(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 109214160 A
(43)申请公布日 2019.01.15

(21)申请号 201811072993.8

(22)申请日 2018.09.14

(71)申请人 温州科技职业学院
地址 325806 浙江省温州市六虹桥路1000号

(72)发明人 李余党 许驰 崔晓军

(74)专利代理机构 重庆市信立达专利代理事务所(普通合伙) 50230
代理人 包晓静

(51)Int.Cl.
G06F 21/32(2013.01)
G06F 21/46(2013.01)
G06K 9/00(2006.01)
H04L 29/06(2006.01)

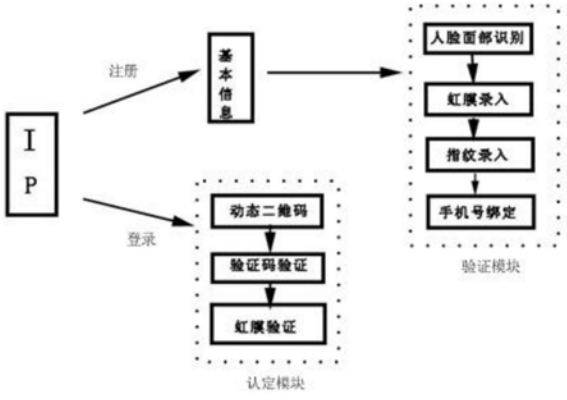
权利要求书9页 说明书20页 附图1页

(54)发明名称

一种计算机网络身份验证系统及方法、计算机程序

(57)摘要

本发明属于信息技术领域,涉及一种计算机网络身份验证系统及方法、计算机程序,计算机网络身份验证系统的IP终端包括登录单元与注册单元,注册单元包括基本信息界面和验证模块,验证模块包括人脸面部识别界面、虹膜上传界面、指纹录入界面;登录单元包括认定模块,认定模块包括动态二维码界面、验证码验证界面、虹膜验证界面;扫描动态二维码界面信息进入验证码验证界面,验证码验证界面信息进入虹膜验证界面。本发明进行了实名认证、人脸面部识别认证、眼睛虹膜认证和指纹认证结合为一体,避免保护个人身份和隐私信息遭到泄露;扫描二维码的方式,提高系统登录的便捷性。



CN 109214160 A

1.一种计算机网络身份验证方法，其特征在于，所述计算机网络身份验证方法包括：

用户注册，填写基本信息之后进行人脸面部识别、虹膜上传、指纹录入；再进行手机号绑定注册；

用户注册基本信息中，需进行基本信息的加密，包括：

第一步，初始化建立算法：首先输入包含所有属性的属性集合U，属性在不同的分层中；然后选择一个阶为N＝$p_1p_2p_3$双线性复合群G，p_1、p_2、p_3为不相同的素数，令G_{p_i}表示阶为p_i的子群，i＝1,2,3；然后选择随机指数a和α、随机群元素$g \in G_{p_1}$、$X_3 \in G_{p_3}$，其中，a,α∈Z_N，Z_N表示1至N-1的整数；对于U中的|U|个属性元素，选择对应的群元素$h_1,...,h_{|U|} \in G_{p_1}$，则公共参数PK和主密钥MSK分别为：

PK＝{N,g,g^{α},e(g,g)^{a},h_1,.....,$h_{|U|}$}；

MSK＝{α,X_3}；

其中，e(g,g)^{a}表示双线性对；

第二步，令属性集合S为属性集合U的分层子集，根据属性集合S、公共参数PK、消息M和一个提前生成的分层门限访问结构(M_V,ρ)将属性集合U所有层次的属性均用一个表达式进行加密得到密文CT，其中，函数ρ表示分层访问结构M_V中的行到属性的映射；令属性集合S的每一层的属性数量超过该层门限，使S满足分层的访问结构；

第三步，通过主密钥MSK和属性集合S，结合步骤S1中的子群G_{p_3}生成密钥SK；

第四步，通过访问结构M_V对应的密文CT和属性集合S对应的密钥SK恢复出消息。

所述分层门限访问结构(M_V,ρ)的生成方法具体如下：

1)系统初始化

定义函数f的运算规则如下：每进行一次f运算，就将多项式的常数项变为0，自变量的系数不变，次数减1，设a、b、c、d为确定的常实数，则有：

f(a+bx+cx^{d})＝0+b+cx^{d-1}；

f(1+2x+$3x^{4}$)＝0+2+$3x^{3}$；

设(k,n)是一个分层的秘密共享系统，主要由一个秘密分发者D和n个参与者组成，属性集合U是n个参与者的集合，且包含m个层次，即$U=\bigcup_{i=0}^{m}U_i$，其中对于i≠j，$U_i \cap U_j$＝Φ；令$\mathbf{k}=\{k_i\}_{i=0}^{m}$是一个单调递增的整数序列0＜$k_0$＜$k_1$＜...＜$k_m$，并且$k_{m-1}$＜$k_m$-1，$k_i$是每一层的门限值，则(k,n)分层的门限访问结构就是要为属性集合U中每个参与者u分配秘密信息s的一个秘密份额σ(u)，使其满足以下访问结构：

$$\Gamma=\left\{S\subseteq U:\left|S\cap\left(\bigcup_{j=0}^{i}U_j\right)\right|\right\}\geq k_i,\forall i\in\{0,1,...,m\};$$

满足上式所描述的访问结构的分层的参与者子集S称为授权子集，可以恢复主秘密，而不满足上述访问结构的任何用户子集将无法获得关于主秘密的任何信息；

2)子秘密分发

秘密分发者D任意选取t-1个随机数a_1,...,a_{t-1}和一个大素数q，然后构造多项式P(x)＝s+a_1x+...+$a_{t-1}x^{t-1}$，其中s是需要被共享的主秘密；系统中的每个参与者u对应域里面的一个元

素表示其身份，用u_j表示，D根据参与者所处的层次i计算参与者的秘密份额$\sigma(u_j)=P_{k_{i-1}}(u_j)$，其中：

$P_0(x)=P(x)$；

$P_1(x)=f^1(P(x))=f(P(x))$；

$P_i(u)=f(P_{i-1}(u))$；

$P_{k_{i-1}}(u_j)$表示多项式P(x)经过k_{i-1}次f运算后在域元素u_j处的值；k_{i-1}是第i-1层的门限值且令$k_{-1}=0$，D公开$\{\sigma(u_1),...,\sigma(u_{l_m})\}$；$l_m$表示第m层中拥有属性集合S的元素数量；

3)秘密恢复

令$S=\{v_1,...,v_{|S|}\}\subset U$，|S|表示S所具有的元素数量，设定满足：

$v_1,...,v_{l_0}\in U_0$；

$v_{l_0+1},...,v_{l_1}\in U_1$；

…

$v_{l_{m-1}+1},...,v_{l_m}\in U_m$；

其中，$U_0,\cdots,U_m$表示集合U的第0至m层，$0\leqslant l_0\leqslant l_1\leqslant...\leqslant l_m=|S|$，当且仅当对于所有的$0\leqslant i\leqslant m$，$l_i\geqslant k_i$，S为一个授权子集，即符合访问结构，则S中所有的参与者合作时，可以组成系数矩阵M_V，其中系数矩阵按行编写为：

$$M_V=\begin{pmatrix}1 & v_1 & v_1^2 & \cdots & v_1^{t-1}\\ & & \cdots & & \\ 1 & v_{l_0} & v_{l_0}^2 & \cdots & v_{l_0}^{t-1}\\ 0 & \cdots\ 1 & \cdots & v_{l_0+1} & \cdots & v_{l_0+1}^{t-1-k_0}\\ & & \cdots & & \\ 0 & \cdots\ 1 & \cdots & v_{l_1} & \cdots & v_{l_1}^{t-1-k_0}\\ & & \cdots & & \\ 0 & \cdots\ 1 & \cdots & v_{l_{m-1}+1} & \cdots & v_{l_{m-1}+1}^{t-1-k_{m-1}}\\ & & \cdots & & \\ 0 & \cdots\ 1 & \cdots & v_{l_m} & \cdots & v_{l_m}^{t-1-k_{m-1}}\end{pmatrix};$$

S中的所有参与者可以合作解出如下的方程组：

$$\begin{cases} s+a_1v_1+a_2v_1^2+\cdots+a_{t-1}v_1^{t-1}=\sigma(u_1) \\ \cdots \\ s+a_1v_{l_0}+a_2v_{l_0}^2+\cdots+a_{t-1}v_{l_0}^{t-1}=\sigma(u_{l_0}) \\ a_{k_0}+a_{k_0+1}v_{l_0+1}+\cdots+a_{t-1}v_{l_0+1}^{t-1-k_0}=\sigma(u_{l_0+1}) \\ \cdots \\ a_{k_0}+a_{k_0+1}v_{l_1}+\cdots+a_{t-1}v_{l_1}^{t-1-k_0}=\sigma(u_{l_1}) \\ \cdots \\ a_{k_{m-1}}+a_{k_{m-1}+1}v_{l_{m-1}+1}+\cdots+a_{t-1}v_{l_{m-1}+1}^{t-1-k_{m-1}}=\sigma(u_{l_{m-1}+1}) \\ \cdots \\ a_{k_{m-1}}+a_{k_{m-1}+1}v_{l_m}+\cdots+a_{t-1}v_{l_m}^{t-1-k_{m-1}}=\sigma(u_{l_m}) \end{cases};$$

即：

$$\begin{pmatrix} 1 & v_1 & v_1^2 & \cdots & v_1^{t-1} \\ & & \cdots\cdots & & \\ 1 & v_{l_0} & v_{l_0}^2 & \cdots & v_{l_0}^{t-1} \\ 0 & \cdots\ 1 & \cdots & v_{l_0+1} \cdots & v_{l_0+1}^{t-1-k_0} \\ & & \cdots\cdots & & \\ 0 & \cdots\ 1 & \cdots & v_{l_1} \cdots & v_{l_1}^{t-1-k_0} \\ & & \cdots\cdots & & \\ 0 & \cdots\ 1 & \cdots & v_{l_{m-1}+1} \cdots & v_{l_{m-1}+1}^{t-1-k_{m-1}} \\ & & \cdots\cdots & & \\ 0 & \cdots\ 1 & \cdots & v_{l_m} \cdots & v_{l_m}^{t-1-k_{m-1}} \end{pmatrix} \begin{pmatrix} s \\ a_1 \\ a_2 \\ \cdot \\ \cdot \\ \cdot \\ a_{t-1} \end{pmatrix} = \begin{pmatrix} \sigma(u_1) \\ \cdots \\ \sigma(u_{l_0}) \\ \sigma(u_{l_0+1}) \\ \cdots \\ \sigma(u_{l_1}) \\ \cdots \\ \sigma(u_{l_{m-1}+1}) \\ \cdots \\ \sigma(u_{l_m}) \end{pmatrix};$$

可以看出，若S满足访问结构，就可以重构出多项式P(x)，从而恢复出秘密S；这个访问结构可以等价于分层矩阵的LSSS的访问结构，即令$I \subseteq \{1,\ldots,l_0,\ldots,l_m\}$被定义为I＝{j:ρ(j)∈S}，如果令$\{\lambda_j = M_v\vec{a}\}_{j\in I}$是秘密s的一个子秘密，则存在常数{ω$_j$∈$Z_N$}使得Σ$_{j∈I}$ω$_j$λ$_j$＝s，其中，$\vec{a} = (a_1,\ldots,a_{t-1})^T$，$Z_N$表示1到N的整数集合；ω$_j$在秘密共享生成矩阵$M_v$大小的多项式时间内总可以被找到，就可以恢复出来主秘密；

