs = "unbounded"/>
  </sequence>
</complexType>
```

在上面的 XML Schema 中,<Signature>是 XML 数字签名的主体元素,即封装签名信息的根元素,可以灵活地将<Signature>元素嵌入至恰当的位置,以实现封内签名、封外签名或分离签名。<SignedInfo>、<SignatureValue>、<KeyInfo>、<Object>为 XML 数字签名的 4 大主要元素。各元素在 XML 数字签名文件中的具体定义如表 1 所示。

2 无可信第三方 IBS 方案

为了避开传统公钥加密机制中复杂的证书管理,文献

收稿日期:2008 - 11 - 11;**修回日期**:2009 - 01 - 04。 **基金项目**:四川省教育厅青年基金资助项目(07ZB049)。
作者简介:叶晓彤(1970 -),男,四川自贡人,副教授,主要研究方向:网络安全、XML; 彭龚(1967 -),男,湖南武岗人,教授,博士,主要研究方向:网络安全、软件工程; 简清明(1969 -),男,四川安岳人,讲师,硕士,主要研究方向:网络工程。

[6]中提出了身份密码学(Identity-Based Cryptosystems,IBC)的思想,同时,给出了一种建立在大整数因子分解问题基础上的身份签名机制,即IBS。文献[7]提出将基于离散对数的签名方案转换到利用双线性映射的基于身份签名方案的一般方法,此后多个基于双线性对的签名方案被提出。

表1 数字签名XML元素的表示

元素名称	语法定义
Signature	XML签名的根元素
SignedInfo	包括关于签名数据以及签名验证的其他附加信息
CanonicalizationMethod	表示产生SignedInfo的规范形式的算法
SignatureMethod	表示签SingedInfo元素的算法
Reference	包括URI属性,用于识别被签名的数据对象
Transforms	包括签名者运用于数据对象的一系列转化
DigestMethod	产生数据对象摘要信息的算法
DigestValue	包括数据对象的摘要信息
SignatureValue	存储了整个SingedInfo元素的数字签名
KeyInfo	储存了接受者得到签名验证密钥的附加信息
Object	可选元素,存储了封装签名或数据对象

上述基于身份的数字签名体系存在的一个大的问题,就是系统必须无条件信任可信第三方PKG,PKG掌握系统主密钥,因而可以计算任何用户的私钥,进而可以伪造用户的签名,因此文献[8]提出了一种无需对可信第三方无条件信任的签名方案(简称CZK方案)。该方案用户签名密钥由PKG与用户共同产生,即PKG产生的密钥S_{ID}只是签名方私钥的一部分,另一部分t由签名方自己掌握,从而保证了即使PKG也无法独立伪造用户的签名。XML数字签名采用这种无可信第三方的IBS方案和对应算法,可以避免传统PKI为XML数字签名带来的缺陷,进一步增强安全性,并简化签名、验证过程和签名文件的构建。

目前,包括CZK在内的基于身份的数字签名方案主要建立在椭圆曲线密码学基础之上,该密码体制主要使用双线性映射函数,该函数通过椭圆曲线Weil配对构造。

设G_1和G_2是两个阶为q的循环群,q是一个大素数,G_1是加法群,G_2是乘法群。两群之间的双线性映射$\hat{e}:G_1\times G_1\to G_2$满足以下条件:

双线性 若$P,Q,R\in G_1$,则$\hat{e}(P,Q+R)=\hat{e}(P,Q)\cdot\hat{e}(P,R)$和$\hat{e}(P+Q,R)=\hat{e}(P,R)\cdot\hat{e}(Q,R)$,对任意$a,b\in Z_q^*$,有$\hat{e}(aP,bQ)=\hat{e}(P,Q)^{ab}=\hat{e}(abP,Q)$。

非退化性 存在$P\in G_1$,使$\hat{e}(P,P)\neq 1_{G_1}$。

可计算性 映射$\hat{e}(P,Q),P,Q\in G_1$能有效计算。

双线性映射具有正向可计算性和不可逆推性,且Weil对具有小参数的特点[9]。

3 基于无可信第三方IBS的XML数字签名方案

XML数字签名规范主要是描述数字签名本身和签名的生成与验证过程,所以,基于无可信第三方IBS的XML签名方案也主要从"签名及验证过程"和"签名文件本身的构建"两方面进行设计和分析。

3.1 签名及验证过程设计

由于所采用的密钥管理体系和签名算法与传统XML数字签名不同,基于无可信第三方IBS的XML数字签名过程也与传统XML数字签名过程不同。如图1所示,根据CZK方案,过程设计为三个组成阶段:密钥生成与提取、签名、验证,整个过程通过调用对应的椭圆曲线双线形映射签名算法(以下简称为CZKDSA)来实现和完成。

3.1.1 密钥生成和提取

1)PKG系统初始化:由q阶的加法群G_1和乘法群G_2构成双线性映射$\hat{e}:G_1\times G_2\to G_2$,并随机选择生成元$P\in G_1$;选择Hash函数$H_1:\{0,1\}^*\times G_1\to G_1$,$H_2:\{0,1\}^*\times G_1\to Z_q^*$;随机选择系统主密钥$s\in Z_q^*$,计算$P_{pub}=s.P$。

