第 19 卷第 4 期　　广西科学院学报　　Vol. 19, No. 4
2003 年 11 月　　Journal of Guangxi Academy of Sciences　　November 2003

浅谈管理信息系统的安全保密设计

Brief Introduction to Design of the Security Protection of Management Information System

郭　荣[1]　　杨　磊[2]

Guo Rong　Yang Lei

（1. 柳州五星商业大厦　柳州　545001；2. 广西计算中心　南宁　530022）

（1. Wuxing Department Store of Liuzhou, Liuzhou, 545001;
2. Guangxi Computer Center, Nanning, 530022）

摘要　针对管理信息系统中软件设计的安全保密问题，提出采用三层客户/服务器数据访问结构、严格的密码保护、限定用户可使用的工作站数量、限定用户访问系统的时间段、限定用户访问数据的部门范围、设定用户可操作的功能权限、及其他安全措施。

关键词　管理信息系统　安全保密　设计

中图法分类号　TP315；TP309

Abstract　The topics of data accessing structure, cipher protection, limitation of usage, limitation of accessing time, limitation of accessing range, initialization of user operating and other securities are discussed according to the security protection in management system design.

Key words　management information system, security protection, design

随着企业信息化工作的不断深化，企业内部计算机网络的作用日益呈显出来，越来越多的企业通过网络沟通、共享和保存信息。这些信息和数据既包含业务数据，也包括财务凭证、报表、人事档案资料以及公司内部公文，还包括合作伙伴供应商的结算信息。这些信息当中有些是企业的商业机密，有些用于企业的规范管理，有些用于辅助决策，它们对企业的生存和发展起到至关重要的作用。因此人们在享受信息化带来便利的同时，也越来越关注信息化的安全保密问题。

管理信息系统的安全保密逐渐成为软件设计人员在分析设计着重考虑的问题。信息化的安全保密工作包括软件设计、硬件保护及管理防范等几个方面，文中主要针对软件设计中要考虑的安全保密措施进行探讨。

1　采用三层客户/服务器数据访问结构

在以往的开发设计过程中，我们发现对数据的访问可以采用许多第三方工具。为了防止一些别有用心的用户绕过有较好安全保护措施的客户端应用程序，直接访问数据库中的数据，我

2003-03-17 收稿，2003-06-02修回。

们采用了三层客户/服务器（C/S）数据访问结构。将软件功能分成表示层、功能层、数据层。中间功能层起到代理作用，用户对数据库的访问必须由表示层向中间功能层申请，中间功能层受理申请后，记录访问要求并核实用户对管理信息系统的访问权限，然后向数据层提出访问申请。这样，用户的访问权限只针对管理信息系统，数据层不必对用户提供直接访问权限。这种访问结构，可以把对数据层访问的识别名称和密码设得足够长、足够复杂，且随时变化，未授权的用户就难以绕过功能层而利用数据库工具或黑客手段非法访问数据层。三层客户/服务器数据访问结构为严格的安全管理奠定了坚实的基础。

2　严格的密码保护

安全保密包含登录密码的保密。为了保证密码不容易被猜出，我们对密码提出了较严格的要求。要求密码长度不小于6位，必须是数字字符和拼音字符相混合，且不能有连续3个字符相同或相近，否则系统自动要求修改密码，不然拒绝运行。我们设定登录密码尝试次数为3次，3次尝试不成功，则锁定该用户并自动关闭系统，不再提供尝试机会，只有专职维护人员才能对用户解锁。这就防止了某些用户通过穷举登录系统，进行非授权的活动。为了保证密码的安全，我们对密码的保存和传输也进行了密码字符移位和按位逻辑运算加密处理。

3　限定用户可使用的工作站数量

为了防止授权用户在监控范围外的其他工作站登录系统，我们根据网卡的 MAC 地址对所有连入企业内部网络的工作站进行统一编号和加密注册。工作站连接服务器并访问数据库时，工作站的 ID 号及 MAC 地址必须和数据库中登记的 ID 号及 MAC 地址一致，没有编号的工作站或未经专职维护人员授权注册的工作站不能启动管理信息系统。对每个用户设定其所能登录的工作站，每个用户只能在指定的工作站上登录系统。

