可视密码安全方案在物联网应用层的研究与设计

韩妍妍[1,2] 张 京[1] 闫晓璇[1] 李 娜[2]

[1](北京电子科技学院通信工程系 北京 100070)

[2](西安电子科技大学通信工程学院 陕西 西安 710071)

摘 要 OIDC[1](OpenID Connect)协议是目前最新的应用在 WoT(Web of Things)应用层的单点登录协议之一。为了解决 WoT(Web of Things)应用层认证和授权的问题,提出一种多秘密可视密码方案,结合 OIDC 协议,实现 WoT 应用层认证和授权的功能。多秘密可视密码技术能够在少量分存中隐藏多个秘密信息,同时可以弥补 OIDC 的缺陷。该方案在减小 WoT 应用层开销的前提下,能够提高安全性。

关键词 物联网 多秘密可视密码 认证 授权

中图分类号 TP309 **文献标识码** A DOI:10.3969/j.issn.1000-386x.2018.12.057

RESEARCH AND DESIGN OF VISUAL CRYPTOGRAPHY SECURITY SOLUTION AT THE APPLICATION LAYER OF WEB OF THINGS

Han Yanyan[1,2] Zhang Jing[1] Yan Xiaoxuan[1] Li Na[2]

[1](*Department of Communication Engineering, Beijing Electronic Science and Technology Institute, Beijing 100070, China*)

[2](*School of Telecommunications Engineering, Xidian University, Xi'an 710071, Shaanxi, China*)

Abstract OpenID connect (OIDC) protocol is latest at present, and is one of the single sign-on protocols in the application layer of Web of Things (WoT). In order to solve the authentication and authorization problem of WoT application layer, a multi-secret visual cryptography scheme was proposed in this paper. It combined OIDC protocol to realize the authentication and authorization function of WoT application layer. Multi-secret visual cryptography could hide a lot of secret information in a small amount of memory and make up for the OIDC defects. This scheme can improve the security under the premise of reducing the cost of WoT application layer.

Keywords WoT Multi-secret visual cryptography Certification Authorization

0 引 言

近年来,物联网作为信息时代的第三次浪潮得到了迅猛的发展。WoT,即 Web of Things,Web 技术作为跨平台的资源和服务共享基础框架,成为物联网实现泛在计算与异构资源共享的技术选择[2]。当前的 WoT 环境中存在着多种威胁,譬如:丢失身份信息、泄露个人信息以及滥用资源等,身份认证和授权是抵御这些威胁的一种重要手段[3]。

Hasan 等[4]提出了一个通过委托许可结合 OAuth 协议的认证授权方案,但是该方案存在着无法控制令牌权限等缺陷。Google 提出了一种扩展 OpenID 和 OAuth 的协议[5],但是该协议存在无法满足依赖方 RP(Relay Part)和 OAuth 使用者不同时的认证需求。OpenID Connect 协议是 2014 年发布的重要单点登录认证协议标准,目前该协议已经被广泛应用到 WoT 行业中。但是,该协议存在认证不完整以及用户口令安全性强度不够的缺陷[6]。

本文提出一种多秘密可视密码方案,通过两种叠加方式能够恢复出两个不同的秘密可视密码方案,结合 OpenID Connect 协议能够有效地解决该协议中认证不完整以及口令安全性强度不够的问题,也可以实现控制权限。可视密码技术可以在少量分存中隐藏多个