2)PKG参数公开:公开的参数包括$\hat{e}$、q、P、P_{pub}、H_1,H_2。

3)密钥提取:签名方若身份为ID,可调用CZKDSA算法选取随机数$t\in Z_q^*$,并计算tP,将ID和tP发送给PKG。PKG确认其身份后,计算$Q_{ID}=H_1(ID,tP)$和$S_{ID}=sQ_{ID}$,将S_{ID}送给签名方作为其私钥的一部分,另一部分t由签名方自己掌握。

这种密钥的生成和提取过程与传统PKI的管理过程不同,同时由于Weil对小参数的特点,减小了XML数字签名的后续过程计算量,提高了签名的运行效率。

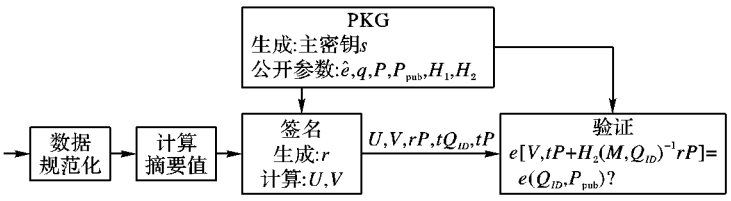

图1 基于无可信第三方的XML数字签名过程

3.1.2 签名

1)签名方根据XML文档中的URL获得需要签名的XML文档或元素,与传统XML数字签名一样,需首先选择一种规范化算法对签名数据进行规范化,以在比特流层次上加以统一。

2)选择一种摘要算法计算出转换后数据的摘要值M,可以选择传统XML数字签名所采用的摘要算法,比如SHA1等。

3)签名方调用CZKDSA算法选取随机数$r\in Z_q^*$,计算$U=H_2(M,Q_{ID})\in Z_q^*$,$V=(t+r/U)^{-1}S_{ID}$,将(U,V,rP,tQ_{ID},tP)作为签名信息传送给接收方。这与传统XML数字签名所要求传递的签名信息不同,并且无需传递和管理公钥。

3.1.3 验证

当接收方接受到XML签名时,接收方通过解析XML签名文件得到签名信息,并从PKG获得公共参数,计算$Q_{ID}=H_1(ID,tP)$,验证$e[V,tP+H_2(M,Q_{ID})^{-1}rP]=e(Q_{ID},P_{pub})$是否成立,若成立,则验证通过。

3.2 XML数字签名文件的构建

根据XML数字签名规范和上述签名过程设计,基于无可信第三方IBS的XML数字签名文件构建方式设计为:

1)根据需要签名数据的位置,创建元素<Transforms>,在<Transforms>中说明需签名数据的信息。

2)创建<CanonicalizationMethod>元素,将使用的规范化算法信息在该元素中说明。

3)创建<DigestMethod>元素,将使用的摘要算法信息在该元素中说明。

4)创建<DigestValue>元素,将通过摘要算法计算的摘要值放入该元素中。

5)创建 < Reference > 元素,将元素 < Transforms >、< DigestMethod >、< DigestValue > 作为其子元素。

6)创建 < SignatureMethod > 元素,在该元素中引用 CZKDSA 签名算法信息。

7)创建 < SignedInfo > 元素,将元素 < CanonicalizationMethod >、< Reference >、< SignatureMethod > 作为其子元素。

8)创建 < SignatureValue > 元素,根据按以上 < SignatureMethod > 操作规范化后的 < SignedInfo >,将采用 CZKDSA 签名算法计算的签名结果 $(U,V,rP,t\ Q_{ID},tP)$ 存入 < SignatureValue > 元素。

9)创建 < KeyInfo > 元素,将涉及 CZKDSA 算法的相关参数加以描述。需要说明的是,并非所有的签名都必须显示的说明这些信息,相关信息完全可以通过其他途径传递,因而 < KeyInfo > 是可选项。

10)创建 < Signature > 元素,使之包括元素 < SignedInfo >、< SignatureValue >、< KeyInfo >,最终生成包含签名的 XML 文档。

由上可见,基于无可信第三方 IBS 的 XML 数字签名文件结构完全符合 XML 数字签名规范的要求,不同的是,在签名文件中对 CZKDSA 签名算法和相关参数进行了相应描述,并传递 CZKDSA 签名算法所要求的签名结果。

4　安全性分析

基于无可信第三方 IBS 的 XML 数字签名采用了无可信第三方的 IBS 方案,传递的签名信息为 CZKDSA 签名算法计算的结果 $(U,V,rP,t\ Q_{ID},tP)$,通过 $e[V,tP + H_2(M,Q_{ID})^{-1}rP] = e(Q_{ID},P_{pub})$ 进行验证,其安全性与传统基于 PKI 的 XM 数字签名相比能得到更充分的保障。

首先,签名的不可伪造性得到保障。根据文献[9]的证明,Weil 对存在 k-CCAP 困难问题,因此,签名 $(h + x)^{-1}P$ 安全,攻击者在不知 S_{ID} 和 t 的情况下,伪造签名 $V = (t + r/U)^{-1}S_{ID}$ 困难。更重要的是,t 由签名者随机产生并以 tP 方式传递给 PKG,在 Weil 对存在 DLP 难解问题的情况下,PKG 难以由 tP 逆推出 t,而签名 $V = (t + r/U)^{-1}S_{ID}$ 中含有单独的 t,所以即使 PKG 也无法伪造签名。