登录时通过扫描动态二维码，产生验证码进行输入进入虹膜验证，根据虹膜验证判断登录是否成功；

验证码进行虹膜验证中，需进行虹膜信息的解密，包括：

在得到密文Z′＝(z$_1$′,…,z$_{2l}$′)后，首先计算：

Y′＝L_2^{-1}(Z′)＝(y$_1$′,…,y$_{2l}$′)；

对于点集P中的每一点(μ,λ)，计算：

$$(y_1'',\cdots,y_{2l}'') = \tilde{F}^{-1}((y_1',\cdots,y_{2l}') + \lambda),$$

然后验证Z(y$_1$″,…,y$_{2l}$″)＝μ，如果不成立，则丢弃这组值；否则进行下一步；

最后计算：

M′＝L_1^{-1}(y$_1$″,…,y$_{2l}$″)＝(m$_1$′,…,m$_{2l}$′)，

如果只有唯一的一组(m$_1$′,…,m$_{2l}$′)，那么M′就一定是对应的明文，如果得到超过一组的(m$_1$′,…,m$_{2l}$′)，则用Hash函数或者增加验证方程的方式来确定唯一明文。

2.如权利要求1所述计算机网络身份验证方法，其特征在于，解密前，需先进行虹膜的加密，包括：

公钥生成：公钥由有限域k，以及它的加法和乘法结构和n个二次多元多项式组成；

私钥生成：私钥由映射F～随机选取的r个线性独立的z$_1$,…,z$_r$∈k[x$_1$,…,x$_{2l}$]、一个点集P、两个可逆仿射变换L_1和L_2以及它们的逆组成；

加密过程即给定明文M′＝(x$_1$′,…,x$_n$′)，用选取的公钥进行加密，形成密文Z′＝(z$_1$′,…,z$_n$′)；

中心映射重新构造的过程包括以下步骤：

首先，选择r是一个比较小的整数，随机选择r个线性独立方程

$$z_1(x_1,\cdots,x_{2l}) = \sum_{j=1}^{2l} \alpha_{j1}x_j + \beta_1$$

⋮

$$z_r(x_1,\cdots,x_{2l})=\sum_{j=1}^{2l}\alpha_{jr}x_j+\beta_r$$

映射Z:$k^{2l}\to k^r$如下确定：

$Z(x_1,\cdots,x_{2l})=(z_1(x_1,\cdots,x_{2l}),\cdots,z_r(x_1,\cdots,x_{2l}))$，

其次，随机选取2l个总次数为2的多项式$\hat{f}_1,\cdots,\hat{f}_{2l}\in k[z_1,\cdots,z_r]$，

映射$\hat{F}:k^r\to k^{2l}$如下确定：

然后，定义扰动映射$F^*:k^{2l}\to k^{2l}$为$\hat{F}$和Z的复合：

其中$f_1^*,\cdots,f_{2l}^*\in k[x_1,\cdots,x_{2l}]$，

最后，用内部扰动映射F^*扰动原来的中心映射$\tilde{F}$，新的公钥映射为：

$$\overline{F}=L_2\circ(\tilde{F}+F^*)\circ L_1=(\overline{f}_1,\cdots,\overline{f}_{2l})；$$

公钥生成包括以下步骤：

选取有限域k，以及它的加法和乘法结构；

选取2l个二次多元多项式组：

$f_1(x_1,\cdots,x_{2l}),\cdots,f_{2l}(x_1,\cdots,x_{2l})\in k[x_1,\cdots,x_{2l}]$；

私钥生成包括以下步骤：

选取映射$\tilde{F}$，即两个随机数α_1,α_2；

随机选取r个线性独立的$z_1,\cdots,z_r\in k[x_1,\cdots,x_n]$；

选取一个点集P，P是所有映射$\hat{F}:k^r\to k^{2l}$的像和原像的集合，即：

$$P=\left\{(\mu,\lambda)\mid\hat{F}(\mu)=\lambda\right\},$$

点集P由随机选取的2l个二次多项式$\hat{f}_1,\cdots,\hat{f}_{2l}\in k[z_1,\cdots,z_r]$确定；

选取两个可逆仿射变换L_1和L_2以及它们的逆；

第二步中具体包括如下步骤：

2.1)令访问结构M_V是一个j×t矩阵；

2.2)选择一个随机向量$\vec{y}=(y_0=s,y_1,.....,y_{t-1})\in Z_N^t$，$Z_N^t$表示1到N的整数集合中的任意t个，其中，s表示秘密值，$y_1,.....,y_{t-1}$为秘密值s的分享；

2.3)令$S=\{v_1,...,v_{|S|}\}\subset U$，|S|表示S所具有的元素数量，设定满足：

$v_1,...,v_{l_0}\in U_0$；

$v_{l_0+1},...,v_{l_1}\in U_1$；

…

$v_{l_{m-1}+1},...,v_{l_m}\in U_m$；

其中，$U_0,\cdots,U_m$表示集合U的第0至m层，$0\leqslant l_0\leqslant l_1\leqslant...\leqslant l_m=|S|$，当且仅当对于所有的

0≤i≤m,有$l_i \geq k_i$,l_i表示第i层中拥有集合S的元素数量,k_i表示第i层中集合S的元素数量门限;

然后对于所有的j=1,...,l_0,...,l_m,计算$\lambda_j = M_j \cdot \vec{y}$,$M_j$表示$M_V$中的第j行;

2.4)对于属性集合U的层次数i∈{0,...,m},设定j=l_{i-1}+c,l_{-1}=0,c为常数,表示第i层的第c个属性,即属性集合U中的第j个属性对应于第i层的第c个属性;

2.5)选择随机数$r_{l_0,\ldots\ldots,r_{l_m}} \in Z_N$;

2.6)将所有层次的属性通过以下表达式进行加密得出密文CT:

$$CT = \begin{Bmatrix} C = Me(g,g)^{\alpha s}, (M_V, \rho) \\ C' = g^s \\ C_j = g^{a\lambda_j} h_{\rho(j)}^{-\sum_{x=l_0,\ldots\ldots l_i} r_x} \\ D_{l_0} = g^{r_{l_0}}, \ldots\ldots, D_{l_m} = g^{r_{l_m}} \end{Bmatrix} k_{i-1} \leq j \leq k_i ;$$

其中,$h_{\rho(j)}$表示与属性集合U中的第ρ(j)个属性元素对应的群元素,ρ(j)表示属性集合U中第j层的属性到访问结构M_v的第j行的映射。

3.如权利要求1所述计算机网络身份验证方法,其特征在于,虹膜识别的算法包括:

(1)提取边缘

用CCD获取的眼睛图像,包括巩膜、虹膜、瞳孔和上眼皮部分,将虹膜从整幅图像中分割出来,首先找出虹膜的内外边缘;

选用高斯—拉普拉斯二阶微分滤波器$\nabla^2 G$,$\nabla^2 G$为二维高斯平滑滤波器G(x,y)与拉普拉斯算子$\nabla^2 f(x,y)$的组合:

$$G(x,y) = \frac{1}{2\pi\sigma^2} e^{-\frac{x^2+y^2}{2\sigma^2}}$$

$$\nabla^2 f(x,y) = \frac{\partial^2 f}{\partial x^2} + \frac{\partial^2 f}{\partial y^2}$$

二阶微分滤波器为:

$$\nabla^2 G = \frac{\partial^2 G}{\partial x^2} + \frac{\partial^2 G}{\partial y^2} = \frac{1}{2\pi\sigma^4}\left(\frac{x^2+y^2}{\sigma^2} - 2\right) e^{-\frac{x^2+y^2}{2\sigma^2}}$$

该滤波器虽不是可分离的,写成:

$$\nabla^2 G = \frac{1}{2\pi\sigma^4}\left(\frac{x^2}{\sigma^2} - 1\right) e^{-\frac{x^2}{2\sigma^2}} e^{-\frac{y^2}{2\sigma^2}} + \frac{1}{2\pi\sigma^4}\left(\frac{y^2}{\sigma^2} - 1\right) e^{-\frac{y^2}{2\sigma^2}} e^{-\frac{x^2}{2\sigma^2}} = G_1 + G_2$$

G1、G2均为可分离滤波器,采用分离算法;

2G与图像进行卷积:$\nabla^2 G * g(x,y)$,g(x,y)表示图像上对应点的强度,“*”表示卷积,卷积后获得边缘;

(2)定位虹膜

设虹膜的外圆、内圆方程为:

$(x-x_1)^2+(y-y1)^2=r_1^2$

$(x-x_2)^2+(y-y_2)^2=r_2^2$

用Houg h变换获得(x_1,y_1,r_1)、(x_2,y_2,r_2)两组参数值，$(x_1,y_1)\neq(x_2,y_2)$，不是同心圆；定义外边界圆的圆心(x_1,y_1)为虹膜的中心；定义外边界圆的半径r_1为虹膜的半径，获得中心坐标(x_1,y_1)，获得实时图像相对参考图像的平移量，中心为(p,q)；获得虹膜半径r_1，获得比例变化因子r_1/r，r为参考虹膜的标准半径；

(3)图像匹配

两个边界圆之间区域还包括眼皮部分，需去除该部分，以虹膜的中心为两坐标系的共同原点，将原直角坐标系转化为极坐标系，在极坐标系中，$\{(\rho,\theta)70°<\theta<110°\}$为含眼皮部分，去除；其余为只含有虹膜的部分，保留；

虹膜的旋转变化较小，在±5°，图像的匹配采用相关系数测度：

$$\rho=\frac{C}{\sqrt{C_{gg}C_{g'g'}}}$$

其中，

$$C=\iint_{(x,y)\in D}\{g(x,y)-E[g(x,y)]\}\{g'(x,y)-E[g'(x,y)]\}\mathrm{d}x\mathrm{d}y$$

$$C_{gg}=\iint_{(x,y)\in D}\{g(x,y)-E[g(x,y)]\}^2\mathrm{d}x\mathrm{d}y$$

$$C_{g'g'}=\iint_{(x,y)\in D}\{g'(x,y)-E[g'(x,y)]\}^2\mathrm{d}x\mathrm{d}y$$

$$E[g(x,y)]=\frac{1}{|D|}\iint_{(x,y)\in D}g(x,y)\mathrm{d}x\mathrm{d}y$$

$$E[g'(x,y)]=\frac{1}{|D|}\iint_{(x,y)\in D}g'(x,y)\mathrm{d}x\mathrm{d}y$$

$g'(x,y)$为参考图像强度值，$|D|$为D的面积。

4.如权利要求1所述计算机网络身份验证方法，其特征在于，指纹录入中，对于指纹采集的图像识别进行优化，具体方法如下：

(1)提取脊线

将指纹图像分割成足够小的子块，满足块中纹理近似平行的条件；

对每个子块的每一个点$p(s,t)$利用Sobel算子分别计算x方向梯度g_x和y方向梯度g_y，s，t＝0,1,……w-1；

每个子块方向$\theta(m,n)$的计算公式如下：

$$\theta(m,n)=\frac{1}{2}\tan^{-1}\left\{\frac{\sum_{s=1}^{w}\sum_{t=1}^{w}2g_x(s',t')g_y(s',t')}{\sum_{s=1}^{w}\sum_{t=1}^{w}\left[g_x^2(s',t')-g_y^2(s',t')\right]}\right\}$$

s′＝s+m Wt′＝t+n W

(2)脊线频率

脊线频率为两条脊线之间间距的倒数，采用GABOR滤波器函数的实部作为模板，以与子块纹线方向垂直的方向作为滤波器方向，以脊线频率作为滤波器频率构建滤波器，滤波过程如下式所示：

$$G_E(s,t)=\left|\frac{1}{S}\sum_{y=\frac{W}{2}}^{\frac{W}{2}}\sum_{y=\frac{W}{2}}^{\frac{W}{2}}h_g(x,y,\theta(m,n),f(m,n),\sigma_x,\sigma_y)G(s+x,t+y)\right|$$