收稿日期:2018-05-07。**韩妍妍**,助理研究员,主研领域:可视密码,信息安全。**张京**,硕士生。**闫晓璇**,硕士生。**李娜**,硕士生。

秘密信息[7],具有技术实现简单、计算复杂度低等优点。

1　基础知识

1.1　多秘密可视密码技术

常规的可视密码方案生成的共享图像是类噪声的,以此来确保秘密信息不可读。由于无法判断所要恢复的秘密图像对应的是哪些共享图像,一旦用户持有的共享图像数量变得庞大,问题会变得更加复杂。具有标签信息的可视密码技术 TVC(Tagged Visual Cryptography)将标签图像隐藏在每个共享中,通过折叠每个单个共享图像就能在视觉上显现出来。然后通过这种有意义的标签图像来识别属于特定秘密图像的共享对,从而方便用户区分管理多个类噪声共享图像。通过将标签图像设置为与每个共享图像相关联的唯一符号,以此建立对未经授权或发生欺骗行为的参与者的验证机制,凡是未经授权或有欺骗行为的共享图像,其标签图像将不能正确地恢复[8]。

1.2　图像伪装

在对噪声图像进行传输时,不希望让攻击者获取实际图像的大小,因此,需要在不能改变图像原有的信息的同时对传输图像的大小进行伪装处理。本方案采用的处理方法是对原有图像进行扩大,即将原来图像的尺寸由 $H \times W$ 变为 $(H+a) \times (W+b)$,伪装后的图像如图 1 所示。扩大后的图像中的 $H \times W$ 部分与原图重合,而多余的边缘部分随机分配二值像素 0 或 1。这样扩大后的图像仍是噪声图,即使攻击者获取了图像,也不能轻易确定原图的大小,加大了暴力破解原图的难度[9]。而服务器和用户在对图像进行传输处理时,会提前约定好图像的大小,服务器在收到用户发来的图像之后会毫无差错地提取出原图。这种方法对于噪声图像的伪装传输是有效的,而对于有意义的图像传输需要视图像信息进行具体伪装。

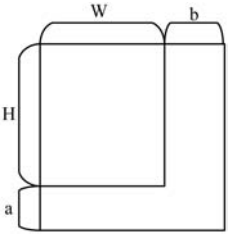


图 1　伪装后的图像

2　方案的设计与实现

本文提出一种新的 TVC 方案,不仅具有 TVC 方案原有的性能,使得分享图像中可以隐藏标签图像的信息,而且恢复的秘密数量有所增加,为可视密码方案增加了更多的信息量。当对齐叠加这两个共享图像,第一个秘密图像就会出现;当把一个共享图像上下翻转再互相叠加,第二个秘密图像就能出现。方案中恢复的秘密图像和标签图像具有良好的视觉识别度[10]。

列举本方案所需要的几个角色,分别是终端用户 EU(End User)、OAuth2 中受信任的客户端 RP(Relying Party)以及用来为 RP 提供 EU 的身份认证信息 OP(OpenID Provider)。其中,OP 包含令牌端点 TE(Token Endpoint)、授权服务器(OAuth2 服务器)以及 UserInfo EndPoint,TE 是主要用于令牌的生成与发送。本方案的总流程图如图 2 所示。

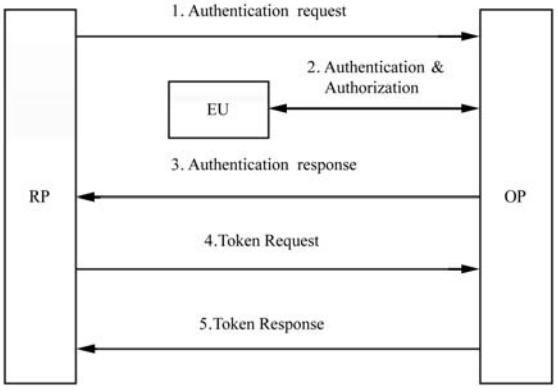


图 2　方案流程

主要步骤如下:

(1) RP 向 OP 发送一个请求认证;

(2) OP 通过使用多秘密可视密码技术对 EU 进行身份认证,并进行授权;

(3) OP 将 ID Token 和 Access Token 返回给 RP;

