# 一种认证增强的对象存储安全机制设计

姚 荻 冯 丹
(华中科技大学计算机科学技术学院 武汉 430074)

**摘 要** 在基于对象的存储结构中,客户端与基于对象的存储设备(OSD)直接交互,可以提高访问性能。但是,这给存储系统带来了安全风险。提出了一套用于对象存储系统的新的安全机制,该机制在对象存储访问的主要通信环节均采用安全密钥交换措施,并对双方身份进行双向认证,避免了多类网络攻击,从而提高了对象存储系统的安全性。

**关键词** 认证,对象,存储,安全机制
**中图法分类号** TP393.08 **文献标识码** A

## Authentication Enhanced Object-based Storage Security Mechanism

YAO Di FENG Dan
(Department of Computer Science, Huazhong University of Science and Technology, Wuhan 430074, China)

**Abstract** To improve the access performance, the client communicates with the object-based storage device(OSD) directly in the object-based storage structure. But this brings security questions. In this paper, a set of new security mechanism for the object-based storage system was proposed. In which, by using the secure key agreement and mutual authentication protocol in the main communications between the devices of the object-based storage system, it can prevent most of the network attacks, and so improves the security of the object-based storage system totally.

**Keywords** Authentication, Object-based, Storage, Security mechanism

随着高性能计算系统向网络化方向发展,网络存储技术也获得了快速发展。其中,基于对象的存储(Object-based Storage,OBS)技术由于集合了高性能、可扩展、跨平台、自管理及安全性方面的优势,成为近年来研究的热点。在基于对象的存储结构中,为了提高访问性能,客户端可以和基于对象的存储设备(OSD)直接交互,避免了服务器成为瓶颈。但是,这也带来了安全方面的问题,因为通过复杂网络连接上来的设备不是可以信赖的,可能存在假冒、欺骗等网络攻击,所以必须建立一套完备安全机制,保证挂在网络上的OSD及其访问的安全。

## 1 基于对象的存储系统及其安全问题

基于对象的存储(Object-based Storage,OBS)技术是一种提供对象接口的新型存储技术,它融合了块存储和文件存储的优点,具有较好的安全性,能实现跨平台的数据共享,并具有高性能和高扩展性。OBS的基本思想是,把文件系统的存储管理功能下移到OSD,简化文件系统的管理功能,同时增强存储设备对其内存放对象的自主管理功能。OBS系统中保存对象的设备称为基于对象的存储设备(Object-based Storage Device,OSD)。OSD中的数据以对象的方式来存储和访问,OSD自主管理其内存放的对象,并保证对象存储的安全性。

对象是可变长的,可包含任何类型的数据。对象还具有属性,用于描述对象的特征,例如一个对象的QoS属性描述了该对象的网络延迟要求。对象具有属性,使得OSD可以灵活地给不同的对象赋予不同的安全属性。正如传统文件服务器中的每个文件都具有不同的属性一样,它增强了访问权限控制安全性。但是,对象存储系统对于数据的操作都在存储设备,元数据管理服务器与数据是分开的,客户端散在复杂的网络环境中,这就导致了新的安全问题,攻击者可利用网络来攻击系统和窃取数据。主要的安全威胁有:

(1)伪造:攻击者假冒成客户端从OSD上获取数据,或者攻击者假冒OSD,让安全管理服务器将密钥发给攻击者,并让客户端将数据存储到攻击者上。

(2)窃听:攻击者利用网络监听技术,从传输通道上获取传输中的数据。

(3)重放攻击:攻击者截获认证数据,然后重放或复制发送认证数据,骗取访问权。

因此,基于对象的存储系统在复杂的网络应用中,仍然需要属性访问权限控制以外的安全机制和设施来解决安全问题。

## 2 研究现状

目前,基于T10标准中的OSD安全模型草案,业界已开始研究安全机制问题。例如,复旦大学的陆华等提出了一种基于单密钥的对象存储安全机制[1],华中科技大学的周功业

到稿日期:2009-10-29 返修日期:2010-01-19 本文受科学基金资助项目(70271029)资助。
姚 荻(1971-),女,博士生,CCF会员,主要研究方向为计算机体系结构、网络存储安全,E-mail:deeyao@21cn.com;冯 丹(1969-),女,教授,博士生导师,主要研究方向为计算机体系结构、信息存储系统、容错处理等。

