基于累加方法的防肩窥图形密码系统的设计与实现

文伟平，尹燕彬
（北京大学软件与微电子学院，北京 102600）

摘 要：本文首先对文本口令认证方式和图形密码方式进行了调研，指出了目前常规身份认证方式在现实应用中存在无法防肩窥的问题。然后阐述了当前的几种防肩窥密码系统的设计思想，分析各个系统的特性。在此基础上提出了基于累加方法的防肩窥图形密码系统，详细地陈述了该系统的设计原则及验证流程，并对其安全性和可用性进行了详细论述，并指出了该系统可能的应用场景。

关键词：身份认证；防肩窥；图形密码
中图分类号：TP309.7 文献标识码：A

0 引言

随着计算机技术和互联网的飞速发展，计算机用户需要经常访问不同的服务器以获取不同的资源。而用户在登陆服务器的时候，需要进行身份认证来确保相应的资源只被合法的用户使用，同时需要识别非法用户恶意的伪造登陆信息的行为，保护信息资源的安全性。

身份认证是指证实主体的真实身份与其所声称的身份是否相符的过程。任何拥有存取控制的非开放的信息系统必须解决身份认证的问题。现有的身份认证技术主要分为三类：基于所知、基于所有和基于所是的认证方式。文本密码是目前得到广泛应用的基于所知的身份认证方式，文本密码既要求易于记忆，又要求难于猜中或者发现、抗分析能力强。但文本密码同时面临字典攻击、密码难于记忆、密码管理困难等问题。图形密码作为文本密码的替代者很好的解决了这个问题，它利用人类对图形记忆要优于对文本记忆的特点设计出来的，用户不用记忆冗长的字符串而是通过识别或记住图形来进行身份认证[1]。肩窥攻击是一种利用直接观察就可以得到所需要信息的攻击技术。肩窥攻击一般发生在相对临近的环境中，在这种环境中攻击者可以很容易的看见临近的人填写的标单、在 ATM 机器上录入的 PIN 和在屏幕上显示的各种信息等等。对于基于所知的身份认证机制有着非常大的威胁。图形密码可以实现容易记忆和防止字典攻击，但是容易受到肩窥攻击。因此，防肩窥图形密码系统作为新的身份识别技术也日益成为研究和应用的热点之一。

1 相关认证技术调研

1.1 文本口令认证

基于文本的口令认证以其简单易行、使用面广的特点成为现在使用最为广泛的身份认证技术。在计算机系统中，操作系统、网络、数据库均采用了口令验证的形式。但是这种方式存在着较大的安全隐患，主要是可记忆性与抗破解能力之间的权衡。如果设置易于记忆的口令，那么攻击者可以通过搜索口令字典数据库的方法对其进行字典攻击；如果设置的口令长度过短，则口令空间过于狭小，攻击者可以采用暴力破解的方法在有效的时间内找到口令密码。要提高抗破解能力的唯一方法是增加口令的长度，并少用人类熟悉的字符串，但是这样可记忆性就会减弱。其次，文本口令的口令空间只包含 94 个字符，这直接限制了其安全性的上界，可以从理论上证明基于文本口令的验证机制安全性的不足。针对口令验证的弱点，目前主要使用单向函数加密口令、用数字签名方式验证口令和一次性口令等几种改进机制的数字密码。一个不加其它防护手段的数字密码很容易遭受穷举所有输入的攻击。因而密码的选择还应增加其他的一些特殊字符，增大密钥空间，提高密码被破解的复杂度。

1.2 图形密码

图形密码机制作为传统的文本口令的替代者被提出。图形密码是通过让用户在图形用户界面上显示的图像中按照特定的顺序进行选择来工作的，是利用人类对图形记忆要优于对文本记忆的特点设计出来的一种新型密码。

由于人类对图形的记忆优于对文本的记忆，因此可以通过增大图片库容量的方法来提高口令空间，提高系统安全性的同时也不会降低可记忆性。对于这种新型的口令，很难采用现有的攻击方法来攻击。由于图片库大，使用暴力破解是不可行的，同时图形中包含的信息庞大且不容易用语言描述，不容易泄露出去。其次，图形密码一般采用鼠标输入的方式，比文本密码的键盘输入更加难以猜测，攻击者跟踪鼠标输入相当困难。因此图形密码对于抗暴力破解、抗字典攻击、防重放攻击等方面相当有效[2]。但是一般的图形密码机制和文本口令方式同样，由于每次用户输入或选择同样的口令或图形，几乎不具备任何防肩窥攻击的能力。因此提出有效的可以对抗肩窥攻击的图形密码方式成为目前密码