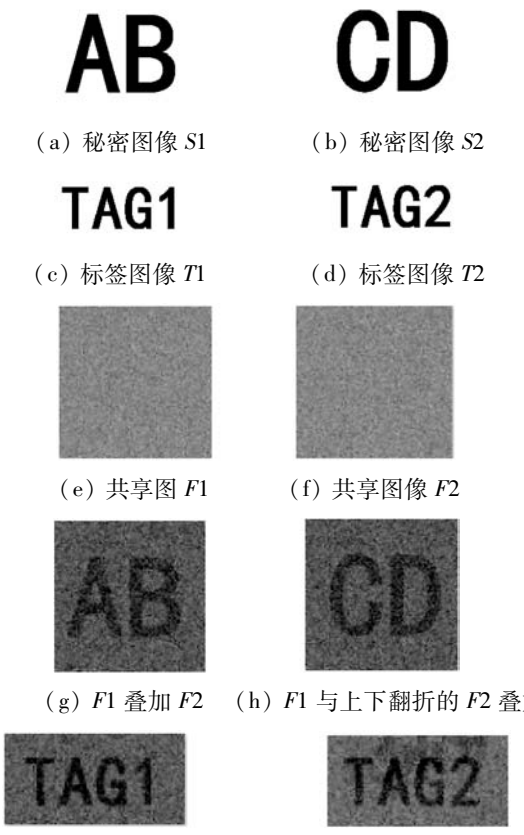
(4) RP 使用 Access Token 发送一个令牌请求;

(5) 令牌响应。

2.1　多秘密可视密码方案构造

假设有两个大小为 $H \times W$ 的秘密图像 $S1$ 和 $S2$,还有两个将要被加密为分享图像的大小为 $H/2 \times W$ 的标签图像 $T1$ 和 $T2$,即标签图像的大小与秘密图像对折之后的大小相同。经过方案的加密过程,将会产生两个共享图像。当直接对齐叠加两个共享图像时,秘密图像 $S1$ 将会显示,将其中一个共享图像上下翻转,再相互叠加,此时将恢复出秘密图像 $S2$。另外,对于每个共享图像,沿着图像的横向对称轴上下对折,将会分别呈现出隐藏的标签图像。

仿真实验如图 3 所示。加密过程分为如下几个阶段:第一步利用(2,2)随机栅格技术[2],将给定的两个秘密图像 $S1$ 和 $S2$(图 3(a)(b))加密成一组过渡图像 $G1$、$G21$ 和 $G22$。第二步,将标签图像加密成两个过渡图像 $L1$ 和 $L2$。最后,将 5 个过渡图像 $G1$、$G21$、$G22$ 和 $L1$、$L2$ 组合起来形成最终的共享图像 $F1$ 和 $F2$(图 3(e)(f))。



(a) 秘密图像 $S1$　(b) 秘密图像 $S2$

(c) 标签图像 $T1$　(d) 标签图像 $T2$

(e) 共享图 $F1$　(f) 共享图像 $F2$

(g) $F1$ 叠加 $F2$　(h) $F1$ 与上下翻折的 $F2$ 叠加

(i) 恢复 $F1$ 的标签图像　(j) 恢复 $F2$ 的标签图像

图 3　恢复后的图像 $q=0.5$

步骤 1　根据秘密图像 $S1$ 和 $S2$ 利用(2,2)随机栅格技术[8]生成过渡图像 $G1$、$G2$。对共享图像 $G1$ 中的某个像素 $G1(i,j)$以相同的 1/2 的概率进行随机取 0(白色)或 1(黑色)的操作,直至全部像素 $G1(i,j)$都被处理。分别将 $S1$ 和 $S2$ 和 $G1$ 按照(2,2)随机栅格技术生成过渡 $G21$ 和 $G22$,再将 $G22$ 经过上下翻转得到 $G22'$。随机生成一个数 k 且 $0\leqslant k\leqslant 1$。如果 $k\leqslant 1/2$,则将像素 $G21(i,j)$分配给 $G2(i,j)$,否则将 $G22'(i,j)$分配给 $G2(i,j)$,直到所有像素处理完。