4　限定用户访问系统的时间段

限定用户能操作系统的时间段，使用户只能在规定的时间范围内使用系统。这个措施可以防止用户在工作时间之外，在没有同事监督的时间段内，随意使用系统或泄露企业信息。

5　限定用户访问数据的部门范围

每个用户工作部门可能不同，所要掌握和了解的数据也不同。我们既要保证各个用户能查询和处理职责范围内的数据，又要防止用户能接触到其职责范围外的数据。这样一来可以防止用户对他不熟悉的数据进行误操作，二来又可以大大减少信息泄漏的机会。我们把数据加上所属部门属性，同时设定每个用户的部门权限范围。这是一个树状授权，用户只要有某一部门的数据权限，就自动拥有其下一级部门的数据权限。这样该用户每次访问数据时，都只能对其授权范围内的数据进行操作。

6　设定用户可操作的功能权限

用户分工不同其工作职能不同，在系统中担任的角色也不同。录入员负责业务单据录入；财务人员负责财务凭证和报表的生成；档案管理人员负责档案维护管理；中层管理人员负责对数据的查询和统计分析；高层决策人员则需要系统提供辅助决策图表。我们把用户进行分组，组内用户拥有相同的默认的功能权限。另外，为了适应各个用户工作的特殊性，每个用户在默认组功能权限的基础上，还可以获得和他工作相关的各个功能的单独授权。用户登录系统成功后，根据用户的功能权限，自动生成动态功能菜单，未授权的功能在菜单上不显示，对

当前用户来说，这些功能如同不存在一样。

7 其他安全措施

为了跟踪用户的操作、查找安全漏洞、防止用户否认其操作记录，我们对用户的数据访问申请进行全程记录，并把记录保存在数据库中。为预防有些用户离职或岗位变动而相关部门没有及时通知维护人员等方面的失误给数据安全保密带来威胁，系统每天自动查找在限定的日期长度内未使用系统的用户，并锁定该用户。有些用户暂时离开工作站但又忘记退出系统，系统在3 min 后会自动锁定，只能输入当前用户密码才能再次使用系统，这样可以防止周围的非授权用户非法使用系统。

系统主要安全保密措施和登录过程如图1、图2所示。

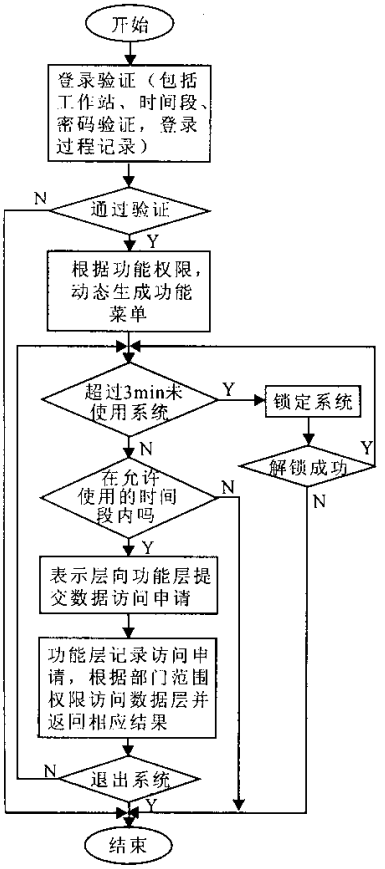

图1 系统主要安全保密措施

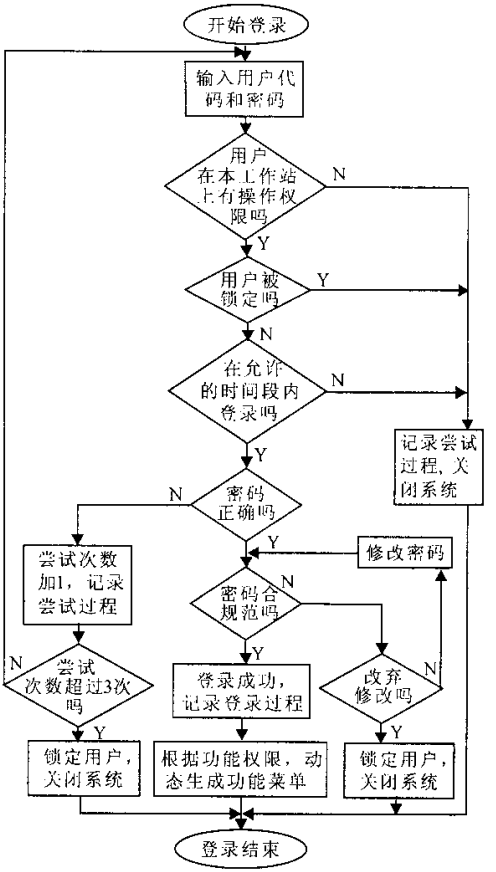

图2 系统登录过程

8 结束语

综合采用以上措施，笔者主持设计的商业进销存管理信息系统在数据的安全保密方面达到了较高的水平，得到了同行专家的认可。在多年的实际使用过程中，也从未出现数据泄密或被攻击现象。管理信息系统的安全保密设计是一个充满挑战的课题，要考虑和防范的问题还很