其中，G(s,t)为原始灰度图像，$G_E(s,t)$是GARBOR滤波后的图像灰度，W为滤波器模板的大小，S为模板系数和，θ为子块的域方向值，GARBOR滤波器的θ与指纹纹理方向垂直，对σ_x和σ_y的取值进行折中，取值σ_x＝4和σ_y＝4。

5.如权利要求1所述计算机网络身份验证方法，其特征在于，人脸面部识别算法为：

(1)对原始数据进行标准化采集，集合x的维度为P，

$x=(X_1,X_2,X_3,\cdots,X_p)^T$，

其中，n个样品的集合X_i为$X_i=(X_{1i},X_{2i},X_{3i},\cdots,X_{pi})^T$，i＝1,2,3,…,n,n＞P，

针对样本阵元进行标准化变换：

$$Z_{ij}=\frac{x_{ij}-\bar{x}_j}{s_j}\quad i=1,2,3,\cdots,n;j=1,2,3,\cdots,P$$

$$\bar{x}_j=\frac{1}{n}\sum_{i=1}^{n}x_{ij},$$

$$s_j^2=\frac{1}{n}\sum_{i=1}^{n}(x_{ij}-\bar{x}_j)^2,$$

称为Z标准化阵；

(2)标准化阵Z的矩阵系数：

$$R=|r_{ij}|_P xP=\frac{Z^TZ}{n-1},$$

其中，

$$r_{ij}=\frac{1}{n-1}(\sum Z_{kj}\cdot Z_{kj})\quad i,j=1,2,3,\cdots,P,$$

(3)求解R的特征方程

$|R-\lambda I_P|_P=0$，

按照$\frac{\sum_{j=1}^{m}\lambda_j}{\sum_{j=1}^{P}\lambda_j}\geq 0.85$，确定m的值，对其中每一个$\lambda_j$，得到单位特征向量$b_j^0$；

(4)将指标变量转化为主成分：

$$U_{ij}=z_i^{\mathrm{T}}b_j^0 \quad j=1,2,3,\cdots,m,$$

式中：U_1为第一主成分；U_2为第二主成分；U_3为第三主成分；U_P为第P主成分；

(5)对载入的人脸图像进行几何归一化处理，假设载入的人脸图像的像素点为m×n，则将像素储存在列向量$(X_1,X_2,X_3,\cdots)^{\mathrm{T}}$中；

(6)求得平均人脸：

$$\mu_X=\frac{1}{M}\sum_{i=1}^{m}X_i,$$

训练样本的协方差矩阵为：

$$c=\frac{1}{M}\sum_{i=1}^{m}(X_i-\mu_X)(X_i-\mu_X)^{\mathrm{T}},$$

取差值向量：

$w_i=x_i-\mu_x$，

令$w=(w_1,w_2,w_3,\cdots,w_n)$；

(7)投射到待检测空间，则每幅图像在特征空间的坐标函数为：

$y_i=U^{\mathrm{T}}(x_i-\mu_x)=U^{\mathrm{T}}w_i$，

其中，

$$\begin{cases}U\in R^{N(M-1)}\\ x_i,\mu_X,W_i\in R^N\\ y_i\in R^{M-1}\end{cases}$$

同样将待测图像x_{test}投射到特征子空间之中，

$y_{test}=U^{\mathrm{T}}(x_{test}-\mu_x)$

(8)利用距离分离器进行辨识，目标函数为：

$minDist=min||y_i-y_{test}||$。

6.一种实现权利要求1～5任意一项所述计算机网络身份验证方法的计算机程序。

7.一种实现权利要求1～5任意一项所述计算机网络身份验证方法的信息数据处理终端。

8.一种计算机可读存储介质，包括指令，当其在计算机上运行时，使得计算机执行如权利要求1-5任意一项所述的计算机网络身份验证方法。

9.一种实现权利要求1所述计算机网络身份验证方法的计算机网络身份验证系统，其特征在于，该计算机网络身份验证系统，包括：

IP终端；

IP终端包括登录单元与注册单元，注册单元包括基本信息界面和验证模块，基本信息

界面读取信息成功进入验证模块；

所述验证模块包括人脸面部识别界面、虹膜上传界面、指纹录入界面；

所述人脸面部识别界面进入眼睛虹膜上传界面，所述眼睛虹膜上传界面进入指纹录入界面；

所述指纹录入界面进入手机号绑定界面；

登录单元包括认定模块，所述认定模块包括动态二维码界面、验证码验证界面、虹膜验证界面；

所述扫描动态二维码界面信息进入验证码验证界面，验证码验证界面信息进入虹膜验证界面；

基本信息认证通过身份证读卡器进行读取；

验证码是由文字、数字、字母构成。

10.一种计算机网络平台，其特征在于，所述计算机网络平台至少搭载权利要求9所述的计算机网络身份验证系统。

一种计算机网络身份验证系统及方法、计算机程序

技术领域

[0001] 本发明属于信息技术领域，尤其涉及一种计算机网络身份验证系统及方法、计算机程序。

背景技术

[0002] 目前，将帐号(有些情况称为用户名)和密码直接通过用户终端输入并传送到服务器，服务器对比预存的帐号和密码，是否相同，决定用户身份的真伪。这种认证方法在认证过程中会暴露密码，密码容易被偷窥和盗取，并且密码也不容易被记住，会存在混乱而无法登录等现象。有些地方通过刷卡进行认证登录，会存在丢失、遗忘等现象，安全性差。同时，这些技术渐渐的将会被淘汰，不能对用户身份信息妥善保管，就很有可能造成大规模用户隐私泄露甚至被不法分子盗用的危险，由此给用户带来了严重的影响。

[0003] 综上所述，现有技术存在的问题是：

[0004] 认证过程中会暴露密码，密码容易被偷窥和盗取，刷卡进行认证登录，会存在丢失、遗忘等现象，安全性较差。

[0005] 现有技术中，用户注册基本信息中，基本信息的加密，保密性差。没有对用户的虹膜信息进行切实可行加解密，不能有效保护用户的利益。

发明内容

[0006] 针对现有技术存在的问题，本发明提供了一种计算机网络身份验证系统及方法、计算机程序。

[0007] 本发明是这样实现的，一种计算机网络身份验证方法，包括：

[0008] 用户注册，填写基本信息之后进行人脸面部识别、虹膜上传、指纹录入；再进行手机号绑定注册；

[0009] 用户注册基本信息中，需进行基本信息的加密，包括：

[0010] 第一步，初始化建立算法：首先输入包含所有属性的属性集合U，属性在不同的分层中；然后选择一个阶为$N=p_1p_2p_3$双线性复合群G，p_1、p_2、p_3为不相同的素数，令G_{p_i}表示阶为p_i的子群，$i=1,2,3$；然后选择随机指数a和α、随机群元素$g\in G_{p_1}$、$X_3\in G_{p_3}$，其中，$a,\alpha\in Z_N$，Z_N表示1至N-1的整数；对于U中的|U|个属性元素，选择对应的群元素$h_1,...,h_{|U|}\in G_{p_1}$，则公共参数PK和主密钥MSK分别为：

[0011] $PK=\{N,g,g^{\alpha},e(g,g)^{a},h_1,.....,h_{|U|}\}$；

[0012] $MSK=\{\alpha,X_3\}$；

[0013] 其中，$e(g,g)^{a}$表示双线性对；

[0014] 第二步，令属性集合S为属性集合U的分层子集，根据属性集合S、公共参数PK、消息M和一个提前生成的分层门限访问结构(M_V,ρ)将属性集合U所有层次的属性均用一个表达式进行加密得到密文CT，其中，函数ρ表示分层访问结构M_V中的行到属性的映射；令属性集

合S的每一层的属性数量超过该层门限，使S满足分层的访问结构；

[0015] 第三步，通过主密钥MSK和属性集合S，结合步骤S1中的子群G_{p_3}生成密钥SK；

[0016] 第四步，通过访问结构M_V对应的密文CT和属性集合S对应的密钥SK恢复出消息。

[0017] 所述分层门限访问结构(M_V,ρ)的生成方法具体如下：

[0018] 1)系统初始化

[0019] 定义函数f的运算规则如下：每进行一次f运算，就将多项式的常数项变为0，自变量的系数不变，次数减1，设a、b、c、d为确定的常实数，则有：

[0020] $f(a+bx+cx^d)=0+b+cx^{d-1}$；

[0021] $f(1+2x+3x^4)=0+2+3x^3$；

[0022] 设(k,n)是一个分层的秘密共享系统，主要由一个秘密分发者D和n个参与者组成，属性集合U是n个参与者的集合，且包含m个层次，即$U=\bigcup_{i=0}^{m}U_i$，其中对于$i\neq j$，$U_i\cap U_j=\Phi$；令$\mathbf{k}=\{k_i\}_{i=0}^{m}$是一个单调递增的整数序列$0<k_0<k_1<\ldots<k_m$，并且$k_{m-1}<k_m-1$，$k_i$是每一层的门限值，则(k,n)分层的门限访问结构就是要为属性集合U中每个参与者u分配秘密信息s的一个秘密份额$\sigma(u)$，使其满足以下访问结构：

[0023] $$\Gamma=\left\{S\subseteq U:\left|S\cap\left(\bigcup_{j=0}^{i}U_j\right)\right|\right\}\geq k_i,\forall i\in\{0,1,\ldots,m\};$$

[0024] 满足上式所描述的访问结构的分层的参与者子集S称为授权子集，可以恢复主秘密，而不满足上述访问结构的任何用户子集将无法获得关于主秘密的任何信息；

[0025] 2)子秘密分发

[0026] 秘密分发者D任意选取t-1个随机数$a_1,\ldots,a_{t-1}$和一个大素数q，然后构造多项式$P(x)=s+a_1x+\ldots+a_{t-1}x^{t-1}$，其中s是需要被共享的主秘密；系统中的每个参与者u对应域里面的一个元素表示其身份，用u_j表示，D根据参与者所处的层次i计算参与者的秘密份额$\sigma(u_j)=P_{k_{i-1}}(u_j)$，其中：

[0027] $P_0(x)=P(x)$；

[0028] $P_1(x)=f^1(P(x))=f(P(x))$；

[0029] $P_i(u)=f(P_{i-1}(u))$；

[0030] $P_{k_{i-1}}(u_j)$表示多项式P(x)经过k_i-1次f运算后在域元素u_j处的值；k_i-1是第i-1层的门限值且令$k_{-1}=0$，D公开$\{\sigma(u_1),\ldots,\sigma(u_{l_m})\}$；$l_m$表示第m层中拥有属性集合S的元素数量；

[0031] 3)秘密恢复

[0032] 令$S=\{v_1,\ldots,v_{|S|}\}\subset U$，|S|表示S所具有的元素数量，设定满足：

[0033] $v_1,\ldots,v_{l_0}\in U_0$；

[0034] $v_{l_0+1},\ldots,v_{l_1}\in U_1$；

[0035] …

[0036] $v_{l_{m-1}+1},\ldots,v_{l_m}\in U_m$；

[0037] 其中，$U_0,\cdots,U_m$表示集合U的第0至m层，$0\leq l_0\leq l_1\leq\ldots\leq l_m=|S|$，当且仅当对于所

有的0≤i≤m,$l_i \geq k_i$,S为一个授权子集,即符合访问结构,则S中所有的参与者合作时,可以组成系数矩阵M_V,其中系数矩阵按行编写为:

[0038] $$M_V=\begin{pmatrix} 1 & v_1 & v_1^2 & \cdots & v_1^{t-1} \\ & & \cdots & & \\ 1 & v_{l_0} & v_{l_0}^2 & \cdots & v_{l_0}^{t-1} \\ 0 & \cdots\ 1 & \cdots & v_{l_0+1} & \cdots\ v_{l_0+1}^{t-1-k_0} \\ & & \cdots & & \\ 0 & \cdots\ 1 & \cdots & v_{l_1} & \cdots\ v_{l_1}^{t-1-k_0} \\ & & \cdots & & \\ 0 & \cdots\ 1 & \cdots & v_{l_{m-1}+1} & \cdots\ v_{l_{m-1}+1}^{t-1-k_{m-1}} \\ & & \cdots & & \\ 0 & \cdots\ 1 & \cdots & v_{l_m} & \cdots\ v_{l_m}^{t-1-k_{m-1}} \end{pmatrix};$$

[0039] S中的所有参与者可以合作解出如下的方程组:

[0040] $$\begin{cases} s+a_1v_1+a_2v_1^2+\cdots+a_{t-1}v_1^{t-1}=\sigma(u_1) \\ \cdots \\ s+a_1v_{l_0}+a_2v_{l_0}^2+\cdots+a_{t-1}v_{l_0}^{t-1}=\sigma(u_{l_0}) \\ a_{k_0}+a_{k_0+1}v_{l_0+1}+\cdots+a_{t-1}v_{l_0+1}^{t-1-k_0}=\sigma(u_{l_0+1}) \\ \cdots \\ a_{k_0}+a_{k_0+1}v_{l_1}+\cdots+a_{t-1}v_{l_1}^{t-1-k_0}=\sigma(u_{l_1}) \\ \cdots \\ a_{k_{m-1}}+a_{k_{m-1}+1}v_{l_{m-1}+1}+\cdots+a_{t-1}v_{l_{m-1}+1}^{t-1-k_{m-1}}=\sigma(u_{l_{m-1}+1}) \\ \cdots \\ a_{k_{m-1}}+a_{k_{m-1}+1}v_{l_m}+\cdots+a_{t-1}v_{l_m}^{t-1-k_{m-1}}=\sigma(u_{l_m}) \end{cases};$$

[0041] 即:

[0042] $$\begin{pmatrix} 1 & v_1 & v_1^2 & \cdots & v_1^{t-1} \\ & & \cdots & & \\ 1 & v_{l_0} & v_{l_0}^2 & \cdots & v_{l_0}^{t-1} \\ 0 & \cdots\ 1 & \cdots & v_{l_0+1} & \cdots\ v_{l_0+1}^{t-1-k_0} \\ & & \cdots & & \\ 0 & \cdots\ 1 & \cdots & v_{l_1} & \cdots\ v_{l_1}^{t-1-k_0} \\ & & \cdots & & \\ 0 & \cdots\ 1 & \cdots & v_{l_{m-1}+1} & \cdots\ v_{l_{m-1}+1}^{t-1-k_{m-1}} \\ & & \cdots & & \\ 0 & \cdots\ 1 & \cdots & v_{l_m} & \cdots\ v_{l_m}^{t-1-k_{m-1}} \end{pmatrix}\begin{pmatrix} s \\ a_1 \\ a_2 \\ \cdot \\ \cdot \\ \cdot \\ a_{t-1} \end{pmatrix}=\begin{pmatrix} \sigma(u_1) \\ \cdots \\ \sigma(u_{l_0}) \\ \sigma(u_{l_0+1}) \\ \cdots \\ \sigma(u_{l_1}) \\ \cdots \\ \sigma(u_{l_{m-1}+1}) \\ \cdots \\ \sigma(u_{l_m}) \end{pmatrix};$$

[0043] 可以看出,若S满足访问结构,就可以重构出多项式P(x),从而恢复出秘密s;这个访问结构可以等价于分层矩阵的LSSS的访问结构,即令$I \subseteq \{1,\ldots,l_0,\ldots,l_m\}$被定义为I={j:(j)∈S},如果令$\{\lambda_j = M_V\vec{a}\}_{j\in I}$是秘密s的一个子秘密,则存在常数{$\omega_j \in Z_N$}使得$\sum_{j\in I}\omega_j\lambda_j$=s,其中,$\vec{a}=(a_1,\ldots,a_{t-1})^T$,$Z_N$表示1到N的整数集合;$\omega_j$在秘密共享生成矩阵$M_v$大小的多项式时间内总可以被找到,就可以恢复出来主秘密;

[0044] 登录时通过扫描动态二维码,产生验证码进行输入进入虹膜验证,根据虹膜验证判断登录是否成功;

[0045] 验证码进行虹膜验证中,需进行虹膜信息的解密,包括:

[0046] 在得到密文Z′=(z_1′,…,z_{21}′)后,首先计算:

[0047] Y′=L_2^{-1}(Z′)=(y_1′,…,y_{21}′);

[0048] 对于点集P中的每一点(μ,λ),计算:

[0049] $(y_1'',\cdots,y_{2l}'')=\tilde{F}^{-1}((y_1',\cdots,y_{2l}')+\lambda)$,

[0050] 然后验证Z(y1″,…,y21″)=μ,如果不成立,则丢弃这组值;否则进行下一步;

[0051] 最后计算:

[0052] M′=L1-1(y1″,…,y21″)=(m1′,…,m21′),

[0053] 如果只有唯一的一组(m1′,…,m21′),那么M′就一定是对应的明文,如果得到超过一组的(m1′,…,m21′),则用Hash函数或者增加验证方程的方式来确定唯一明文;

[0054] 进一步,解密前,需先进行虹膜的加密,包括:

[0055] 公钥生成:公钥由有限域k,以及它的加法和乘法结构和n个二次多元多项式组成;

[0056] 私钥生成:私钥由映射$\tilde{F}$随机选取的r个线性独立的z1,…,zr∈k[x1,…,x21]、一个点集P、两个可逆仿射变换L1和L2以及它们的逆组成;

[0057] 加密过程即给定明文M′=(x1′,…,xn′),用选取的公钥进行加密,形成密文Z′=(z1′,…,zn′);

[0058] 中心映射重新构造的过程包括以下步骤:

[0059] 首先,选择r是一个比较小的整数,随机选择r个线性独立方程

[0060] $z_1(x_1,\cdots,x_{2l})=\sum_{j=1}^{2l}\alpha_{j1}x_j+\beta_1$

[0061] ⋮

[0062] $z_r(x_1,\cdots,x_{2l})=\sum_{j=1}^{2l}\alpha_{jr}x_j+\beta_r$

[0063] 映射Z:k21→kr如下确定:

[0064] Z(x1,…,x21)=(z1(x1,…,x21),…,zr(x1,…,x21)),

[0065] 其次,随机选取2l个总次数为2的多项式$\hat{f}_1,\cdots,\hat{f}_{2l}\in k[z_1,\cdots,z_r]$,

[0066] 映射$\hat{F}$:kr→k21如下确定:

[0067] 然后,定义扰动映射F*:k21→k21为$\hat{F}$和Z的复合:

[0068] 其中f1*,…,f21*∈k[x1,…,x21],

[0069] 最后,用内部扰动映射F*扰动原来的中心映射$\tilde{F}$,新的公钥映射为:

[0070] $\overline{F}=L_2\circ(\tilde{F}+F^*)\circ L_1=(\overline{f}_1,\cdots,\overline{f}_{2l})$;

[0071] 公钥生成包括以下步骤:

[0072] 选取有限域k,以及它的加法和乘法结构;

[0073] 选取2l个二次多元多项式组:

[0074] f1(x1,…,x21),…,f21(x1,…,x21)∈k[x1,…,x21];

[0075] 私钥生成包括以下步骤:

[0076] 选取映射$\tilde{F}$,即两个随机数α1,α2;

[0077] 随机选取r个线性独立的z1,…,zr∈k[x1,…,xn];

[0078] 选取一个点集P,P是所有映射$\hat{F}:k^r\rightarrow k^{21}$的像和原像的集合,即:

[0079] $$P=\left\{(\mu,\lambda)\,|\,\hat{F}(\mu)=\lambda\right\},$$

[0080] 点集P由随机选取的21个二次多项式$\hat{f}_1,\cdots,\hat{f}_{2l}\in k[z_1,\cdots,z_r]$确定;

[0081] 选取两个可逆仿射变换L_1和L_2以及它们的逆;

[0082] 第二步中具体包括如下步骤:

[0083] 2.1)令访问结构M_V是一个j×t矩阵;

[0084] 2.2)选择一个随机向量$\vec{y}=(y_0=s,y_1,.....,y_{t-1})\in Z_N^t$,$Z_N^t$表示1到N的整数集合中的任意t个,其中,s表示秘密值,y_1,.....,y_{t-1}为秘密值s的分享;

[0085] 2.3)令$S=\left\{v_1,...,v_{|S|}\right\}\subset U$,|S|表示S所具有的元素数量,设定满足:

[0086] $v_1,...,v_{l_0}\in U_0$;

[0087] $v_{l_0+1},...,v_{l_1}\in U_1$;

[0088] …

[0089] $v_{l_{m-1}+1},...,v_{l_m}\in U_m$;

[0090] 其中,$U_0,\cdots,U_m$表示集合U的第0至m层,$0\leqslant l_0\leqslant l_1\leqslant...\leqslant l_m=|S|$,当且仅当对于所有的$0\leqslant i\leqslant m$,有$l_i\geqslant k_i$,$l_i$表示第i层中拥有集合S的元素数量,$k_i$表示第i层中集合S的元素数量门限;

[0091] 然后对于所有的$j=1,...,l_0,...,l_m$,计算$\lambda_j=M_j\cdot\vec{y}$,$M_j$表示$M_V$中的第j行;

[0092] 2.4)对于属性集合U的层次数$i\in\{0,...,m\}$,设定$j=l_{i-1}+c$,$l_{-1}=0$,c为常数,表示第i层的第c个属性,即属性集合U中的第j个属性对应于第i层的第c个属性;

[0093] 2.5)选择随机数$r_{l_0,.....,}r_{l_m}\in Z_N$;

[0094] 2.6)将所有层次的属性通过以下表达式进行加密得出密文CT:

[0095] $$CT=\left\{\begin{array}{c}C=Me(g,g)^{\alpha s},(M_V,\rho)\\ C'=g^s\\ C_j=g^{a\lambda_j}h_{\rho(j)}^{-\sum_{x=l_0,.....l_i}r_x}\\ D_{l_0}=g^{r_{l_0}},.....,D_{l_m}=g^{r_{l_m}}\end{array}\right\}k_{i-1}\leq j\leq k_i;$$

[0096] 其中,$h_{\rho(j)}$表示与属性集合U中的第ρ(j)个属性元素对应的群元素,ρ(j)表示属性集合U中第j层的属性到访问结构M_v的第j行的映射。

[0097] 进一步,验证模块对于虹膜识别的算法为:

[0098] (1)提取边缘

[0099] 用CCD获取的眼睛图像,包括巩膜、虹膜、瞳孔和上眼皮部分,将虹膜从整幅图像中分割出来,首先找出虹膜的内外边缘;

[0100] 选用高斯—拉普拉斯二阶微分滤波器∇^2G,∇^2G为二维高斯平滑滤波器G(x,y)与

拉普拉斯算子$\nabla^2 f(x,y)$的组合：

[0101] $$G(x,y)=\frac{1}{2\pi\sigma^2}e^{-\frac{x^2+y^2}{2\sigma^2}}$$

[0102] $$\nabla^2 f(x,y)=\frac{\partial^2 f}{\partial x^2}+\frac{\partial^2 f}{\partial y^2}$$

[0103] 二阶微分滤波器为：

[0104] $$\nabla^2 G=\frac{\partial^2 G}{\partial x^2}+\frac{\partial^2 G}{\partial y^2}=\frac{1}{2\pi\sigma^4}\left(\frac{x^2+y^2}{\sigma^2}-2\right)e^{-\frac{x^2+y^2}{2\sigma^2}}$$