步骤 2　根据标签图像 $T1$ 和 $T2$(图 3(c)(d))生成过渡图像 $L1$ 和 $L2$。先按照(2,2)随机栅格技术将 Tx $(x=1,2)$生成两个过渡图像 $Cx1$ 和 $Cx2$,再将 $Cx2$ 上下翻转再与 $Cx1$ 上下拼接起来,形成 Lx,其中 $x=1,2$。

步骤 3　将过渡共享图像 $Gx(x=1,2)$和 $Lx(x=1,2)$组合为最终共享图像 $Fx(x=1,2)$。给定一个概率值 p,再随机生成一个数 q 且 $0\leqslant q\leqslant 1$。如果 $q\leqslant p$,则将像素 $Gx(i,j)$分配给 $Fx(i,j)$,否则将 $Lx(i,j)$分配给 $Fx(i,j)$。

方案的解密过程只需要通过简单的叠加及翻转。当叠加分享图像 $F1$ 和 $F2$,秘密图像 $S1$ 即可恢复(图 3(g));将 $F1$ 与上下翻转过的 $F2$ 记为 $F2'$ 相互叠加,秘密图像 $S2$ 即可恢复(图 3(h))。并且通过将共享图像按其横向对称轴进行对折,就可看到隐藏在共享图像中的标签图像(图 3(i)(j))。

2.2　整体方案设计

2.2.1　认证请求

RP 要获取 EU 在 OP 上的私有数据,首先向 OP 发送身份认证请求信息。该请求消息包括 client_id、response_type、scope、redirect_uri 和 state 这五种重要参数。其中:client_id 是指客户端的 id;response_type 是指授权方式的响应类型;scope 是指访问阈值;redirect_uri 是指重定向地址;state 表示请求和反馈之间的状态值。

2.2.2　向认证及授权

Authorization Server 首先判断来自 RP 发送的请求信息中 client_id 的有效性,如果无效则停止认证。如果有效则 Authorization Server 产生认证 EU 的请求消息。EU 将一张随机栅格图像 g 和注销认证码存储起来,同时,自动生成临时随机数 N。再根据自己的 ID 生成对应的标志图像 TUSER,根据随机数 N 生成对应的随机数图像 SN。将图像 SN 和 TUSER 作为两个秘密图像,将图像 g 作为其中的一个分享图像,利用之前的多秘密可视密码算法,加密生成对应另外一个分享图像 $F1$。将 $F1$ 的大小进行伪装后和 ID 一起发送给 Authorization Server。

Authorization Server 先判断 ID 的有效性,如果无效就停止认证。如果有效,则 Authorization Server 根据 ID 找到对应的图像 g,从伪装的 $F1$ 图像中提取出真正的 $F1$ 图像,将 g 与 $F1$ 进行叠加;从恢复的第一个秘密图像中读取 EU 标志信息 ID,并验证与 Authorization Server 发送的 ID 是否一致。再将 $F1$ 上下翻转后再与 g 叠加,从恢复的第二个秘密图像中读取用户发送的随机数 N。以上过程完成了 Authorization Server 对 EU 的认证。

Authorization Server 将图像 SN 和自己的标志图像 TSERVER 作为两个要隐藏的秘密图像,将 EU 的分享图像 g 作为其中的一个分享图像,加密生成对应的分享图像 $F2$。然后将图像 $F2$ 进行大小伪装后发送给 EU 进行验证。

当 EU 收到伪装图像 $F2$,先提取出真正的 $F2$,将其与 g 进行叠加,从恢复的第一个秘密图像中读取标志信息,并验证与此时通信的服务器是否一致。再将 $F2$ 进行翻转后再与 g 叠加,可从恢复的第二个秘密图像中读取用户发送的随机数 N,并验证是否与 Authorization Server 此次会话发送的随机数一致。如果都一致,则这一过程完成了 EU 对 Authorization Server 的认证。