等提出了基于角色访问控制的对象存储安全机制[2]等。但是，这些安全机制有些建立在单个密钥的基础上，要求各设备间具有安全通道，不进行相互身份认证；有的仅在部分设备间进行相互身份认证。这就无法抵御实际的复杂网络环境中中间人等类型的攻击。

## 3 认证增强的对象存储安全机制

考虑到实际应用中的复杂网络环境，本文提出了认证增强的对象存储安全机制，主要设计目标为：

(1)系统中不可信设备间的通信，要求双方先进行身份认证。

(2)密钥安全协商或交换。

(3)密钥管理简单。

(4)实现简单。

安全机制具体描述如下。

### 3.1 安全模型

本安全模型(见图 1)基于 T10 草案进行设计，包含了 3 个组件：(1)客户端，发起 I/O 请求；(2)OSD，对象存储设备；(3)安全管理服务器，密钥管理、认证、授权。

系统工作流程如下：

(1)客户端向安全管理服务器发出文件访问请求。

(2)安全管理服务器对客户端进行身份验证，通过验证后，向客户机发信任状，并将信任状“抄送”OSD。

(3)客户端向相应的 OSD 发对象访问请求，OSD 对客户端进行验证检查，同时进行会话密钥协商。

(4)通过验证后，OSD 与客户端间采用协商出的共享密钥直接进行数据传输。

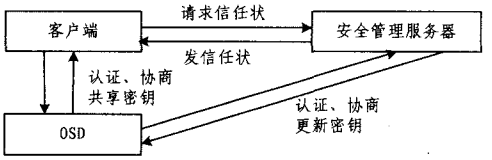



图 1 安全模型

### 3.2 安全协议描述

本方案设计(见图 2)由 3 个协议组成：(1)客户端-安全管理服务器协议，用于客户端请求访问时进行身份授权认证，并取得信任状；(2)安全管理服务器-OSD 协议，用于双方身份核实，并协商更新共享密钥；(3)客户端-OSD 协议，用于客户端与 OSD 进行双向身份认证并协商出共享会话密钥。

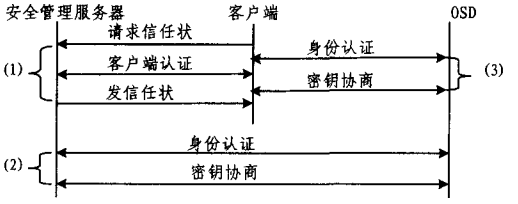



图 2 安全协议

#### 3.2.1 客户端-安全管理服务器协议

在一个安全存储系统中，访问该系统权限的客户端应该在安全管理服务器中有注册信息。因此安全管理服务器中维持有一个客户信息数据库，包含客户身份及口令等信息。安全管理服务器是共知的、可信任的，客户端是不可信的。安全管理服务器需要对客户端进行认证，客户端也要对安全管理服务器发来的信息的真实性进行认证，同时安全管理服务器发来的信息包含了许可证明信息，需进行加密传输。考虑到客户口令是安全管理服务器和客户端共同预知的，相当于预共享私钥(由客户端进行手工修改)，因此可利用该口令来进行加密(任意选一种对称加密算法 E)。协议过程如下：

(1)客户端向安全管理服务器发出访问请求$\{ID_c, F_c, t_c\}$，其中，$ID_c$ 为客户端身份码，$F_c$ 为请求的文件名，$t_c$ 为发出请求的时间戳。

(2)安全管理服务器收到客户端请求后，先对客户端身份码进行认证。如果确认客户端属于合法用户，则向元数据管理器查询该客户端请求文件的操作权限及对应的对象元数据信息 $M_f$。然后计算：

$$h_s = \mathrm{HMAC}(ID_c, t_c, M_f, T_{\exp})$$

使用客户端口令作为密钥将$\{h_s, M_f, T_{\exp}\}$加密，也即将$E_{cpw}\{h_s, M_f, T_{\exp}\}$发给客户端，其中 $T_{\exp}$ 为有效时间。

(3)客户端收到后，利用口令进行解密 $D_{cpw}\{h_s, M_f, T_{\exp}\}$，获得$\{h_s, M_f, T_{\exp}\}$，客户端根据自身保留的 $ID_c$，$t_c$ 和获得的 $M_f$，$T_{\exp}$ 计算 $\mathrm{HMAC}(ID_c, t_c, M_f, T_{\exp})$。若相等，则验证通过，可确认该信息是发给安全管理服务器再回传的信息。否则不是，信息不可用。