认证系统迫切的安全需求。

2 防肩窥图形密码系统的设计与实现

2.1 防肩窥攻击原理

肩窥攻击也称为窥视攻击，是一种利用直接观察就可以得到所需要信息的攻击技术。肩窥攻击一般发生在相对临近的环境中，特别是在比较拥挤的地方，在这种环境中攻击者可以很容易的看见临近的一些人所填写的标单、在 ATM 机器上录入的 PIN、在公用电话上使用的电话卡、在屏幕上显示的各种信息等等。当然在摄像头、望远镜、录像机等硬件设备和远程控制软件的支持下，肩窥攻击的发生可以没有时间空间的限制。同时它也属于一种社会工程攻击，对于基于所知的身份认证机制有很大的安全威胁。肩窥攻击被人提出已经有 20 多年的历史，随着移动网络和移动计算的发展越来越得到了重视和发展。

肩窥攻击基本上有四种形式：临近偷看、使用设备、声学跟踪、电磁泄露。其中临近偷看是现实生活中最为常见和容易的肩窥方式。目前主要通过引入其余认证方式、改变知识的输入方式和知识动态变化等方式解决肩窥攻击的问题。其中知识动态变化可以采用挑战响应协议。在挑战响应协议中，首先想要得到认证的用户向服务器发送认证请求，服务器对此发回任意的数值。用户按照特定的算法合成用户输入的口令和挑战，生成响应的数值，再发回给服务器。在服务器方面，用发送给用户的挑战和预先登记的用户口令制作响应，与被传送回的响应比较。如果响应相符，则口令正确，认证成功。此外还可采用零知识证明的方式来对抗肩窥攻击。零知识证明是身份认证者知道某种事物或某种认证算法，而肩窥者不能通过你的证明知道这个事物或这个算法，也就是不能掌握你知道的信息。由于在证明的过程中没有透露认证者的任何信息，因此可有效地对抗肩窥攻击。下面从数学理论上分析一下防肩窥攻击机制的实现机理。

在防肩窥攻击机制中，为了达到防肩窥的目的，用户每次输入的登陆口令并不是注册时选择的密码，而是能够反映用户知道注册时选择的密码的另一种形式，因此在登陆口令和选择的密码之间存在着一定的映射关系，函数 Z=f(N) 表示一次登陆过程中可能的口令和密码之间的映射关系，其中 N 表示一次登陆过程中所有可能存在的密码组合。用户选择的密码 $p \in N$ 且 p 具有唯一性。Z 表示一次登陆过程中输入的登陆口令。利用 $N=f^{1}(Z)$ 公式，从攻击者角度分析，肩窥者通过肩窥得到登陆过程中输入的登陆口令 Z，然后分析出 N 这个集合，再从 N 中分析出用户的密码 p。下面给出密码空间的定义：

选择密码空间 (Select Password Space，简称 SPS)：表示用户注册时可选择的密码空间大小。

输入密码空间 (Enter Password Space，简称 EPS)：表示用户每次登陆时可输入的密码空间大小。

防监窥能力 (Anti-should-surfing Ability，简称 ASA)：定义 ASA=log2(|SPS|/|EPS|)，当它的值大于零时，指平均对于单位个输入口令，我们在理论上可以求出的对应的可能的密码空间势的位数最小值。比如为 8，说明通过分析平均最少可以排除到只剩下 2^8 个可能的密码。数值越大，说明我们求出的对应密码空间越大，攻击者也就更难获得真正的密码。当它的值小于等于零时，我们认为这个系统是不安全的。