双向认证之后,再发送授权验证码。EU 将随机数 $N+1$ 生成图像 $SN+1$,以图像 g 作为一个分享图像,再利用(2,2)随机栅格可视密码算法,生成另一个分享图像 $F3$,将 $F3$ 大小伪装处理后发送给 Authorization Server。Authorization Server 收到伪装大小的图像 $F3$,从中提取出真正的 $F3$,与分享图像 g 直接叠加,验证收到的图像信息,如果是 $N+1$,可确认是刚才会话的 EU,则开始分发授权验证码。Authorization Server 随机生成会话密钥 m,再生成对应的验证码图像 Sm,然后将图像 $SN+1$ 和图像 Sm 作为两个要隐藏的秘密图像,将 EU 的分享图像 g 作为其中的一个分享图像,利用所构造的多秘密可视密码算法,加密生成对应的分享图像 $F4$。将图像 $F4$ 进行大小伪装处理后返回给 EU。

当 EU 收到大小伪装后的 $F4$,从中提取出真正的 $F4$,将其与 g 进行叠加,从恢复的第一个秘密图像中读取随机数,并验证是否是 $N+1$ 以确保发送密钥的 Authorization Server 是会话的服务器,没有被第三方欺骗。如果不是,则拒绝会话。如果是,将 $F4$ 进行旋转再与 g 叠加,可从恢复的第二个秘密图像中读取授权验证码信息 m,此时需要用户将验证码 m 手动输入,会在客户端生成对应的图像。此时的文字不再是扭曲的,以便 Authorization Server 可以自动识别。EU 将验证码图像和随机数 $N+2$ 当作两个秘密,以 g 为分享图像,用同样的算法加密生成另一个分享图像 $F5$ 发送到 Authorization Server。最后 Authorization Server 验证收到的随机数是否等于 $N+2$,以及验证码是否等于 m,如果相等,则 EU 产生一个授权消息 End_user grant 给 Authorization Server。认证和授权过程如图 4 所示。

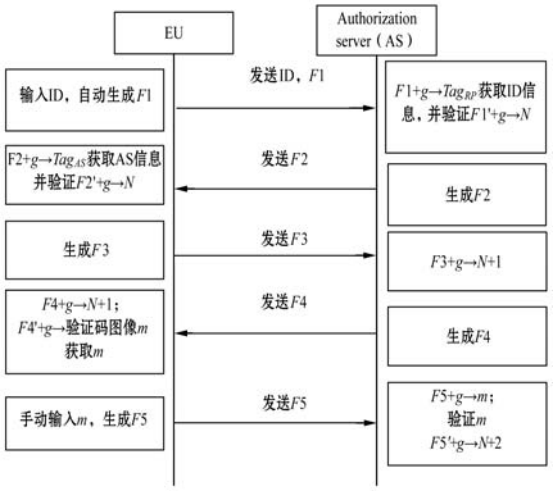


图 4　认证流程

2.2.3　认证响应

Authorization Server 收到 EU 的授权消息之后,将包含有授权码 code 和身份令牌 id_Token 的认证响应消息生成分别包含授权码 code 和令牌 id_Token 的两个图像 $S1$ 和 $S2$。然后通过之前提到的多秘密可视密码构造方案进行加密处理,发送给 RP。

2.2.4　令牌请求

RP 收到秘密图像之后,先进行解密处理,获取到授权码 code。然后检查授权码是否合格,验证成功之后,生成一个令牌请求。该请求消息中包含了 4 个主要参数,分别是 code、client_id、radirect_uri、RP 和 OP 公用的随机栅格图像 g。其中,RP 需要用授权码 code 换取访问令牌 Access Token。最后 RP 将令牌请求(Token Request)发送给 OP。