客户端得到的$\{M_f, T_{\exp}\}$信息即信任状，根据该信任状就可以与目标 OSD 的通信做准备了。

#### 3.2.2 安全管理服务器-OSD 协议

安全管理服务器与 OSD 都是对象存储系统的组件，相互是已知的，可以采用预共享密钥方式。当然，每个 OSD 与安全管理服务器的共享密钥不同，这些密钥还应周期性地更换。

为了使通信双方通过非安全信道周期性地更换新的共享密钥，需要采用密钥交换协议，以保证共享密钥的安全性。比较有代表性的密钥交换算法是 Diffie-Hellman 协议。这个算法的安全性基于求离散对数的困难性。但是该算法存在的主要问题是没有进行通信双方的身份认证，所以不能抵抗中间人攻击。

本文方案中采取一种包含身份认证的密钥交换算法[3]来进行安全管理服务器与 OSD 之间共享密钥的更新。本协议是基于 Diffie-Hellman 协议的，但是克服了 Diffie-Hellman 协议不能抵抗中间人攻击的缺陷，不仅可以避免中间人攻击，而且可以抵抗密钥猜测攻击、保证前向安全。

假设通信双方预先共享密钥为 $K_0$，同时系统使用两个在 Diffie-Hellman 中定义的公开参数 $g$ 和 $p$，其中 $p$ 是大素数，$g$ 是 $p$ 的本原根。协议过程如下：

1)安全管理服务器与 OSD 分别使用预先定义的函数，从上次使用的密钥 $K_0$ 得出两个整数 $Q$ 以及 $Q^{-1} \bmod (p-1)$。具体的生成函数不作规定，要求 $Q$ 以及 $Q^{-1} \bmod (p-1)$ 与 $p-1$ 互质。并且由不同的密钥 $K$ 生成 $Q$ 具有抗碰撞性。

2)安全管理服务器选择一个随机整数 $a$，计算 $X_1 = g^{aQ} \bmod p$ 以及 $X_2 = g^{a^2 Q} \bmod p$ 并且发送给 OSD。

3)OSD 选择一个随机整数 $b$，计算 $Y_1 = g^{bQ} \bmod p$ 以及 $Y_2 = g^{b^2 Q} \bmod p$ 并且发送给安全管理服务器。

4)安全管理服务器计算 $K_1 = Y_1^{aQ^{-1}} \bmod p = g^{ab} \bmod p$，$R_a = (Y_2^{Q^{-1}})^a \bmod p = g^{b^2 a} \bmod p$，并将 $R_a$ 发送给 OSD。

5)OSD 计算 $K_2 = X_1^{bQ^{-1}} \bmod p = g^{ab} \bmod p$，$R_b =$

$(X_2^{Q^{-1}})^b \bmod p = g^{a^2 b} \bmod p$，并将 $R_b$ 发送给安全管理服务器。

6)安全管理服务器验证 $K_1^q \bmod p = R_b$，如果成立，则接受这次通信，否则拒绝。OSD 验证 $K_2^b \bmod p = R_a$，如果成立，则接受这次通信，否则拒绝。如果双方都接受通信，则双方各自由 $K_1 = Y_1^{qQ^{-1}} \bmod p$ 和 $K_2 = X_1^{tQ^{-1}} \bmod p$ 计算出的 $g^{ab} \bmod p$ 就是新的共享密钥。

安全管理服务器将发给客户端的信任状用与 OSD 间的共享密钥加密后发送给 OSD，以便 OSD 做好与客户端通信的准备。

3.2.3 客户端-OSD 协议

客户端在获得信任状之后，申请与 OSD 通信。客户端与 OSD 原本都没有对方的信息，相互不信任，没有预共享密钥，因此需要进行双向身份认证和协商会话密钥。从安全角度考虑，用公钥密码体制较合适。在公钥密码体制中，椭圆曲线密码体制具有较大的优势，其安全性较高、在同等安全条件下所需密钥长度较短、计算量小，因此本方案选择采用基于椭圆曲线密码体制的设计。

椭圆曲线密码体制(Elliptic Curves Cryptosystems，ECC)是基于椭圆曲线离散对数问题的公钥密码体制。椭圆曲线离散对数问题是指在椭圆曲线构成的 Abel 群 $E_p(a,b)$ 上考虑方程 $Q=kP$，其中 $P,Q \in E_p(a,b)$，$k<p$，则由 $k$ 和 $P$ 易求 $Q$，但由 $P,Q$ 求 $k$ 则是困难的。整数 $k$ 称为 $Q$ 基于 $P$ 的离散对数，表示为 $k=\log_P Q$。ECC 是用有限域上的椭圆曲线有限群代替了有限循环群后得到的一类基于对数问题的公钥密码体制。由于攻击有限循环群离散对数问题的方法，对于椭圆曲线离散对数问题无效，而且椭圆曲线有限群具有丰富的群结构和多选择性，造成攻击椭圆曲线离散对数问题更加复杂和困难。椭圆曲线密码体制的高安全性就是基于椭圆曲线离散对数问题的高难度。