多，希望我们的开发人员在互相交流学习的过程中，逐步提高安全保密意识和设计能力。

参考文献

1　高　阳. 计算机网络原理与实用技术. 长沙：中南工业大学出版社，1998.
2　熊忠阳，张玉芳. 信息管理系统安全策略. 电脑技术信息，2002，2：25～26.
3　付连续，罗　飞，文绍纯等. 基于网络用户安全的信息管理系统的设计. 计算机应用，2001，12：37～38，41.

（责任编辑：黎贞崇）

对拉普拉斯金字塔和对比度金字塔图像融合方法的性能比较

玉振明[1]　高　飞[2]

（1. 广西大学梧州分校　梧州　543002；2. 北京航空航天大学203教研室　北京　100083）

摘要　图像融合作为信息融合的一个重要领域，已经广泛应用于遥感、计算机视觉、医学、军事目标探测和识别等方面。因此，探索有效的图像融合算法是当前的热点课题。近年来有不少学者提出了各种图像融合的方法，归结起来占主流的是源于多分辨率的方法，这类方法一大类是基于图像的高斯金字塔分解，然后派生出拉普拉斯金字塔，对比度金字塔等；另一大类是基于小波分解的算法，基本思想是把图像分解到不同分辨率下的一系列子图像，其中每一级包含一个包含了低频信息的模糊子图像和三个行、列、对角线方向上的高频细节子图像。这两类方法的共同之处都是在不同的分辨率下各自按一定的规则融合，得到一个融合后的图像序列，然后重构图像。虽然这些方法在实用中效果很好，但是目前还没有对各类图像融合都普遍适用的理想方法，因此对不同方法的融合效果进行主观和客观的评价是重要的。图像融合效果的评价也是一个目前讨论的热点问题，目前融合效果的评价有主观视角效果评价和客观指标评价两种，首先应进行详细的主观评价，因为到目前为止还没有能非常准确描述融合质量的客观物理指标，在某些情况下可以通过融合图像和标准图像比较来评价融合效果，但是在大多数情况特别是实际应用中，标准图像几乎是不可能存在的，所以主观评价仍然是现在评价融合效果的主要方法，但缺点也是明显的，因为人的视角是有差别的，不同人的评价可能有很大的差异。而客观评价目前主要是通过计算图像信息量指标的方法来进行，典型的做法是计算图像的熵和交叉熵，熵反映融合图像的信息量大小，而交叉熵反映的是融合后的图像和原图像的差异。

本文阐述了基于高斯金字塔分解的拉普拉斯金字塔和对比度金字塔两种图像融合原理和方法，并使用这两种方法对上海某地区的蓝光和红外两个波段卫星遥感图像进行了融合实验。由于蓝光在可见光内，成像的场景比较清晰，但对温度不敏感，所以不能突出高温物体。相反红外波段对场景成像比较模糊，但对高温目标敏感。所以两幅图像中有许多互补的信息。实验表明两种图像融合方法都能得出较好的融合效果。

本文通过计算熵和交叉熵两种描述图像信息量和互信息量的指标对融合质量进行了比较，发现从这两个常用的客观指标上来看对比度方法都优于拉普拉斯方法，但从实际的视角效果评价并不能得出同样的结论，只能说对比度方法具有特别突出红外特征明显的目标的特点，从整幅图像的视角效果看并不优于用拉普拉斯金字塔融合的图像，从图像平滑、视角不失真的角度看拉普拉斯金字塔的融合方法可能还优于对比度金字塔的方法。这说明用熵或交叉熵评价融合性能并不一定可靠。所以，评价融合效果单从一些客观指标来看是不够可靠的，真正能合面、真实反映融合质量的物理指标还有待探索。

关键词　拉普拉斯金字塔　对比度金字塔　图像融合　熵　交叉熵