2.2.5　令牌响应

当 OP 收到令牌请求消息之后,首先验证授权码和时间戳,验证成功之后,产生令牌响应消息 Token Response。其中,令牌响应消息中包括 4 个主要参数:Access Token、token_type、id_token 以及 express_in(Access Token 的生命周期)。

3　性能分析

3.1　可行性分析

在本协议中主要运用了(2,2)双秘密可视密码算法进行秘密信息的传递。EU 和授权服务器具有公共的分享图像,双方根据要传递的秘密图像和公共分享图像 g,使用本节的多秘密可视密码算法,加密生成另外一个分享图像。通过传递该分享图像来秘密传输各自的标志图像信息、随机数信息及验证码信息进行判断及认证,并且从每个分享图像不会得到原始秘密图像的任何信息。当对两个分享图像进行叠加,就能显示出原始的标志图像、随机数图像以及验证码图像,双方均通过传送各自的标志图像实现了相互认证。在每次交互式通信过程中一项重要的安全防护措施就是对随机数信息的传递,协议全程以此随机数为主线,保障了认证过程中一定是此次会话中的合法用户及合法服务器,增加了认证的安全性。在协议交互认证的最后,服务器向用户发送了只有人类视觉系统能识别的验证码,确保了人类的参与,避免使用计算机代理技术自动登录代替用户采取行为。

3.2　安全性分析

3.2.1　冒充攻击

假设攻击者猜测到一个合法的用户 ID 并伪造出一个随机数 N,试图生成一张分享图像发送给服务器。然而用户能够生成一张合法的分享图像的前提是具有用户和服务器共享的分享图像 g,而攻击者在知道分

享图像真实大小的前提下猜测成功的概率为(1/2)$^{H\times W}$。若攻击者截获到用户发送给服务器的分享图像 $F1$,企图模拟合法服务器,此时攻击者需要生成分享图像 $F2$,而 $F2$ 是由服务器的标志图像及随机数 N 还有共享合法图像 g 所确定。由于攻击者只有 $F1$,从中无法推出随机数信息,也没有共享图像 g 的信息,即使伪造服务器的标志图像也无法通过用户的验证[11]。因此,冒充攻击是无法实现的。

3.2.2 重放攻击

对于每个新的登录请求,本协议生成不同的随机数 N。如果攻击者获取到上一次认证中用过的 $F1$,并将其转发给服务器,即使攻击者收到服务器返回的 $F2$,没有用户和服务器的共享图像 g,攻击者也无法解密此次会话中的随机数 N,也无法构造 $F3$ 继续向服务器请求验证码图像,因此可有效抵制重放攻击。

3.2.3 中间人攻击

假设攻击者通过各种技术手段,可以截取用户和服务器之间的通信信息,并试图修改信息进行欺骗。当攻击者获取用户发送给服务器的 $F1$,由于 $F1$ 是噪声图像,无法得到任何相应的秘密信息,能够成功解密的唯一途径就是具有用户和服务器的共享图像 g。但此共享图像 g 并没有在认证过程中进行传输,攻击者获取的任何信息都无法解密,也无从伪造后续传递的信息,因此在第三步服务器要确认随机数 $N+1$ 时就会被拒绝,所以中间人攻击也会失败。

3.2.4 口令猜测攻击

本方案中的认证协议的安全性很大程度上决定于用户与服务器之前的共享图像 g,一旦图像 g 遭到成功的猜测,则攻击者将会完成控制整个认证过程。但要猜测出正确的共享图像 g 具有两大问题:(1) 因为在信道中传输的图像的大小是经过伪造的,而且每次的大小都是不同的,所以攻击者无法确定共享图像 g 的大小。(2) 即使攻击者确定了共享图像的大小,假设其尺寸为 128 × 128,则能够成功暴破的概率为(1/2)$^{128\times128}$。综合这两种因素,试图猜测共享图像 g 也基本无法成功。