密码强度 (Password Space Size)：表示选择密码的强度，简称 PSS，定义 PSS= log2|SPS|。

防猜测能力 (Anti-Guess Ability)：表示攻击者直接猜测登陆成功率，简称 AGA，定义 AGA= log2|EPS|。

传统的文本密码之所以不能有效地防肩窥攻击是因为其选择密码空间 SPS 和输入密码空间 EPS 相等。然而，在防肩窥攻击系统中，通常是 EPS<SPS。

上述三个参数 (ASA、PSS 和 AGA) 构成了衡量一个防肩窥系统是否安全的基础。密码强度 PSS 是设计防肩窥系统的重要评估指标，它的大小直接决定另外两种能力的上界。所以我们首先要有足够大的密码空间，例如在图形密码中图形的空间要足够大。对于防猜测能力 AGA，它与攻击者一次成功登录的概率有关。对于这种攻击我们往往可以通过限制登录不成功次数来对抗。而即使是一次成功登录，攻击者也没法拿到密码。所以它的重要性设为中等。而最重要的参数就是防肩窥能力 ASA，它描述了攻击者可能通过肩窥获得密码的能力。对于 AGA 和 ASA，不同的系统要求是不一样的，一般我们认为这两个值比较接近时，系统的设计是比较合理的。

总之，防肩窥攻击密码系统的实现原理主要是采用挑战响应协议，使用户每次登录时输入的口令与注册的密码不同，确保即使攻击者每次都记下或录下用户的登录口令，也不能在有效的时间内推测出用户的注册密码，以此来抵抗肩窥攻击。

2.2 防肩窥密码图片系统

防肩窥密码图片系统实现的基本安全需求：即使攻击者记录下了验证的所有过程和用户的所有输入，攻击者依然无法还原出用户的隐秘信息（密码）。这就要求在验证过程中用户的输入和用户的密码之间的关系不是一一对应的，而是随机变化的。图形密码本身的防肩窥攻击的能力要弱于文本密码。但是可以采用知识的动态变化方法中挑战响应协议来解决这个问题。典型的防肩窥攻击的图形密码机制有以下几种实现方案。

第一种方案 [3]（如图 1），在注册阶段，用户在屏幕上的一系列图片中选择几个口令图片。在认证阶段，系统屏幕上显示一系列用户已经设定的口令图片和很多非口令图片。用户识别出自己的口令图片后，只需在这几个口令图片组成的多边形的中间区域点击即可。由于每一次进行认证时，系统屏幕上显示的图片的位置都不同，因此即使使用摄像设备录下全部过程也不能推测出用户的口令密码。但是系统屏幕上显示的图片总数必须进行详细考虑，如果图片数过多会导致过于拥挤使得用户难以

辨认；如果图片数过少又会使得口令空间小，导致系统不安全。

图1 防肩窥密码图片系统方案一

第二种方案[3]，要求用户识别注册时的口令图片 (例如：注册时选择了 3 个口令图片)，然后通过旋转框架或其中一个图片的方式将这三个图片最终旋转至一条直线上 (图 2)。

图2 防肩窥密码图片系统方案二

第三种方案[3]，要求用户在每一屏显示的图片中都包含用户设定的四个口令图片。认证时用户识别出口令图片后，用户只需能正确点击四张图片的交点即可完成认证 (四个图片的连线一定交于一点且不可见) (图 3)。

图3 防肩窥密码图片系统方案三

第四种方案是 Volker Roth 和 Kai Richter 设计的安全登陆系统 (图 4)[4]，用户密码为 0-9 的数字，每次对用户密码进行验证，如果用户的密码出现在黑色区域，则点击黑键，反之，点击白键。下图是一个对密码为 3 的情况进行验证的过程：

图4 方案四的密码验证过程

在上图中，攻击者通过简单的观察很难得出被验证的密码是 3，可以实现简单防肩窥效果。但如果整个验证过程被记录下来，然后进行详细的分析：

第一次　　白色包含 1 2 3 9 0

第二次　　黑色包含 2 3 6 8 9

第三次　　白色包含 3 4 5 8 0

第四次　　黑色包含 1 2 3 4 6

通过上面的数字陈列，发现 3 是每次都符合验证的数字。

另外，该系统每次输入只有黑键和白键两种输入，这意味着攻击者随意的输入 (非黑即白)，也有可能通过验证。因此这个系统虽然具有一定的防肩窥效果，但整个系统的安全性还有待提高。