其次,签名的不可欺骗性也得到保障。由于验证是通过计算 $e[V,tP + H_2(M,Q_{ID})^{-1}rP] = e(Q_{ID},P_{pub})$ 完成,其中 $V = (t + r/U)^{-1}S_{ID}$ 包含主密钥 S_{ID},而 $S_{ID} = sQ_{ID}$,显然,签名方无法独立生成 S_{ID},因而签名方不能使用虚假的公钥欺骗接收方。同样,由于 PKG 要验证 $\hat{e}(t\ Q_{ID},P) = \hat{e}(Q_{ID},tP)$ 是否成立,所以签名方也无法用虚假的 $t\ Q_{ID}$ 和 tP 欺骗 PKG。

5　实现分析

根据以上签名方案,在实现基于 IBS 的 XML 数字签名时,应用系统可调用 CZKDSA 密码服务完成密码提取、签名、验证的过程,同时,通过基于 DOM 的软件编程生成相应的 XML 数字签名文件。下面以. NET 平台为例,就这两个关键环节的实现进行具体分析和说明。

5.1　基于 CZKDSA 的 XML 数字签名的实现

XML 数字签名规范主要描述的是 DSA 和 RSA 算法,在. NET现有密码体系结构中也没有提供实现 CZKDSA 算法的密码服务,因此,要实现基于无可信第三方 IBS 的 XML 数字签名,就必须对 CZKDSA 算法进行定义。这里可通过创建提供 CZKDSA 密码服务的 Provider 来实现,并将该 Provider 集成到. NET 现有密码体系中,以供应用系统调用。

设计的 Provider 分别包含 CZKDSA 算法中实现密钥提取、签名、验证的类,应用系统可通过类的实例化操作完成 XML 数字签名。密钥提取类 CZKDSAKeyGenerator、签名类 CZKDSASignAture、验证类 CZKDSAVerification 可定义为:

```
Public Class CZKDSAKeyGenerator
  Public Function GetKey(ByVal PKGurl As Object) As Object
                                        //从 PKG 获得公开参数
  End Function
  Public Function GetPrivateKey (ByVal ID As Object, ByVal t As
    Object, ByVal PKGurl As Object) As Object
     //计算 tP,和 ID 一起发送给 PKG,并从 PKG 获得私钥 S_ID
  End Function
End Class
Public Class CZKDSASignAture
  Public Function Getdata(ByVal DataURL As Object) As Object
                                        //由 URL 获得签名数据
  End Function
  Public Function Pretreatment (ByVal Data As Object, ByVal
    CanonicaMethod As Object, ByVal DigestMethod As Object) As
    Object
    //根据规范化算法对数据规范化,根据摘要算法计算摘要值
  End Function
  Public Function SignAture (ByVal r As Object, ByVal M as
    Object) As Object
      //由 r 和 M 计算 U、V,传递签名信息(U,V,rP,t Q_ID,tP)
  End Function
End Class
Public Class CZKDSAVerification
  Public Function Verify () As Object
        // 验证 e[V,tP + H2(M,Q_ID)^-1 rP] = e(Q_ID,P_pub)
                                        // 是否成立
  End Function
End Class
```

5.2　签名文件的生成

如上所述,基于无可信第三方 IBS 的 XML 数字签名文件的结构完全符合 XML 数字签名规范的语法要求,具体来讲,与传统 XML 数字签名所不同的主要是:需在 < SignatureMethod > 元素中引用 CZKDSA 算法;在 < SignatureValue > 元素中应按 CZKDSA 算法的参数传递要求保存签名结果;如需要,还需在 < KeyInfo > 元素中说明 CZKDSA 算法的相关参数信息。基本实现代码如下:

```
dim Signaturenode as xmlElement = doc. createelement ("Signatur")
dim Signinfonode as xmlnode = doc. createelement ("Signinfo")
dim CanonicalizationMethodnode as xmlnode =
  doc. createelement("CanonicalizationMethod")
CanonicalizationMethodnode. innertext = " * * * *"