3.3 效率分析

本文设计的认证授权协议中采用的加密方法主要是基于随机栅格的多秘密可视密码算法,而常规身份认证协议中采用的加密方法主要有对称加密算法如 AES 和非对称加密算法如 RSA。本文采用的基于随机栅格的可视密码算法基于图像像素点的逻辑运算,AES 算法基于数据的排列和置换,而 RSA 算法基于大数分解,三种算法的计算复杂度依次升高。为了对这三种算法进行定量分析,本文对它们的加解密速度进行测试,即同时加密相同长度的明文,比较三种算法完成加密及解密所消耗的总时间如表 1 所示。

表 1 三种密码算法对比图

加密算法	(2,2)多秘密可视密码算法	AES	RSA
运行时间	0.11 s	1.06 s	858 s

文献[12]除了运用可视密码方案,还用到对称加密算法和 MAC 消息验证码,相较而言,本文的认证效率相对较高。文献[13]使用公钥对方案中的图像密钥进行更新,而本方案只是重新生成随机栅格实现密钥的更新,在计算成本上有所减小。与文献[14]相比,两个方案都用到随机数发生器,但文献[14]使用消息验证码对消息进行验证,而本方案使用随机数 N 来实现验证功能,确保消息没有被篡改,效率更高。

综上,本文提出的结合多秘密可视密码方案的 OIDC 协议能够有效完成 EU 与服务器之前的双向认证,并能抵抗常见的攻击,具有良好的安全性能。另外,相比于常规的现代密码算法更加简单,易于实现,而且加解密速度更快。此方案在 WoT 下可以节省更多开销,提高计算性能。

4 结 语

OIDC 协议使用安全传输层协议等来保证其安全性,但是,部署安全传输层协议需要很大且十分复杂的开销,大大降低了通信的效率。同时,该协议在 EU 和授权服务器的双向认证上,假设攻击者获取到相关参数进行攻击会使得双方失去相互认证性。并且,攻击者能够截取到用户口令,这使得用户口令失去秘密性。本方案采用多秘密可视密码技术,其保证在少分存的前提下,安全有效地完成 EU 和授权服务器的双向认证,其中未涉及到用户口令,从而保证了用户口令的秘密性。本方案在交互过程中可以一次传递两个互相制约的秘密信息,而且每次交互过程中通过随机数信息来保证会话的一致性,增强方案的安全性能。此外本方案的登录验证码可以防止机器暴力破解。可行性、安全性和效率分析表明了本协议能够提供有效安全的认证和授权功能,此方案不仅在运行效率上具有优势,而且安全性也具有保障。

参 考 文 献

[1] OpenID. What is OpenID Connect? [EB/OL]. http://openid.net/connect.

(下转第 333 页)

4 结　语

本文提出了以总旅行预算费用为约束条件获取最大旅行体验的旅游景点规划问题,建立了景点综合评价指数模型。通过 0 - 1 背包算法求得费用约束条件下综合评价指数最高的景点集合,再利用旅行商算法遍历景点获取最短游览路径以降低交通费用,最后通过二分法循环优化上述过程得到景点规划最优解。

本文以南京主要景点为例给出其景点评价指数和景点距离矩阵,通过上述优化算法分别对预算总费用为 1 000 元和 500 元两种情况进行规划,其规划景点及游览路径合理,满足预算费用要求。

参 考 文 献

[1] 袁光辉, 谢科, 邓林胜,等. 旅游路线动态规划问题研究——以西安市出发为例[J]. 数学的实践与认识, 2016, 46(15):125 - 133.

[2] 王艳, 印国成, 孙茂圣. 最佳游览路线生成方案的设计与实现[J]. 物联网技术, 2015, 5(12):87 - 89.

[3] 杨丽萍. 最短路径算法在校园导游系统中的应用[J]. 计算机时代, 2014(2):31 - 32.

[4] 邹时林, 阮见, 刘波,等. 最短路径算法在旅游线路规划中的应用——以庐山为例[J]. 测绘科学, 2008, 33(5): 190 - 192.