客户端与 OSD 间的协议过程如下：

首先选取一大素数 $p$ 和两个参数 $s,t$，则得椭圆曲线及其上面的点构成的 Abel 群 $E_p(s,t)$。取 $E_p(s,t)$ 的一个生成元 $G(x_1,y_1)$，要求 $G$ 的阶是满足 $nG=O$ 的最小整数 $n$。$E_p(s,t)$ 和 $G$ 作为公开参数。

(1)客户端随机选择一小于 $n$ 的整数 $d_c$，作为秘密钥，并计算 $P_c=d_cG$，产生 $E_p(s,t)$ 上的一点 $(x_c,y_c)$ 作为公开钥，将 $\{ID_c,P_c\}$ 发送给 OSD。

(2)OSD 随机选择一个小于 $n$ 的整数 $d_o$，作为秘密钥，并计算 $P_o=d_oG$，产生 $E_p(s,t)$ 上的一点 $(x_o,y_o)$ 作为公开钥。

(3)OSD 收到客户端发来的 $\{ID_c,P_c\}$ 后，计算 $d_oP_o$ $P_c=(x_2,y_2)$，取 $v_o=\overline{x_2} \bmod n$，将 $\{v_o,P_o\}$ 发送给客户端。

(4)客户端计算 $d_c(P_o)^2=(x_{22},y_{22})$，验证 $v_o=\overline{x_{22}} \bmod n$，如果成立则接受这次通信，完成客户端对 OSD 的认证，否则拒绝，因为只有 $d_c(P_o)^2=d_oP_oP_c=d_cd_o^2G$，$\overline{x_{22}} \bmod n$ 和 $v_o$ 才有条件相等。

(5)客户端计算 $d_cP_cP_o=(x_3,y_3)$，取 $r_c=\overline{x_3} \bmod n$，客户端将 $r_c$ 发送给 OSD。

(6)同样，OSD 计算 $d_o(P_c)^2=(x_{33},y_{33})$，验证 $r_c=\overline{x_{33}} \bmod n$。如果成立，则接受这次通信，完成 OSD 对客户端的认证，否则拒绝。

(7)最后 OSD 与客户端分别由 $K=d_oP_c$ 和 $K=d_cP_o$ 生成双方共享的秘密钥。这是因为 $K=d_oP_c=d_o(d_cG)=d_c(d_oG)=d_cP_o$。

## 4 安全性分析

本方案在整个系统流程的 3 个协议中，均实现了通信数据完整性保证和抵抗网络带来的攻击。

在客户端-安全管理服务器协议中，实现了如下安全：(1)安全管理器用客户端口令来加密信任状，可对双方进行身份验证，避免伪造攻击。这是因为只有安全管理器才预先掌握客户端口令，而客户端只有知道口令才能解密并获得信任状。如果其中任何一方出现假冒，都无法解密。(2)两端分别计算和比较杂凑值 $h_c$，以此避免篡改客户端请求和信任状，保证其完整性，同时避免客户端请求重放、延迟攻击。(3)采用口令加密后传输信任状，可抵御窃听攻击。

安全管理服务器-OSD 协议在实现身份认证和密钥更新的过程中，(1)可以避免中间人攻击，因为中间人不知道 $Q$ 以及 $Q^{-1}$，就无法生成检验值 $R_a$ 和 $R_b$；同时，根据 $R_a$ 不能算出 $R_b$，反之亦不能，所以中间人不能通过采用重发收到的检验值来冒充安全管理服务器或 OSD。(2)其可以抵抗密码猜测攻击，如果攻击者对密钥 $Q$ 进行猜测，可能得到 $g^a$，$g^b$，$g^{a^2}$ 和 $g^{b^2}$ 的假设值，但这些值不能与验证信息的 $g^{a^2b}$，$g^{b^2a}$ 构成等式，所以无法进行猜测攻击。(3)从上面分析可见，可以避免伪造、窃听攻击。(4)它可以抵抗重放攻击。由于验证身份所用到的随机数 $a,b$ 是由客户端、OSD 随机选取，每次不同的组合生成不同的会话密钥，因此可以抵御重放攻击。(5)它可以保持前向安全，即使泄露了老密钥 $Q$，新的密钥仍不会泄露，因为攻击者即使获得了 $Q$，也只能恢复出 $g^a$，$g^b$，$g^{a^2}$ 和 $g^{b^2}$。没有随机数 $a,b$，仍然无法得到新密钥 $g^{ab} \bmod p$。