2.3 基于累加方法的防肩窥密码图片系统

2.3.1 系统设计原理

系统相关定义：

SN：密码空间

Sn：用户密码，*Sn* ∈ *SN*

Sni：在一次验证中用到的密码，属于集合 *Sn*，*i* ∈ (*0*，*n*)，*Si* ∈ *Sn*

Sx：密码和非密码混合生成的随即序列，用于验证

input：在一次验证过程中用户计算出的结果，作为输入反馈给验证系统

F：一种密码和输入的对应关系，在该系统中是累积集合 *Sn* 中的元素在随机序列 *Sx* 出现的次数。

F (*Si*) =*input*；根据 *i* 的变化，*input* 随之而变化。用户累加 *Si* 中的元素在随即显示序列 *Sx* 出现的次数，即 *input*，输入系统进行验证。如图 5：

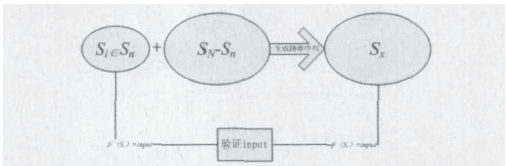

图5 基于累加方法的防肩窥图像密码设计原理图

因此攻击者知道 *F* 函数和 *input*，但不知道 *i*，是无法还原出 *Sn* 的。

我们提出了新的的防肩窥图形密码系统——基于累加方法的防肩窥图像密码系统。密码空间为 30 幅图片，即 *N=30,* 客户需要从中选择 5 幅作为自己的密码图片，即 *n=5*，*i* ∈ *[0,5]*, 在每次验证过程中，系统会显示 15 幅图片，5 幅密码图片在其中按照某种算法随机的出现，客户需要数出密码图片的出现次数，这个次数被控制在 0-9 之间，即 *input* ∈ *(0,9)*, 然后这个次数 *input* 就作为一次输入。重复这样的验证过程 4 次，如果客户的输入正确，就完成了客户身份的验证。

2.3.2 系统的可行性分析

该密码系统需要记住 5 幅图片作为密码，在验证过程中需要数出密码图片的累计出现次数。记住四幅图片的难度和现有的六位枯燥的毫无意义的数字密码难度相比，用户更容易记住图片。

而对密码图片的出现次数进行计数也是非常简单的，我们很多人都有过这样的经历，就是在一个集合中迅速地查找出符合某种条件的个体的数量。例如，在停车场查出所有国产车的数量。

因为这种密码验证的方式适合于各种知识背景和年龄段的人群。

2.3.3 验证流程

用户从程序所展示出来的 30 幅图片中选择 5 幅作为自己的密码，如图 6 所示：

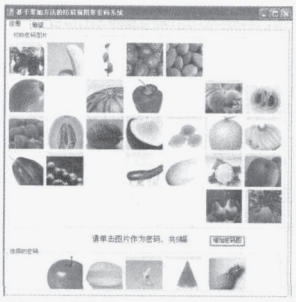

图6 基于累加方法的防肩窥图像密码系统登录界面

在程序的后台，图形密码和一个唯一的编号一一对应， 这样降低了服务器和客户端传送的数据量。注册过程中客户端将用户选定的 5 幅图片对应的编码传送给服务器，服务器根据相应的规则将客户 ID 和对应的密码以及其他客户信息存储到数据库中。

用户根据自己在注册过程中选择的密码图片，计算出密码图片累计在随机序列中出现的次数，将累计的结果输入，进行验证，验证过程如图 7 所示：

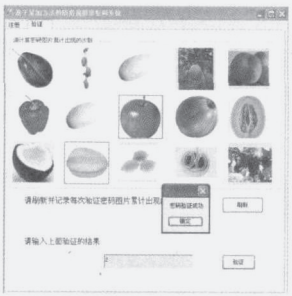

图7 基于累加方法的防肩窥图像密码验证过程实现

服务器端接收到客户端的密码验证请求，根据用户 ID 取出用户的密码图片，然后根据相应的算法生成混合密码图片和非密码图片的随机序列，计算出这个随机序列的结果，然后将这个结果保存，将随机序列发送到客户端。

客户端在收到随机序列后，调用相应的显示模块将随机序列对应的图片序列显示在屏幕上，客户根据自己记忆的图片知识和终端屏幕的显示，计算出结果，输入终端，由终端传送给服务器进行验证，如果服务器的计算结果和客户输入相符则验证成功。