                                        //规范化算法引用
Signinfonode. appendchild(CanonicalizationMethodnode)
dim Referencenode as xmlnode = doc. createelement ("Reference")
dim Transformsnode as xmlnode = doc. createelement ("Transforms")
Transformsnode. innertext = " * * * *"          //签名对象 url
Referencenode. appendchild(Transformsnode)
dim DigestMethodnode as xmlnode =
  doc. createelement ("DigestMethod")
DigestMethodnode. innertext = " * * * *"        //摘要算法引用
```

```
Referencenode appendchild(DigestMethodnode)
dim DigestValuenode as xmlnode =
  doc.createelement ("DigestValue")
DigestValuenode.innertext = "***"                    //摘要值
Referencenode appendchild(DigestValuenode)
Signinfonode.appendchild(Referencenode)
dim SignatureMethodnode as xmlnode =
  doc.createelement ("SignatureMethod")
SignatureMethodnode.innertext = "CZKDSA"
                                        //签名算法为 CZKDSA
Signinfonode.appendchild(SignatureMethod)
Signaturenode.appendchild(Signinfonode)
dim SignatureValuenode as xmlnode =
  doc.createelement ("SignatureValue")
SignatureValuenode.innertext = "***"
                                  //签名信息 (U,V,rP,t Q_ID,tP)
Signaturenode.appendchild(SignatureValuenode)
dim KeyInfonode as xmlnode = doc.createelement ("KeyInfo")
KeyInfonode.innertext = "***"        //CZKDSA 密钥参数信息
Signaturenode.appendchild(KeyInfonode)
root.appendchild(Encryptednode)
doc.save (server.mappath("Signaturefile.xml"))
```

6 结语

由于无可信第三方 IBS 具有管理简化、安全性高的特点，同时，其对应椭圆曲线双线性映射算法 CZKDSA 使用的是较小的密钥，运算量小，因此，基于无可信第三方 IBS 的 XML 数字签名能克服传统基于 PKI 的 XML 数字签名的不足，是一种具有优势的新型 XML 数字签名方案。本方案对应 XML 数字签名文件的构建完全符合 XML 数字签名规范，是对 XML 数字签名规范的发展和引申。总之，XML 数字签名引入无可信第三方 IBS 方案能更好地促进 XML 数字签名技术在数字交换领域的应用和发展。

参考文献：

[1] 陈赫贝，阮飞. XML 数字签名及其应用研究[J]. 微机发展，2005，15(2)：53－55.

[2] 田野，张玉军，李忠诚. 使用对技术的基于身份密码学研究综述[J]. 计算机研究与发展，2006，43(10)：1810－1819.

[3] 唐春明，赵延孟. 使用双线性对构造基于身份的不可否认签名[J]. 深圳大学学报：理工版，2006，23(1)：85－89.

[4] 刘宏伟，谢维信，喻建平. 一种基于身份的无可信第三方签名方案[J]. 深圳大学学报：理工版，2006，23(1)：85－89

[5] XML-signature syntax and processing [EB/OL]. (2001－08－20) [2008－09－06]. http://www.w3.org/TR/2001/PR-xmldsig-core.

[6] SHAMIR A. Identity-base cryptosystems and signature schemes [C]// Proceedings of CRYPTO 84 on Advances in Cryptology, LNCS 196. Berlin: Springer-Verlag, 1985: 47－53.