[0105] 该滤波器虽不是可分离的,但可写成：

[0106] $$\nabla^2 G=\frac{1}{2\pi\sigma^4}\left(\frac{x^2}{\sigma^2}-1\right)e^{-\frac{x^2}{2\sigma^2}}e^{-\frac{y^2}{2\sigma^2}}+\frac{1}{2\pi\sigma^4}\left(\frac{y^2}{\sigma^2}-1\right)e^{-\frac{y^2}{2\sigma^2}}e^{-\frac{x^2}{2\sigma^2}}=G_1+G_2$$

[0107] G1、G2均为可分离滤波器,采用分离算法,可以大大减少计算的复杂性；

[0108] 2G与图像进行卷积:$\nabla^2 G*g(x,y)$,g(x,y)表示图像上对应点的强度,“*”表示卷积,卷积后获得边缘；

[0109] (2)定位虹膜

[0110] 设虹膜的外圆、内圆方程为：

[0111] $(x-x_1)^2+(y-y_1)^2=r_1^2$

[0112] $(x-x_2)^2+(y-y_2)^2=r_2^2$

[0113] 用Houg h变换可获得(x_1,y_1,r_1)、(x_2,y_2,r_2)两组参数值,一般情况下$(x_1,y_1)\neq(x_2,y_2)$,即不是同心圆,因为瞳孔并不位于虹膜的中心,总是有所偏离,两个圆之间的部分,定义为虹膜部分；定义外边界圆的圆心(x_1,y_1)为虹膜的中心；定义外边界圆的半径r_1为虹膜的半径,获得了中心坐标(x_1,y_1),即获得了实时图像相对参考图像的平移量,中心为(p,q)；获得了虹膜半径r_1,即获得了比例变化因子r_1/r,r为参考虹膜的标准半径；根据平移量和比例变化因子对实时图像进行平移和比例校正,用双线性插值法插补,就消除了平移和比例变化；

[0114] (3)图像匹配

[0115] 上一步两个边界圆之间区域还包括眼皮部分,需去除该部分,以虹膜的中心为两坐标系的共同原点,将原直角坐标系转化为极坐标系,在极坐标系中,$\{(\rho,\theta)\ 70^\circ<\theta<110^\circ\}$为含眼皮部分,去除；其余为只含有虹膜的部分,保留；保留下来可用于匹配、识别的虹膜部分约占全部虹膜面积的85%；

[0116] 一般情形下,虹膜的旋转变化较小,约在±5°左右,而虹膜图像相关性较强,有较长的相关长度,因此,将旋转变化等效为噪声即可,这样也可以简化计算；图像的匹配采用相关系数测度：

[0117] $$\rho=\frac{C}{\sqrt{C_{gg}C_{g'g'}}}$$

[0118] 其中,

[0119] $$C=\iint_{(x,y)\in D}\{g(x,y)-E[g(x,y)]\}\{g'(x,y)-E[g'(x,y)]\}\mathrm{d}x\mathrm{d}y$$

[0120] $$C_{gg}=\iint_{(x,y)\in D}\{g(x,y)-E[g(x,y)]\}^2\mathrm{d}x\mathrm{d}y$$

[0121] $$C_{gg}''=\iint_{(x,y)\in D}\{g'(x,y)-E[g'(x,y)]\}^2\mathrm{d}x\mathrm{d}y$$

[0122] $$E[g(x,y)]=\frac{1}{|D|}\iint_{(x,y)\in D}g(x,y)\mathrm{d}x\mathrm{d}y$$

[0123] $$E[g'(x,y)]=\frac{1}{|D|}\iint_{(x,y)\in D}g'(x,y)\mathrm{d}x\mathrm{d}y$$

[0124] g′(x,y)为参考图像强度值,|D|为D的面积。

[0125] 进一步,指纹录入中,对于指纹采集的图像识别进行优化,具体方法如下:

[0126] (1)提取脊线

[0127] 将指纹图像分割成足够小的子块,以满足块中纹理近似平行的条件;

[0128] 对每个子块的每一个点p(s,t)利用Sobel算子分别计算x方向梯度g_x和y方向梯度g_y,s,t=0,1,……w-1;

[0129] 每个子块方向θ(m,n)的计算公式如下:

[0130] $$\theta(m,n)=\frac{1}{2}\tan^{-1}\left\{\frac{\sum_{s=1}^{w}\sum_{t=1}^{w}2g_x(s',t')g_y(s',t')}{\sum_{s=1}^{w}\sum_{t=1}^{w}\left[g_x^2(s',t')-g_y^2(s',t')\right]}\right\}$$

[0131] s′=s+m W t′=t+n W

[0132] (2)脊线频率

[0133] 脊线频率被定义为两条脊线之间间距的倒数,采用GABOR滤波器函数的实部作为模板,以与子块纹线方向垂直的方向作为滤波器方向,以脊线频率作为滤波器频率来构建滤波器,滤波过程如下式所示:

[0134] $$G_E(s,t)=\left|\frac{1}{S}\sum_{y=\frac{W}{2}}^{\frac{W}{2}}\sum_{y=\frac{W}{2}}^{\frac{W}{2}}h_g(x,y,\theta(m,n),f(m,n),\sigma_x,\sigma_y)G(s+x,t+y)\right|$$

[0135] 其中,G(s,t)为原始灰度图像,G_E(s,t)是GARBOR滤波后的图像灰度,W为滤波器模板的大小,S为模板系数和,θ为子块的域方向值,GARBOR滤波器的θ与指纹纹理方向垂直,对σ_x和σ_y的取值进行折中,取值σ_x=4和σ_y=4。

[0136] 进一步,人脸面部识别算法为:

[0137] (1)对原始数据进行标准化采集,该集合x的维度为P,

[0138] $x=(X_1,X_2,X_3,\cdots,X_p)^T$,

[0139] 其中,n个样品的集合X_i为$X_i=(X_{1i},X_{2i},X_{3i},\cdots,X_{pi})^T$,i=1,2,3,…,n,n>P,

[0140] 针对样本阵元进行标准化变换:

[0141] $$Z_{ij}=\frac{x_{ij}-\bar{x}_j}{s_j}\quad i=1,2,3,\cdots,n;j=1,2,3,\ \cdots,P$$

[0142] $$\bar{x}_j=\frac{1}{n}\sum_{i=1}^{n}x_{ij},$$

[0143] $$s_j^2=\frac{1}{n}\sum_{i=1}^{n}(x_{ij}-\bar{x}_j)^2,$$

[0144] 称为Z标准化阵;

[0145] (2)标准化阵Z的矩阵系数:

[0146] $$R=|\ r_{ij}\ |_P xP=\frac{Z^TZ}{n-1},$$

[0147] 其中,

[0148] $$r_{ij}=\frac{1}{n-1}(\sum Z_{kj}\cdot Z_{kj})\quad i,j=1,2,3,\cdots,P,$$

[0149] (3)求解R的特征方程

[0150] $|R-\lambda I_P|_P=0$,

[0151] 按照$\frac{\sum_{j=1}^{m}\lambda_j}{\sum_{j=1}^{P}\lambda_j}\geq 0.85$,确定m的值,对其中每一个$\lambda_j$,得到单位特征向量$b_j^0$;

[0152] (4)将指标变量转化为主成分:

[0153] $$U_{ij}=z_i^Tb_j^0\quad j=1,2,3,\cdots,m,$$

[0154] 式中:U_1为第一主成分;U_2为第二主成分;U_3为第三主成分;U_P为第P主成分;

[0155] (5)对载入的人脸图像进行几何归一化处理,假设载入的人脸图像的像素点为m×n,则将像素储存在列向量$(X_1,X_2,X_3,\cdots)^T$中;

[0156] (6)求的平均人脸:

[0157] $$\mu_X=\frac{1}{M}\sum_{i=1}^{m}X_i,$$

[0158] 训练样本的协方差矩阵为:

[0159] $$c=\frac{1}{M}\sum_{i=1}^{m}(X_i-\mu_X)(X_i-\mu_X)^T,$$

[0160] 取差值向量:

[0161] $w_i=x_i-\mu_x$,

[0162] 令$w=(w_1,w_2,w_3,\cdots,w_n)$;

[0163] (7)投射到待检测空间，则每幅图像在特征空间的坐标函数为：

[0164] $y_i=U^T(x_i-\mu_x)=U^Tw_i$，

[0165] 其中，

[0166] $$\begin{cases} U \in R^{N(M-1)} \\ x_i,\mu_X,W_i \in R^N \\ y_i \in R^{M-1} \end{cases}$$

[0167] 同样可以将待测图像x_{test}投射到特征子空间之中，

[0168] $y_{test}=U^T(x_{test}-\mu_x)$

[0169] (8)利用距离分离器进行辨识，目标函数为：

[0170] $\min Dist=\min||y_i-y_{test}||$。

[0171] 本发明的另一目的在于提供一种实现所述计算机网络身份验证方法的计算机程序。

[0172] 本发明的另一目的在于提供一种实现所述计算机网络身份验证方法的信息数据处理终端。

[0173] 本发明的另一目的在于提供一种计算机可读存储介质，包括指令，当其在计算机上运行时，使得计算机执行所述的计算机网络身份验证方法。

[0174] 本发明的另一目的在于提供一种实现所述计算机网络身份验证方法的计算机网络身份验证系统，包括：

[0175] IP终端；

[0176] IP终端包括登录单元与注册单元，注册单元包括基本信息界面和验证模块，基本信息界面读取信息成功进入验证模块；

[0177] 所述验证模块包括人脸面部识别界面、虹膜上传界面、指纹录入界面；

[0178] 所述人脸面部识别界面进入眼睛虹膜上传界面，所述眼睛虹膜上传界面进入指纹录入界面；

[0179] 所述指纹录入界面进入手机号绑定界面；

[0180] 登录单元包括认定模块，所述认定模块包括动态二维码界面、验证码验证界面、虹膜验证界面；

[0181] 所述扫描动态二维码界面信息进入验证码验证界面，验证码验证界面信息进入虹膜验证界面；

[0182] 基本信息认证通过身份证读卡器进行读取；

[0183] 验证码是由文字、数字、字母构成。

[0184] 本发明的另一目的在于提供一种计算机网络平台，所述计算机网络平台至少搭载所述的计算机网络身份验证系统。

[0185] 本发明的优点及积极效果为：

[0186] 该计算机网络身份验证系统用户需要先进行注册，填写基本信息，成功之后进行人脸面部识别、虹膜上传、指纹录入，最后进行手机号绑定注册成功，登录时通过扫描动态二维码，产生验证码进行输入进入虹膜验证(用户也可以同时选择人脸面部验证、指纹验证)，根据虹膜验证判断登录是否成功。实名认证、人脸面部识别认证、眼睛虹膜认证和指纹

认证结合为一体,避免保护个人身份和隐私信息遭到泄露。通过采用优化算法进行虹膜识别,大大提高了虹膜识别的准确性,提高匹配速率;通过对指纹采集图像识别的优化,改善了图像的质量,提高了指纹采集的精准度;优化人脸面部识别算法,降低计算维度,简化计算过程,加快了对人脸识别的速度;扫描二维码的方式,提高系统登录的便捷性。

[0187] 登录时通过扫描动态二维码,产生验证码进行输入进入虹膜验证,根据虹膜验证判断登录是否成功;

[0188] 本发明验证码进行虹膜验证中,需进行虹膜信息的解密,包括:

[0189] 在得到密文$Z'=(z_1',\cdots,z_{21}')$后,首先计算:

[0190] $Y'=L_2^{-1}(Z')=(y_1',\cdots,y_{21}')$;

[0191] 对于点集P中的每一点(μ,λ),计算:

[0192] $$(y_1'',\cdots,y_{2l}'')=\tilde{F}^{-1}((y_1',\cdots,y_{2l}')+\lambda),$$

[0193] 然后验证$Z(y_1'',\cdots,y_{21}'')=\mu$,如果不成立,则丢弃这组值;否则进行下一步;

[0194] 最后计算:

[0195] $M'=L_1^{-1}(y_1'',\cdots,y_{21}'')=(m_1',\cdots,m_{21}')$,

[0196] 如果只有唯一的一组$(m_1',\cdots,m_{21}')$,那么M'就一定是对应的明文,如果得到超过一组的$(m_1',\cdots,m_{21}')$,则用Hash函数或者增加验证方程的方式来确定唯一明文;

[0197] 解密前,需先进行虹膜的加密,包括:

[0198] 公钥生成:公钥由有限域k,以及它的加法和乘法结构和n个二次多元多项式组成;

[0199] 私钥生成:私钥由映射$\tilde{F}$随机选取的r个线性独立的$z_1,\cdots,z_r\in k[x_1,\cdots,x_{21}]$、一个点集P、两个可逆仿射变换$L_1$和$L_2$以及它们的逆组成;

[0200] 加密过程即给定明文$M'=(x_1',\cdots,x_n')$,用选取的公钥进行加密,形成密文$Z'=(z_1',\cdots,z_n')$;切实保证了个人身份和隐私信息不遭到泄露。

[0201] 用户注册,填写基本信息之后进行人脸面部识别、虹膜上传、指纹录入;再进行手机号绑定注册;

[0202] 本发明用户注册基本信息中,需进行基本信息的加密,包括:初始化建立算法:首先输入包含所有属性的属性集合U,属性在不同的分层中;然后选择一个阶为$N=p_1p_2p_3$双线性复合群G,p_1、p_2、p_3为不相同的素数,令G_{pi}表示阶为p_i的子群,i=1,2,3;然后选择随机指数a和α、随机群元素$g\in G_{p_1}$、$X_3\in G_{p_3}$,其中,$a,\alpha\in Z_N$,Z_N表示1至N-1的整数;对于U中的|U|个属性元素,选择对应的群元素$h_1,...,h_{|U|}\in G_{p_1}$,则公共参数PK和主密钥MSK分别为:

[0203] $PK=\{N,g,g^{\alpha},e(g,g)^{a},h_1,.....,h_{|U|}\}$;

[0204] $MSK=\{\alpha,X_3\}$;

[0205] 其中,$e(g,g)^{a}$表示双线性对;

[0206] 令属性集合S为属性集合U的分层子集,根据属性集合S、公共参数PK、消息M和一个提前生成的分层门限访问结构(M_V,ρ)将属性集合U所有层次的属性均用一个表达式进行加密得到密文CT,其中,函数ρ表示分层访问结构M_V中的行到属性的映射;令属性集合S的每一层的属性数量超过该层门限,使S满足分层的访问结构;

[0207] 通过主密钥MSK和属性集合S,结合步骤S1中的子群G_{p_3}生成密钥SK;

[0208] 通过访问结构Mv对应的密文CT和属性集合S对应的密钥SK恢复出消息。切实保证了用户的信息,具有很强的保密性和安全性。

附图说明

[0209] 图1是本发明实施例提供的计算机网络身份验证系统的结构示意图;

[0210] 图2是本发明实施例提供的基本信息界面的结构示意图;

具体实施方式

[0211] 为能进一步了解本发明的发明内容、特点及功效,兹例举以下实施例,并配合附图详细说明如下。

[0212] 下面结合附图对本发明的结构作详细的描述。

[0213] 图1,本发明实施例提供的计算机网络身份验证系统,包括:

[0214] IP终端;

[0215] IP终端包括登录单元与注册单元,注册单元包括基本信息界面和验证模块,基本信息界面读取信息成功进入验证模块;

[0216] 所述验证模块包括人脸面部识别界面、虹膜上传界面、指纹录入界面;

[0217] 所述人脸面部识别界面进入眼睛虹膜上传界面,所述眼睛虹膜上传界面进入指纹录入界面;

[0218] 所述指纹录入界面进入手机号绑定界面;

[0219] 登录单元包括认定模块,所述认定模块包括动态二维码界面、验证码验证界面、虹膜验证界面;

[0220] 所述扫描动态二维码界面信息进入验证码验证界面,验证码验证界面信息进入虹膜验证界面;

[0221] 基本信息认证通过身份证读卡器进行读取;

[0222] 验证码是由文字、数字、字母构成。

[0223] 本发明的工作原理是:

[0224] 用户需要先进行注册,填写基本信息,成功之后进行人脸面部识别、虹膜上传、指纹录入,最后进行手机号绑定注册成功,登录时通过扫描动态二维码,产生验证码进行输入进入虹膜验证(用户也可以同时选择人脸面部验证、指纹验证),根据虹膜验证判断登录是否成功。

[0225] 该计算机网络身份验证系统实名认证、人脸面部识别认证、眼睛虹膜认证和指纹认证结合为一体,避免保护个人身份和隐私信息遭到泄露。扫描二维码的方式,提高系统登录的便捷性。

[0226] 下面结合具体分析对本发明作进一步描述。

[0227] 本发明实施例提供的计算机网络身份验证方法,包括:

[0228] 用户注册,填写基本信息之后进行人脸面部识别、虹膜上传、指纹录入;再进行手机号绑定注册;

[0229] 用户注册基本信息中,需进行基本信息的加密,包括:

[0230] 第一步,初始化建立算法:首先输入包含所有属性的属性集合U,属性在不同的分

层中;然后选择一个阶为N＝$p_1p_2p_3$双线性复合群G,p_1、p_2、p_3为不相同的素数,令G_{p_i}表示阶为pi的子群,i＝1,2,3;然后选择随机指数a和α、随机群元素$g \in G_{p_1}$、$X_3 \in G_{p_3}$,其中,a,α∈Z_N,Z_N表示1至N-1的整数;对于U中的|U|个属性元素,选择对应的群元素$h_1,...,h_{|U|} \in G_{p_1}$,则公共参数PK和主密钥MSK分别为:

[0231] PK＝{N,g,g^{α},e(g,g)^a,h_1,.....,$h_{|U|}$};

[0232] MSK＝{α,X_3};

[0233] 其中,e(g,g)^{a}表示双线性对;

[0234] 第二步,令属性集合S为属性集合U的分层子集,根据属性集合S、公共参数PK、消息M和一个提前生成的分层门限访问结构(M_V,ρ)将属性集合U所有层次的属性均用一个表达式进行加密得到密文CT,其中,函数ρ表示分层访问结构M_V中的行到属性的映射;令属性集合S的每一层的属性数量超过该层门限,使S满足分层的访问结构;

[0235] 第三步,通过主密钥MSK和属性集合S,结合步骤S1中的子群G_{p_3}生成密钥SK;

[0236] 第四步,通过访问结构M_V对应的密文CT和属性集合S对应的密钥SK恢复出消息。

[0237] 所述分层门限访问结构(M_V,ρ)的生成方法具体如下:

[0238] 1)系统初始化

[0239] 定义函数f的运算规则如下:每进行一次f运算,就将多项式的常数项变为0,自变量的系数不变,次数减1,设a、b、c、d为确定的常实数,则有:

[0240] f(a+bx+cx^d)＝0+b+cx^{d-1};

[0241] f(1+2x+3x^4)＝0+2+3x^3;

[0242] 设(k,n)是一个分层的秘密共享系统,主要由一个秘密分发者D和n个参与者组成,属性集合U是n个参与者的集合,且包含m个层次,即$U=\bigcup_{i=0}^{m}U_i$,其中对于i≠j,$U_i \cap U_j=\Phi$;令$\mathbf{k}=\{k_i\}_{i=0}^{m}$是一个单调递增的整数序列0＜$k_0$＜$k_1$＜...＜$k_m$,并且$k_{m-1}$＜$k_m$-1,$k_i$是每一层的门限值,则(k,n)分层的门限访问结构就是要为属性集合U中每个参与者u分配秘密信息s的一个秘密份额σ(u),使其满足以下访问结构:

[0243] $$\Gamma=\left\{S\subseteq U:\left|S\cap\left(\bigcup_{j=0}^{i}U_j\right)\right|\right\}\geq k_i,\forall i\in\{0,1,...,m\};$$

[0244] 满足上式所描述的访问结构的分层的参与者子集S称为授权子集,可以恢复主秘密,而不满足上述访问结构的任何用户子集将无法获得关于主秘密的任何信息;

[0245] 2)子秘密分发

[0246] 秘密分发者D任意选取t-1个随机数a_1,...,a_{t-1}和一个大素数q,然后构造多项式P(x)＝s+a_1x+...+$a_{t-1}x^{t-1}$,其中s是需要被共享的主秘密;系统中的每个参与者u对应域里面的一个元素表示其身份,用u_j表示,D根据参与者所处的层次i计算参与者的秘密份额$\sigma(u_j)=P_{k_{i-1}}(u_j)$,其中:

[0247] P_0(x)＝P(x);

[0248] P_1(x)＝f^1(P(x))＝f(P(x));

[0249] P_i(u)＝f(P_{i-1}(u));

[0250] $P_{k_{i-1}}(u_j)$表示多项式P(x)经过k_i-1次f运算后在域元素u_j处的值;k_i-1是第i-1层的门限值且令$k_{-1}=0$,D公开$\{\sigma(u_1),...,\sigma(u_{l_m})\}$;$l_m$表示第m层中拥有属性集合S的元素数量;

[0251] 3)秘密恢复

[0252] 令$S=\{v_1,...,v_{|S|}\}\subset U$,|S|表示S所具有的元素数量,设定满足:

[0253] $v_1,...,v_{l_0}\in U_0$;

[0254] $v_{l_0+1},...,v_{l_1}\in U_1$;

[0255] …

[0256] $v_{l_{m-1}+1},...,v_{l_m}\in U_m$;

[0257] 其中,$U_0,\cdots,U_m$表示集合U的第0至m层,$0\leqslant l_0\leqslant l_1\leqslant...\leqslant l_m=|S|$,当且仅当对于所有的$0\leqslant i\leqslant m$,$l_i\geqslant k_i$,S为一个授权子集,即符合访问结构,则S中所有的参与者合作时,可以组成系数矩阵M_V,其中系数矩阵按行编写为:

[0258] $$M_V=\begin{pmatrix}1 & v_1 & v_1^2 & \cdots & v_1^{t-1}\\ & & \cdots & & \\ 1 & v_{l_0} & v_{l_0}^2 & \cdots & v_{l_0}^{t-1}\\ 0 & \cdots\ 1 & \cdots & v_{l_0+1} & \cdots\ v_{l_0+1}^{t-1-k_0}\\ & & \cdots & & \\ 0 & \cdots\ 1 & \cdots & v_{l_1} & \cdots\ v_{l_1}^{t-1-k_0}\\ & & \cdots & & \\ 0 & \cdots\ 1 & \cdots & v_{l_{m-1}+1} & \cdots\ v_{l_{m-1}+1}^{t-1-k_{m-1}}\\ & & \cdots & & \\ 0 & \cdots\ 1 & \cdots & v_{l_m} & \cdots\ v_{l_m}^{t-1-k_{m-1}}\end{pmatrix};$$

[0259] S中的所有参与者可以合作解出如下的方程组:

[0260] $$\begin{cases} s+a_1v_1+a_2v_1^2+\cdots+a_{t-1}v_1^{t-1}=\sigma(u_1) & ;\\ \cdots & \\ s+a_1v_{l_0}+a_2v_{l_0}^2+\cdots+a_{t-1}v_{l_0}^{t-1}=\sigma(u_{l_0}) & \\ a_{k_0}+a_{k_0+1}v_{l_0+1}+\cdots+a_{t-1}v_{l_0+1}^{t-1-k_0}=\sigma(u_{l_0+1}) & \\ \cdots & \\ a_{k_0}+a_{k_0+1}v_{l_1}+\cdots+a_{t-1}v_{l_1}^{t-1-k_0}=\sigma(u_{l_1}) & \\ \cdots & \\ a_{k_{m-1}}+a_{k_{m-1}+1}v_{l_{m-1}+1}+\cdots+a_{t-1}v_{l_{m-1}+1}^{t-1-k_{m-1}}=\sigma(u_{l_{m-1}+1}) & \\ \cdots & \\ a_{k_{m-1}}+a_{k_{m-1}+1}v_{l_m}+\cdots+a_{t-1}v_{l_m}^{t-1-k_{m-1}}=\sigma(u_{l_m}) & \end{cases}$$

[0261] 即:

[0262] $$\begin{pmatrix}1 & v_1 & v_1^2 & \cdots & v_1^{t-1}\\ & & \cdots & & \\ 1 & v_{l_0} & v_{l_0}^2 & \cdots & v_{l_0}^{t-1}\\ 0 & \cdots\ 1 & \cdots & v_{l_0+1} & \cdots\ v_{l_0+1}^{t-1-k_0}\\ & & \cdots & & \\ 0 & \cdots\ 1 & \cdots & v_{l_1} & \cdots\ v_{l_1}^{t-1-k_0}\\ & & \cdots & & \\ 0 & \cdots\ 1 & \cdots & v_{l_{m-1}+1} & \cdots\ v_{l_{m-1}+1}^{t-1-k_{m-1}}\\ & & \cdots & & \\ 0 & \cdots\ 1 & \cdots & v_{l_m} & \cdots\ v_{l_m}^{t-1-k_{m-1}}\end{pmatrix}\begin{pmatrix}s\\ a_1\\ a_2\\ \cdot\\ \cdot\\ \cdot\\ a_{t-1}\end{pmatrix}=\begin{pmatrix}\sigma(u_1)\\ \cdots\\ \sigma(u_{l_0})\\ \sigma(u_{l_0+1})\\ \cdots\\ \sigma(u_{l_1})\\ \cdots\\ \sigma(u_{l_{m-1}+1})\\ \cdots\\ \sigma(u_{l_m})\end{pmatrix};$$

[0263] 可以看出，若S满足访问结构，就可以重构出多项式P(x)，从而恢复出秘密s；这个访问结构可以等价于分层矩阵的LSSS的访问结构，即令$I \subseteq \{1,\ldots,l_0,\ldots,l_m\}$被定义为I＝{j:ρ(j)∈S}，如果令$\{\lambda_j = M_v\vec{a}\}_{j\in I}$是秘密s的一个子秘密，则存在常数{ω$_j$∈$Z_N$}使得∑$_{j∈I}$ω$_j$λ$_j$＝s，其中，$\vec{a} = (a_1,\ldots,a_{t-1})^T$，$Z_N$表示1到N的整数集合；ω$_j$在秘密共享生成矩阵$M_v$大小的多项式时间内总可以被找到，就可以恢复出来主秘密；

[0264] 登录时通过扫描动态二维码，产生验证码进行输入进入虹膜验证，根据虹膜验证判断登录是否成功；

[0265] 验证码进行虹膜验证中，需进行虹膜信息的解密，包括：

[0266] 在得到密文Z′＝(z$_1$′,…,z$_{21}$′)后，首先计算：

[0267] Y′＝L_2^{-1}(Z′)＝(y$_1$′,…,y$_{21}$′)；

[0268] 对于点集P中的每一点(μ,λ)，计算：

[0269] $(y_1'',\cdots,y_{2l}'') = \tilde{F}^{-1}((y_1',\cdots,y_{2l}') + \lambda)$，

[0270] 然后验证Z(y$_1$″,…,y$_{21}$″)＝μ，如果不成立，则丢弃这组值；否则进行下一步；

[0271] 最后计算：

[0272] M′＝L_1^{-1}(y$_1$″,…,y$_{21}$″)＝(m$_1$′,…,m$_{21}$′)，

[0273] 如果只有唯一的一组(m$_1$′,…,m$_{21}$′)，那么M′就一定是对应的明文，如果得到超过一组的(m$_1$′,…,m$_{21}$′)，则用Hash函数或者增加验证方程的方式来确定唯一明文；

[0274] 解密前，需先进行虹膜的加密，包括：

[0275] 公钥生成：公钥由有限域k，以及它的加法和乘法结构和n个二次多元多项式组成；

[0276] 私钥生成：私钥由映射$\tilde{F}$随机选取的r个线性独立的z$_1$,…,z$_r$∈k[x$_1$,…,x$_{21}$]、一个点集P、两个可逆仿射变换L_1和L_2以及它们的逆组成；

[0277] 加密过程即给定明文M′＝(x$_1$′,…,x$_n$′)，用选取的公钥进行加密，形成密文Z′＝(z$_1$′,…,z$_n$′)；

[0278] 中心映射重新构造的过程包括以下步骤：

[0279] 首先，选择r是一个比较小的整数，随机选择r个线性独立方程

[0280] $z_1(x_1,\cdots,x_{2l}) = \sum_{j=1}^{2l}\alpha_{j1}x_j + \beta_1$

[0281] ⋮

[0282] $z_r(x_1,\cdots,x_{2l}) = \sum_{j=1}^{2l}\alpha_{jr}x_j + \beta_r$

[0283] 映射Z:k^{2l}→k^r如下确定：

[0284] Z(x$_1$,…,x$_{21}$)＝(z$_1$(x$_1$,…,x$_{21}$),…,z$_r$(x$_1$,…,x$_{21}$))，

[0285] 其次，随机选取2l个总次数为2的多项式$\hat{f}_1,\cdots,\hat{f}_{2l} \in k[z_1,\cdots,z_r]$，

[0286] 映射$\hat{F}$:k^r→k^{2l}如下确定：

[0287] 然后，定义扰动映射$F^*:k^{21}\rightarrow k^{21}$为$\hat{F}$和Z的复合：

[0288] 其中$f_1^*,\cdots,f_{21}^*\in k[x_1,\cdots,x_{21}]$，

[0289] 最后，用内部扰动映射F^*扰动原来的中心映射$\tilde{F}$，新的公钥映射为：

[0290] $$\overline{F}=L_2\circ(\tilde{F}+F^*)\circ L_1=(\overline{f}_1,\cdots,\overline{f}_{2l})；$$

[0291] 公钥生成包括以下步骤：

[0292] 选取有限域k，以及它的加法和乘法结构；

[0293] 选取21个二次多元多项式组：

[0294] $f_1(x_1,\cdots,x_{21}),\cdots,f_{21}(x_1,\cdots,x_{21})\in k[x_1,\cdots,x_{21}]$；

[0295] 私钥生成包括以下步骤：

[0296] 选取映射$\tilde{F}$，即两个随机数α_1,α_2；

[0297] 随机选取r个线性独立的$z_1,\cdots,z_r\in k[x_1,\cdots,x_n]$；

[0298] 选取一个点集P，P是所有映射$\hat{F}:k^r\rightarrow k^{21}$的像和原像的集合，即：

[0299] $$P=\left\{(\mu,\lambda)\,|\,\hat{F}(\mu)=\lambda\right\},$$

[0300] 点集P由随机选取的21个二次多项式$\hat{f}_1,\cdots,\hat{f}_{2l}\in k[z_1,\cdots,z_r]$确定；

[0301] 选取两个可逆仿射变换L_1和L_2以及它们的逆；

[0302] 第二步中具体包括如下步骤：

[0303] 2.1)令访问结构M_V是一个j×t矩阵；

[0304] 2.2)选择一个随机向量$\vec{y}=(y_0=s,y_1,.....,y_{t-1})\in Z_N^t$，$Z_N^t$表示1到N的整数集合中的任意t个，其中，s表示秘密值，$y_1,.....,y_{t-1}$为秘密值s的分享；

[0305] 2.3)令$S=\{v_1,...,v_{|S|}\}\subset U$，|S|表示S所具有的元素数量，设定满足：

[0306] $v_1,...,v_{l_0}\in U_0$；

[0307] $v_{l_0+1},...,v_{l_1}\in U_1$；

[0308] …

[0309] $v_{l_{m-1}+1},...,v_{l_m}\in U_m$；

[0310] 其中，$U_0,\cdots,U_m$表示集合U的第0至m层，$0\leqslant l_0\leqslant l_1\leqslant...\leqslant l_m=|S|$，当且仅当对于所有的$0\leqslant i\leqslant m$，有$l_i\geqslant k_i$，$l_i$表示第i层中拥有集合S的元素数量，$k_i$表示第i层中集合S的元素数量门限；

[0311] 然后对于所有的$j=1,...,l_0,...,l_m$，计算$\lambda_j=M_j\cdot\vec{y}$，$M_j$表示$M_V$中的第j行；

[0312] 2.4)对于属性集合U的层次数$i\in\{0,...,m\}$，设定$j=l_{i-1}+c$，$l_{-1}=0$，c为常数，表示第i层的第c个属性，即属性集合U中的第j个属性对应于第i层的第c个属性；

[0313] 2.5)选择随机数$r_{l_0,.....,}r_{l_m}\in Z_N$；

[0314] 2.6)将所有层次的属性通过以下表达式进行加密得出密文CT：

[0315] $$CT=\begin{Bmatrix} C=Me(g,g)^{\alpha s},(M_V,\rho) \\ C'=g^{s} \\ C_j=g^{a\lambda_j}h_{\rho(j)}^{-\sum_{x=l_0,\ldots\ldots l_i}r_x} \\ D_{l_0}=g^{r_{l_0}},\ldots\ldots,D_{l_m}=g^{r_{l_m}} \end{Bmatrix} k_{i-1}\le j\le k_i;$$

[0316] 其中，$h_{\rho(j)}$表示与属性集合U中的第ρ(j)个属性元素对应的群元素，ρ(j)表示属性集合U中第j层的属性到访问结构M_v的第j行的映射。

[0317] 验证模块对于虹膜识别的算法为：

[0318] (1)提取边缘

[0319] 用CCD获取的眼睛图像，包括巩膜、虹膜、瞳孔和上眼皮部分，将虹膜从整幅图像中分割出来，首先找出虹膜的内外边缘；

[0320] 选用高斯—拉普拉斯二阶微分滤波器∇^2G，∇^2G为二维高斯平滑滤波器G(x,y)与拉普拉斯算子$\nabla^2 f(x,y)$的组合：

[0321] $$G(x,y)=\frac{1}{2\pi\sigma^2}e^{-\frac{x^2+y^2}{2\sigma^2}}$$

[0322] $$\nabla^2 f(x,y)=\frac{\partial^2 f}{\partial x^2}+\frac{\partial^2 f}{\partial y^2}$$

[0323] 二阶微分滤波器为：

[0324] $$\nabla^2 G=\frac{\partial^2 G}{\partial x^2}+\frac{\partial^2 G}{\partial y^2}=\frac{1}{2\pi\sigma^4}\left(\frac{x^2+y^2}{\sigma^2}-2\right)e^{-\frac{x^2+y^2}{2\sigma^2}}$$

[0325] 该滤波器虽不是可分离的，但可写成：

[0326] $$\nabla^2 G=\frac{1}{2\pi\sigma^4}\left(\frac{x^2}{\sigma^2}-1\right)e^{-\frac{x^2}{2\sigma^2}}e^{-\frac{y^2}{2\sigma^2}}+\frac{1}{2\pi\sigma^4}\left(\frac{y^2}{\sigma^2}-1\right)e^{-\frac{y^2}{2\sigma^2}}e^{-\frac{x^2}{2\sigma^2}}=G_1+G_2$$