验证过程顺序流程图如图 8 所示：

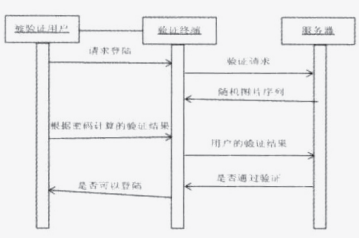

图8 基于累加方法的防肩窥图像密码验证过程顺序流程图

3 系统的安全性分析

3.1 图形序列的生成规则

图形序列的生成规则如下：

（1）密码图片最多可重复 3 次；

（2）非密码图片数组下标为偶数的可重复 3 次；

（3）非密码图片数组下标为奇数的可重复 2 次。

这样的规则是出于混淆密码图片的目的，一方面由于密码图片只有 5 张，非密码图片有 25 张，所以密码图片出现的几率大，设置密码图片的重复次数为 3，可适当提高密码图片出现的几率（这个几率是指单张图片相对于别的图片的出现几率），使得密码图片累计出现次数在 0-9 范围内比较均匀的分布。另一方面，非密码图片中必须要有可以重复出现 3 次的图片，否则一旦一张图片出现 3 次就暴露了自己是密码图片的身份。

3.2 密码生成规则

密码生成规则如下：

（1）四位数之和应该大于等于 8；

（2）四位数之和应该小于等于 30。

这个规则为了预防几种不安全的情况，当输入为 0 的情况下，意味着所有的图片都可以确定为非密码图片，如果重复的出现 0，出现两次理论上有可能暴露所有图片。当出现输入为 9 的情况下，意味着本次验证最多包含 5 张密码图片，最少 3 张，因此重复出现 9 也是很危险的。

3.3 本系统的安全性分析

3.3.1 攻击方式分析

针对本系统的肩窥攻击主要有三种：

（1）穷举攻击，其困难度是 10n ，其中 n 为密码验证的轮数。我们采取 4 轮验证，因此这种攻击的困难度应该是 104；

（2）是试图猜测密钥图片，假设我们有 30 幅画，选择其中的 5 幅作为密码，这种方法需要实验 30*29*28*27*26/5*4*3*2*1 次；

（3）数学分析，假设攻击者得到了一一对应的验证图片和客户输入，攻击者根据几轮不同的输入之间的联系，可能会排出一些不是密码的图片，也有可能会确认一些图片就是密码，这种方法极有可能成功，因此我们对此做出分析并加以改进。

3.3.2 边界值分析

客户输入为 0 的情况下，本次所出现的图片在最坏的情况下会使攻击者排出 15 幅图，即知道了这 15 幅图不是密钥。他的问题变成了从剩下的 10 幅图中选 5 幅，试验次数为 10*9*8*7*6/5*4*3*2, 难度依然足够大。但是如果连续的输入都为 0，最坏的情况下两次就可以暴露密钥。因此连续的出现 0、1 这样的小数字很危险。但是密码生成的规则限制了连续出现小数的概率。客户输入为 9，最坏的情况是 15-9=6，其中有 6 幅非密码图片（可能有重复）和 9 幅密码图片（可能有重复）。例如：3 幅

（下转 16 页）

使有人通过某种途径得到用户的认证卡，但由于不知 USB 卡密码，故难以使用之；

加密算法采用的是成熟的 RSA 非对称算法，该算法已被证明是安全性很高的一种经典非对称加密算法；

公文收发借用了稳定的 POP3、ESMTP 邮件协议，使得整个系统具有较好的实用性，开发成本较低。虽然该协议对于用户确认机制还不够精密完善，但邮件服务器上存放的所有公文均为加密文件，加上对于登录用户权限已经作了一定限制（如 3 天以内发送的邮件不得删除），这样，即使非法用户攻破服务器，也不能得到明文信息或损毁密文；

加密和解密密钥都存放在身份认证卡上，由用户随身携带，无卡人员根本无法开机，从而保证了本机信息安全；

定期刷新 USB 卡内用于身份认证的种子值和用户公文加密密钥对，并提示用户修改身份认证卡开卡密码。将可能的损失降低到最小的程度。

总之，本系统实现了各用户之间机要公文的分发传输，保障了传输数据的安全性，采用了 USB 口接入的身份认证卡，用软硬结合的手段实现了用户需求，具有很好的推广价值。（责编 杨晨）