[5] 徐婷婷, 王柱, 徐海洋. 旅游路线规划数学模型的建立与应用探讨[J]. 廊坊师范学院学报(自然科学版), 2016, 16(1):23 - 26.

[6] 蓝雯飞,吴子莹,杨波. 背包问题的动态规划改进算法[J]. 中南民族大学学报(自然科学版), 2016, 35(4): 101 - 105.

[7] 王乐, 王世卿, 张静乐. 基于 Matlab 的 0 - 1 背包问题的动态规划方法求解[J]. 计算机技术与发展, 2006, 16(4):88 - 89.

[8] 王永静. 基于动态规划法和模拟退火算法求解旅行商问题[J]. 商丘职业技术学院学报. 2016,15(5):5 - 7.

[9] 王敏. TSP 问题及几种常见算法的比较研究[J]. 长春理工大学学报, 2010(5):184 - 185.

[10] 张子寒, 张落成. 基于多种模型的旅游线路规划探讨——以南京主要景区游览为例[J]. 计算机应用,2016, 36(S1):278 - 280.

[11] 携程. 南京景点推荐[DB/OL]. http://you. ctrip. com/sight/nanjing9. html.

(上接第 312 页)

[2] 马德新. 基于 Web 的物联网体系结构和感知域关键技术研究[D]. 北京:北京邮电大学,2014.

[3] 胡朝建. 一种物联网开放平台认证授权机制的设计与实现[D]. 广州:华南理工大学,2014.

[4] Hasan R, Winslett M, Conlan R, et al. Please permit me: stateless delegated authorization in mashups[C]//Annual Computer Security Applications Conference(ACSAC). 2008: 173 - 182.

[5] OpenID OAuth Extension Website[EB/OL]. http://step2. googlecode. com/svn/spec/openid_oauth_extension/lastest/openid_oauth_extension. htm.

[6] 鲁金钿, 尧利利, 何旭东,等. 改进的 OpenIDConnect 协议及其安全性分析[J]. 计算机应用, 2017, 37(5):1347 - 1352.

[7] 韩妍妍. 可视密码技术的研究[D]. 西安:西安电子科技大学,2009.

[8] 杨健, 汪海航, 王剑,等. 云计算安全问题研究综述[J]. 小型微型计算机系统,2012, 33(3):472 - 479.

[9] Ranjbar N, Abdinejadi M. Authentication and authorization for mobile device[D]. Sweden: University of Gothenburg, 2012.

[10] Jones M, Handt D. The OAuth 2.0 authorization framework: bearer token usage[EB/OL]. https://tools. ietf. org/html/rfc6750.

[11] Zhang J L, Lu J T, Wan Z Y, et al. Security analysis of OpenID connect protocol with cryptoverif in the computational model[C]//Proceedings of the 11th International Conference on P2P, Parallel, Grid, Cloud and Internet Computing. Berlin:Springer, 2016:925 - 934.

[12] 杨雪松,王书文,刘勇,等. 一种基于视觉密码的云平台访问控制方案[J]. 甘肃科技,2014, 30(3):11 - 13.

[13] 曹晟,陈峥,崔喆,等. 基于视觉密码的无线网络远程身份认证[J]. 计算机应用,2008, 28(6):39 - 42.

[14] 冯国柱,李超,吴翊. 基于视觉密码的身份认证方案[J]. 计算机应用,2006,26(10):2318 - 2319.

(上接第 328 页)

[7] 张鹏伟,李建文. 数据库系统开发中字符编码问题的研究[J]. 陕西科技大学学报,2013,31(5):139 - 143.

[8] 闫静,王天宝,罗浩. 应用开发中的中文乱码原因及其解决方案[J]. 成都信息工程学院学报,2012,27(5):458 - 461.

[9] 谭园园. WEB 开发中的乱码及其解决方法[J]. 数字技术与应用,2012(7):86 - 88.