[0327] G1、G2均为可分离滤波器，采用分离算法，可以大大减少计算的复杂性；

[0328] 2G与图像进行卷积：$\nabla^2 G*g(x,y)$，g(x,y)表示图像上对应点的强度，“*”表示卷积，卷积后获得边缘；

[0329] (2)定位虹膜

[0330] 设虹膜的外圆、内圆方程为：

[0331] $(x-x_1)^2+(y-y_1)^2=r_1^2$

[0332] $(x-x_2)^2+(y-y^2)^2=r_2^2$

[0333] 用Houg h变换可获得(x_1,y_1,r_1)、(x_2,y_2,r_2)两组参数值，一般情况下$(x_1,y_1)\neq(x_2,y_2)$，即不是同心圆，因为瞳孔并不位于虹膜的中心，总是有所偏离，两个圆之间的部分，定义为虹膜部分；定义外边界圆的圆心(x_1,y_1)为虹膜的中心；定义外边界圆的半径r_1为虹膜的半径，获得了中心坐标(x_1,y_1)，即获得了实时图像相对参考图像的平移量，中心为(p,q)；获得了虹膜半径r_1，即获得了比例变化因子r_1/r，r为参考虹膜的标准半径；根据平移量

和比例变化因子对实时图像进行平移和比例校正,用双线性插值法插补,就消除了平移和比例变化;

[0334] (3)图像匹配

[0335] 上一步两个边界圆之间区域还包括眼皮部分,需去除该部分,以虹膜的中心为两坐标系的共同原点,将原直角坐标系转化为极坐标系,在极坐标系中,{(ρ,θ)70°<θ<110°}为含眼皮部分,去除;其余为只含有虹膜的部分,保留;保留下来可用于匹配、识别的虹膜部分约占全部虹膜面积的85%;

[0336] 一般情形下,虹膜的旋转变化较小,约在±5°左右,而虹膜图像相关性较强,有较长的相关长度,因此,将旋转变化等效为噪声即可,这样也可以简化计算;图像的匹配采用相关系数测度:

[0337] $$\rho = \frac{C}{\sqrt{C_{gg}C_{g'g'}}}$$

[0338] 其中,

[0339] $$C = \iint_{(x,y)\in D} \{g(x,y) - E[g(x,y)]\}\{g'(x,y) - E[g'(x,y)]\}\mathrm{d}x\mathrm{d}y$$

[0340] $$C_{gg} = \iint_{(x,y)\in D} \{g(x,y) - E[g(x,y)]\}^2\mathrm{d}x\mathrm{d}y$$

[0341] $$C_{g'g'} = \iint_{(x,y)\in D} \{g'(x,y) - E[g'(x,y)]\}^2\mathrm{d}x\mathrm{d}y$$

[0342] $$E[g(x,y)] = \frac{1}{|D|}\iint_{(x,y)\in D} g(x,y)\mathrm{d}x\mathrm{d}y$$

[0343] $$E[g'(x,y)] = \frac{1}{|D|}\iint_{(x,y)\in D} g'(x,y)\mathrm{d}x\mathrm{d}y$$

[0344] g′(x,y)为参考图像强度值,|D|为D的面积。

[0345] 指纹录入中,对于指纹采集的图像识别进行优化,具体方法如下:

[0346] (1)提取脊线

[0347] 将指纹图像分割成足够小的子块,以满足块中纹理近似平行的条件;

[0348] 对每个子块的每一个点p(s,t)利用Sobel算子分别计算x方向梯度gx和y方向梯度g_y,s,t=0,1,……w-1;

[0349] 每个子块方向θ(m,n)的计算公式如下:

[0350] $$\theta(m,n) = \frac{1}{2}\tan^{-1}\left\{\frac{\sum_{s=1}^{w}\sum_{t=1}^{w} 2g_x(s',t')g_y(s',t')}{\sum_{s=1}^{w}\sum_{t=1}^{w}\left[g_x^2(s',t') - g_y^2(s',t')\right]}\right\}$$

[0351] $s'=s+m\ W\ t'=t+n\ W$

[0352] (2)脊线频率

[0353] 脊线频率被定义为两条脊线之间间距的倒数，采用GABOR滤波器函数的实部作为模板，以与子块纹线方向垂直的方向作为滤波器方向，以脊线频率作为滤波器频率来构建滤波器，滤波过程如下式所示：

[0354]

$$G_E(s,t)=\left|\frac{1}{S}\sum_{y=\frac{W}{2}}^{\frac{W}{2}}\sum_{y=\frac{W}{2}}^{\frac{W}{2}}h_g(x,y,\theta(m,n),f(m,n),\sigma_x,\sigma_y)G(s+x,t+y)\right|$$

[0355] 其中，G(s,t)为原始灰度图像，$G_E(s,t)$是GARBOR滤波后的图像灰度，W为滤波器模板的大小，S为模板系数和，θ为子块的域方向值，GARBOR滤波器的θ与指纹纹理方向垂直，对σ_x和σ_y的取值进行折中，取值$\sigma_x=4$和$\sigma_y=4$。

[0356] 人脸面部识别算法为：

[0357] (1)对原始数据进行标准化采集，该集合x的维度为P，

[0358] $x=(X_1,X_2,X_3,\cdots,X_p)^T$，

[0359] 其中，n个样品的集合X_i为$X_i=(X_{1i},X_{2i},X_{3i},\cdots,X_{pi})^T$，$i=1,2,3,\cdots,n,n>P$，

[0360] 针对样本阵元进行标准化变换：

[0361] $$Z_{ij}=\frac{x_{ij}-\bar{x}_j}{s_j}\quad i=1,2,3,\cdots,n;j=1,2,3,\ \cdots,P$$

[0362] $$\bar{x}_j=\frac{1}{n}\sum_{i=1}^{n}x_{ij},$$

[0363] $$s_j^2=\frac{1}{n}\sum_{i=1}^{n}(x_{ij}-\bar{x}_j)^2,$$

[0364] 称为Z标准化阵；

[0365] (2)标准化阵Z的矩阵系数：

[0366] $$R=|r_{ij}|_PxP=\frac{Z^TZ}{n-1},$$

[0367] 其中，

[0368] $$r_{ij}=\frac{1}{n-1}(\sum Z_{kj}\cdot Z_{kj})\quad i,j=1,2,3,\cdots,P,$$

[0369] (3)求解R的特征方程

[0370] $|R-\lambda I_P|_P=0$，

[0371] 按照$\frac{\sum_{j=1}^{m}\lambda_j}{\sum_{j=1}^{P}\lambda_j}\geq 0.85$，确定m的值，对其中每一个$\lambda_j$，得到单位特征向量$b_j^0$；

[0372] (4)将指标变量转化为主成分：

[0373] $$U_{ij} = z_i^{\mathrm{T}} b_j^0 \quad j = 1,2,3,\cdots,m,$$

[0374] 式中:U_1为第一主成分;U_2为第二主成分;U_3为第三主成分;U_P为第P主成分;

[0375] (5)对载入的人脸图像进行几何归一化处理,假设载入的人脸图像的像素点为m×n,则将像素储存在列向量$(X_1,X_2,X_3,\cdots)^{\mathrm{T}}$中;

[0376] (6)求的平均人脸:

[0377] $$\mu_X = \frac{1}{M}\sum_{i=1}^{m} X_i,$$

[0378] 训练样本的协方差矩阵为:

[0379] $$c = \frac{1}{M}\sum_{i=1}^{m}(X_i - \mu_X)(X_i - \mu_X)^{\mathrm{T}},$$

[0380] 取差值向量:

[0381] $w_i = x_i - \mu_x$,

[0382] 令$\omega = (\omega_1, \omega_2, \omega_3, \cdots, \omega_n)$;

[0383] (7)投射到待检测空间,则每幅图像在特征空间的坐标函数为:

[0384] $y_i = U^{\mathrm{T}}(x_i - \mu_x) = U^{\mathrm{T}}\omega_i$,

[0385] 其中,

[0386] $$\begin{cases} U \in R^{N(M-1)} \\ x_i, \mu_X, W_i \in R^N \\ y_i \in R^{M-1} \end{cases}$$

[0387] 同样可以将待测图像x_{test}投射到特征子空间之中,

[0388] $y_{test} = U^{\mathrm{T}}(x_{test} - \mu_x)$

[0389] (8)利用距离分离器进行辨识,目标函数为:

[0390] $\min \mathrm{Dist} = \min||y_i - y_{test}||$。

[0391] 在上述实施例中,可以全部或部分地通过软件、硬件、固件或者其任意组合来实现。当使用全部或部分地以计算机程序产品的形式实现,所述计算机程序产品包括一个或多个计算机指令。在计算机上加载或执行所述计算机程序指令时,全部或部分地产生按照本发明实施例所述的流程或功能。所述计算机可以是通用计算机、专用计算机、计算机网络、或者其他可编程装置。所述计算机指令可以存储在计算机可读存储介质中,或者从一个计算机可读存储介质向另一个计算机可读存储介质传输,例如,所述计算机指令可以从一个网站站点、计算机、服务器或数据中心通过有线(例如同轴电缆、光纤、数字用户线(DSL)或无线(例如红外、无线、微波等)方式向另一个网站站点、计算机、服务器或数据中心进行传输)。所述计算机可读取存储介质可以是计算机能够存取的任何可用介质或者是包含一个或多个可用介质集成的服务器、数据中心等数据存储设备。所述可用介质可以是磁性介质,(例如,软盘、硬盘、磁带)、光介质(例如,DVD)、或者半导体介质(例如固态硬盘SolidStateDisk(SSD))等。

[0392] 以上所述仅是对本发明的较佳实施例而已,并非对本发明作任何形式上的限制,

凡是依据本发明的技术实质对以上实施例所做的任何简单修改，等同变化与修饰，均属于本发明技术方案的范围内。

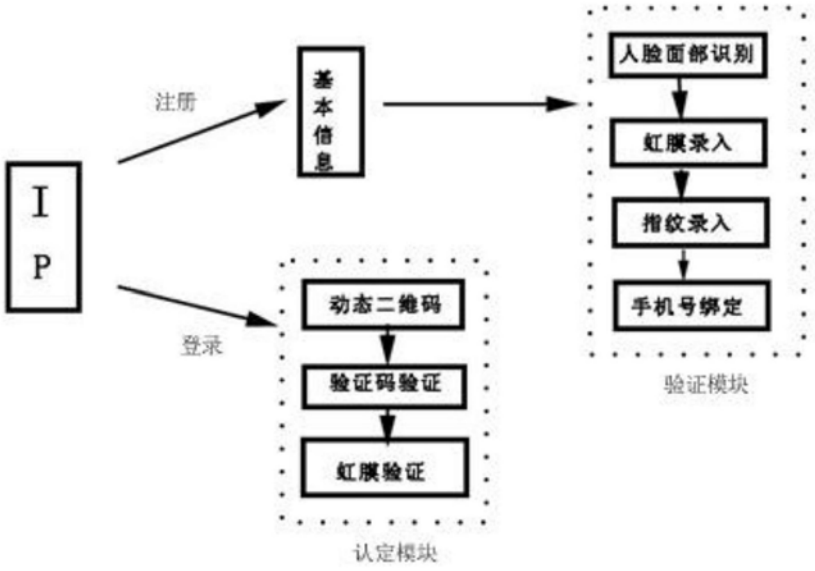

IP
注册
基本信息
登录
人脸面部识别
虹膜录入
指纹录入
手机号绑定
验证模块
动态二维码
验证码验证
虹膜验证
认定模块

图1


姓名
年龄
性别
地址
民族
身份证号
照片

图2