课题背景：该课题项目单位目前的网络为局域网，树形结构，总机站连接 6 台分机站，下面再连接多台终端。现有终端至少 200 台。该系统要能在该局域网内部实现，保证高安全等级信息的传递和存储安全，即机要公文的安全分发。其具体要求如下：

要求是最好能有保密等级和权限，例如某高权限网卡对应高级领导的机器，并可以访问低级机器，而低级机器则无法访问高级用户机器；

要求采用 USB 接口卡进行身份认证；

发送的信息应当自动加密。该加密算法应有一定强度，使得恶意攻击者在有限时间内无法破译；

对机密文件给予特殊标志，最好能够实现机密文件的隐藏，进一步防止攻击者的攻击。

作者简介：刘玉（1957-），女，教授，主要研究方向：计算机网络安全、多媒体通信；王长强（1980-），男，硕士研究生，主要研究方向：计算机网络安全、量子密码学；李豫霞（1974-），女，讲师，硕士研究生，主要研究方向：经济犯罪案件侦查、计算机犯罪侦查取证。

（上接 10 页）

密码图片重复出现 3 次，而非密码图片无重复 3 次的情况出现，这时候攻击者很显然会主动猜测 3 幅重复 3 次的图片为密码，但还有两张密码图片是未知的。这种情况出现的概率是 C53/(C54+ C54+ C53)*(C153+ C154+ C152)/(C153+ C154+ C152+ C153+ C154+ C155+ C156) =0.37。前提是 3 幅密码图片重复出现 3 次，这个概率是很小的。

另外，攻击者不但会单独分析一次验证过程，还会利用各轮验证之间的联系进行分析，记录每张图片在不同的验证过程出现的次数。如果在两次验证中，密钥图片相同，非密钥图片却完全不相同（即非密钥图片没起到干扰的作用），并且客户的输入也相同，这样对于分析攻击是非常有利的。最坏的情况下，连续两次出现 9，而 5 张密钥图片都出现了，两次干扰图片完全不同，攻击者对比两张图片序列，把相同的图片提取出来，攻击者就能够获得密钥。

4 结论

本文对防肩窥图形密码机制进行了有效调研的总结，在此基础上，针对目前日益广泛的密码需求提出了一种新的基于累加方法的防肩窥攻击的图形密码机制。 然后给出了该防肩窥攻击图形密码系统的设计与实现。该系统可广泛应用于信息安全的各个应用领域，尤其是身份认证的各类相关应用。但是，防肩窥图形密码机制的研究也是一个长期的过程，还有很多研究工作有待完善：①缺少防肩窥图形密码系统攻击的理论模型。尽管已经有人对于防肩窥攻击的图形密码机制提出了可能的几种方案，但是仍然没有一个统一的衡量图形密码机制防肩窥攻击能力的标准，缺少分析防肩窥攻击能力的模型；②目前的防肩窥攻击的图形密码认证系统基本没有考虑认证过程传输的安全性。（责编 杨晨）

参考文献：

[1] S. Xiaoyuan, Z. Ying, G. Scott. Graphical Passwords: A Survey. In 21st Annual Computer Security Applications Conference(ACSAC) (Dec.5-9), 2005.

[2] M. Kumar, T. Garfinkel, D. Boneh, and T. Winograd, Reducing Shouldersurfing by Using Gaze-based Password Entry. Technical Report CSTR 2007-05, Stanford University, Stanford 2007.

[3] 高晶元 .《一种防肩窥攻击的图形密码的设计和实现》. 硕士研究生学位论文 . 北京大学 .2008.

[4] Volker Roth, Kai Richter, and Rene Freidinger. A PIN entry method resilient against shoulder surfing. In Proc. 11th ACM Conference on Computer and Communications Security, Washington, DC, USA, October 2004.

作者简介：文伟平 (1976－)，男，副教授，主要研究方向：网络攻击与防范、恶意代码研究、信息系统逆向工程和可信计算技术等。尹燕彬 (1984－)，男，北京大学软件与微电子学院，在读硕士研究生，主要研究方向：网络安全。