在客户端-OSD 协议中，实现了以下安全：(1)在实现双向身份认证的同时，可以抵抗中间人攻击。因为中间人不知道 $d_c$ 以及 $d_o$，就无法生成检验值 $v_o$ 和 $r_c$；同时，根据 $v_o$ 不能算出 $r_c$，反之亦不能，所以中间人不能通过采用重发收到的检验值来冒充客户端或 OSD。(2)由上面分析可知，可以抵抗窃听攻击。(3)可以抵抗重放攻击。由于验证身份所用到的随机数 $d_c,d_o$ 是由客户端、OSD 随机选取，每次不同的组合生成不同的会话密钥，因此可以抵御重放攻击。

**结束语** 本文提出了一种新的对象存储安全机制，针对对象存储系统不同设备间的不同关系，设计制订了不同的协议，并给出了安全机制实现的算法。在协议设计中，不仅考虑密钥交换传递的安全性，而且注重对双方身份的认证。经安全性分析，本安全机制具有抵抗各类网络攻击的能力，可提高整个对象存储系统的安全性。同时，主要密钥均为随机生成，不需要专门保存和管理，因此在提高安全性的同时，减轻了系统密钥管理难度。

## 参 考 文 献


[1] 陆华，张世永，钟亦平. 一个基于单密钥的对象存储安全机制设计[J]. 计算机工程，2005，4(31)：148-150

[2] 周功业，易佳，陈进才. 基于角色访问控制的对象存储安全认证机制[J]. 计算机工程与设计，2007，12(28)：5847-5849

[3] 李亚敏，李小鹏，吴果. 身份认证的密钥交换算法[J]. 计算机工程，2006，6(32)：171-172

[4] Seo D, Sweeney P. Simple Authenticated Key Agreement Algorithm[J]. Electronics Letters, 1999, 35(13): 1073-1074

[5] Lin I C, Chang C C, Hwang M S. Security Enhancement for the Simple Authenticated Key Agreement Algorithm[C]// 24th Annual International Computer Software and Application Conference. 2000: 113-115

[6] Kim M, Cetin K K. Enhanced Security for the Modified Authenticated Key Agreement Scheme[J]. IJCSNS International Journal of Computer Science and Network Security, 2006, 6(7B): 164-169

(上接第 271 页)

## 4 本文算法及实验结果

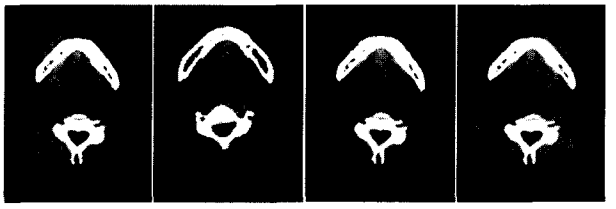
本文提出的基于移动最小二乘法医学图像配准方法的基本步骤如下。

步骤一 在图像感兴趣区域的外部用初始曲线圈定，然后用 snake 模型驱动其收敛到感兴趣区域的边界。

步骤二 按照上一节半自动的方法选取一一对应的两组点集，作为图像配准中的对应标记点集。

步骤三 对这些标记点集使用移动最小二乘法作为变形模型，对图像进行变形，得到最后的配准图像。

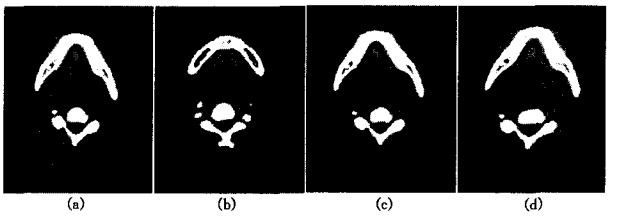
运用本文方法，在 AMD Sempron(tm) processor 2500+ 处理器，内存 1G 的计算机上运行，对不同病人喉管部位的 CT 图像进行了配准。实验结果如图 3 所示，(a)为标准模型喉部 CT 图像，作为变形的模板图像；(b)为待配准病人相同部位的 CT 图像；(c)是对图像选取 12 个标记点，采用最小移动二乘法的仿射变换得到的配准后图像；(d)是运用 30 个标记点采用最小移动二乘法的仿射变换得到的配准后图像。从这个实验看出，点数越多，配准的效果越好。