[7] HESS F. Eficient identity based signature schemes based on pairings [C]// The 9th Annual International Workshop on Selected Areas in Cryptography: SAC&apos 02. Berlin: Springer-Verlag, 2003: 3 1 0－324.

[8] CHEN XIAO-FENG, ZHANG FANG-GUO, KIM K. A New ID-based group signature scheme from bilinear pairings [EB/OL]. [2008－08－06]. http://eprint.iacr.org/2003/116.pdf.

[9] BONEH D, LYNN B, SHACHAM H. Short signatures from the weil pairing [C]// Asiacrypt'01, LNCS 2248. Berlin: Springer-Verlag, 2001: 514－532

(上接第1296页)

4 结语

本文引入描述图像纹理特征的差分图像和新定义的刻画两图像差异程度的互信息距离相结合进行图像置乱效果的评价研究。该方法原理简单，易于实现，且能抓住人的视觉认知本身所具有的不确定性因素。实验结果表明，该方法能够较好地刻画图像的置乱程度并反映置乱次数与程度的关系，与人的视觉感知基本相符；另外，由于 Arnold 变换等本身具有周期性，其置乱度曲线也有周期性变化的规律。而且对于不同的图像，该评价方法在一定程度上客观地反映了所用的置乱变换在各置乱阶段的效果。

参考文献：

[1] 丁伟，齐东旭. 数字图像变换及信息隐藏与伪装技术[J]. 计算机学报，1998，21(9)：839－943.

[2] 齐东旭，邹建成，韩效宥. 一类新的置乱变换及其在图像信息隐蔽中的应用[J]. 中国科学：E辑，2000，30(5)：440－447.

[3] 齐东旭. 矩阵变换及其在图像信息隐藏中的应用研究[J]. 北京工业大学学报，1999，11(1)：24－48.

[4] 邹建成，李国富，齐东旭. 广义 Gray 码及其在数字图像置乱中的应用[J]. 高等应用数学学报：A辑，2002，17(3)：363－373.

[5] 柏森，曹长修. 亚仿射变换的性质及其应用[J]. 计算机辅助设计与图形学学报，2003，15(2)：205－208，214.

[6] 熊昌镇，邹建成. 数字图像抽样技术的置乱效果及分析[J]. 北方工业大学学报，2002，14(3)：5－12.

[7] 柏森，曹长修. 图像置乱程度研究[C]//第3届信息隐藏全国学术研讨会论文集. 西安：西安电子科技大学出版社，2001：75－81.

[8] 商艳红，李南，邹建成. Fibonacci 变换及其在数字图像水印中的应用[J]. 中山大学学报：自然科学版，2004，43(增刊2)：148－151，155.

[9] 柏森，廖晓峰. 基于 Walsh 变换的图像置乱程度评价方法[J]. 中山大学学报：自然科学版，2004，43(增刊2)：58－61.

[10] 李志伟，陈燕梅，张胜元. 基于 SNR 的数字图像置乱程度评价方法[J]. 厦门大学学报：自然科学版，2006，45(4)：484－487.

[11] 卢振泰，黎罗罗. 一种新的衡量图像置乱程度的方法[J]. 中山大学学报：自然科学版，2005，44(增刊)：126－129.

[12] BARRITI R. Using mutual information for selecting features in supervised neural net learning[J]. IEEE Transactions on Neural Networks, 1994, 5(4): 537－550.

[13] 吕庆文，陈武凡. 基于互信息量的图像分割[J]. 计算机学报，2006，29(2)：296－300.

[14] 吕庆文，陈武凡. 基于互信息熵差测度的医学图像自动优化分割[J]. 中国科学：E辑，2006，49(4)：484－493.

[15] MAES F, COLLIGNON A. Multimodality image registration by maximization of mutual information[J]. IEEE Transactions on Medical Image, 1997, 16(2): 187－198.

[16] 卢振泰，陈武凡. 基于共生互信息量的医学图像配准[J]. 计算机学报，2007，30(6)：1022－1026.

[17] 范自柱，刘二根，徐保根. 互信息在图像检索中的应用[J]. 电子科技大学学报，2007，36(6)：1311－1314.

[18] 高琰，谷士文，唐璀，等. 一种基于互信息的模糊聚类集成算法[J]. 小型微型计算机系统，2007，28(6)，1068－1071.

[19] 史玉峰，靳奉祥. 数字信息模式识别理论与应用[M]. 北京：科学出版社，2007：49－51.