(a)标准的喉部模型 CT 图像；(b)待配准病人的 CT 图像
(c)12 个标记点配准后图像；(d)30 个标记点配准后图像

图 3 病人与标准模板图像选取不同标记点的配准结果比较

在医学图像中，不同的组织形变是不同的，这需要具有一定的专业知识的医生进行指定。基于移动最小二乘法的变形模型，有 3 种不同的变换可以选择，即仿射变换、相似变换和刚性变换。如图 4 所示，(a)为标准模型喉部 CT 图像，作为模板图像；(b)为待配准病人相同部位的 CT 图像；(c)为对喉管部位，采用移动最小二乘法的刚体变换得到配准后的图像；(d)为对喉管部位采用移动最小二乘法的仿射变换得到配准后的图像。在本实验中，对待配准的图像分别采用刚体变换和仿射变换。从实验结果可以看出，仿射变换是本实验理想的模型选择。




(a)标准的喉部模板图像；(b)待配准病人的 CT 图像
(c)MLS 采用刚体变换配准后的图像；(d)MLS 采用仿射变换配准后的图像

图 4 病人与标准模板图像采用刚体变换和仿射变换的配准结果

如图 5 所示，本文对尺度不变(sift)自动选点方法[9]和半自动选点方法做了比较。(a)和(b)是标准模板和待配准病人的喉部 CT 图像，(c)是采用 sift 得到的结果，(d)是采用本文方法得到的结果。从图中结果可知，采用半自动选点方法可以更好地选取用户感兴趣区域，并且得到较好的对应结果。采用自动选点方法，虽不需人工干预，但不能得到很好地选取用户所需区域，以致不能满足用户最终所需的图像。

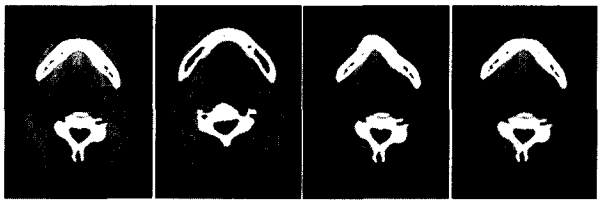


图 5 本文方法与 sift 自动选点的配准方法的比较

**结束语** 本文提出并实现了一种新的基于图像点特征的医学图像配准方法。方法先用一种半自动方法在图像上选取标记点，它能够快速、有效、方便地选取多个对应标记点。基于这些对应标记点采用移动最小二乘法对图像进行形变，从而实现了医学图像配准。选择基于移动最小二乘法的形变模型时，可以根据不同区域或者机体的不同组织选择不同的变换，更好地仿真各个组织的真实形变。实验结果表明，本文的医学图像配准方法是一种有效的、稳定的、可行的配准方法。

## 参 考 文 献

[1] Maintzjb A, Viergeverv M. A Survey of Medical Image registration[J]. Medical Image Analysis, 1998, 2(1): 1-37

[2] Van Den Elsen P A, Pol E-J D, Viergever M A. Medical image matching: A review with classification[J]. IEEE Transactions on Biomedical Engineering, 1993, 16(3): 26-39

[3] Tang Min. Image registration based on improved mutual information with hybrid optimizer[J]. Chinese Journal of Biomedical Engineering, 2008, 17(1): 18-25

[4] 周永新，罗述谦. 基于基形状特征点最大互信息的医学图像配准[J]. 计算机辅助设计与图像学学报，2002，14(7)：654-658

[5] Nikhil R P, Sankar K P. A review of image segmentation techniques[J]. Pattern Recognition, 1993, 26(9): 1277-1294

[6] Schafer S, Mcphail T, Warren J. Image deformation using moving least squares[J]. ACM Transactions on Graphics, 2006, 25(3): 533-540

[7] Pringce L, Xu C. A new external force model for snakes[C]// Image and Multidimensional Signal Processing Workshop. 1996: 30-31

[8] Aminia T S, Weymouth E. Using dynamic programming for minimizing the energy of active contours in the presence of hard constraints[C]// Second International Conference on Computer Vision. 1998: 95-99

[9] Lowe D G. Distinctive image features from scale-invariant keypoints[J]. International Journal of Computer Vision, 2004, 60(2): 91-110