Computer Science and Application 计算机科学与应用, 2018, 8(5), 582-590
Published Online May 2018 in Hans. http://www.hanspub.org/journal/csa
https://doi.org/10.12677/csa.2018.85066

Hans汉斯

Design and Research of Face Recognition and Homomorphic Encryption Scheme Based on Image Subspace and Nuclear Sparse Representation

Sujian Wang, Xuan Wang

School of Physics and Information Technology, Shaanxi Normal University, Xi'an Shaanxi
Email: 250103041@qq.com

Received: Apr. 12th, 2018; accepted: Apr. 26th, 2018; published: May 3rd, 2018

Abstract

With the arrival of the era of big data and cloud computing, more and more user information is completely exposed on major Internet media. This poses great hidden dangers and security problems. In order to achieve protection of the user's personal privacy information, completing the secret calculation of face image data on the server side, this paper presents a facial image based on Kernel Discriminative Sparse Keeping Embedded Algorithm (KDSPE) combined with homomorphic encryption in cryptography and inadvertent transfer protocol based on Identity Encryption System (IBE) stealth identification algorithm. The terminal collects the data of the sample to be tested and the face image data of the database to compare, so as to judge whether the face data collected by the terminal exists in the database. The kernel sparse matrix obtained by the discriminative sparse hold embedding algorithm (KDSPE) is used here, and then the Euclidean distances of the nuclear sparse matrices of the human face of the terminal and the server are secretly calculated using the homomorphic encryption and the inadvertent transport protocol based on the identity encryption system (IBE) and then determining whether it matches. The advantage of this algorithm is that it can not only effectively extract facial nonlinear features, but also has good robustness in non-constrained environments (attitude, expression, lighting, occlusion, age, and shooting angle); in addition to the combination of knowledge of cryptography, this algorithm can also guarantee the data security of the communication participants and the security of the communication channel. Experimental results show that the proposed algorithm improves the face recognition rate and has certain algorithm security.

Keywords

Nuclear Technology, Face Recognition, Homomorphic Encryption, IBE Inadvertently Transmits

文章引用: 王素健, 王晅. 基于图像子空间和核稀疏表示的人脸识别及同态加密方案设计与研究[J]. 计算机科学与应用, 2018, 8(5): 582-590. DOI: 10.12677/csa.2018.85066

基于图像子空间和核稀疏表示的人脸识别及同态加密方案设计与研究

王素健，王　晅

陕西师范大学物理学与信息技术学院，陕西　西安
Email: 250103041@qq.com

收稿日期：2018年4月12日；录用日期：2018年4月26日；发布日期：2018年5月3日

摘　要

随着大数据和云计算时代的到来，越来越多的用户信息被完全暴露在各大互联网媒体上，这样就存在很大的隐患和安全性问题，为了保护用户的个人隐私信息，完成人脸图像数据在服务器端的隐秘计算，本文提出了核鉴别稀疏保持嵌入算法(KDSPE)结合密码学领域的同态加密和基于身份加密系统(IBE)的不经意传输协议的一种人脸图像隐秘识别方案。终端采集待测样本的数据和数据库的人脸图像数据进行对比，从而判断终端采集的人脸数据是否在数据库存在。这里利用KDSPE算法得到核鉴别稀疏矩阵，然后利用同态加密和基于身份加密系统(IBE)的不经意传输协议来隐秘计算终端和服务器人脸的核鉴别稀疏矩阵的欧式距离，进而判断是否匹配。该算法的优点在于除了可以有效的提取人脸非线性特征外，同时在非约束环境下(姿态，表情，光照，遮挡，年龄，拍摄角度)也有较好的鲁棒性，此外由于结合密码学的知识，该算法还可以保证通信参与者的数据安全和通信通道的安全性，实验结果表明本文算法提高了人脸识别率，同时具有一定的算法安全性。

关键词

核技术，人脸识别，同态加密，IBE不经意传输

1. 引言

随着互联网技术的高速发展，获得较好的人脸识别效果已经满足不了现在用户的需求，越来越多的用户开始注重自己的个人隐私数据的保护。比如现在的支付宝，微信，银行理财 APP 等许多关系到客户切身利益的系统，都需要来保证隐私安全，由于摄像机，监控，扫描器等是生物特征提取较为方便快捷的手段，也是现实生活中比较常见的获取人脸图像的终端，传统的人脸图像数据是以明文的形式存在数据库或者云端。而这种情况会被一些不法分子，投机者利用，来窃取，传播，篡改用户信息，尤其是在现今社会的资源共享，虚拟经济高速发展的大环境下，人脸数据的隐私性是现在必须要考虑进去的。所以在尽可能的保证人脸识别正确率的前提下，找到一种隐秘安全的计算方法应用到人脸识别技术当中，如果这种设计方案可以保证人脸数据的安全，那就说明这种方案是有用的。

稀疏保局投影(SPP)算法[1]是基于稀疏表示理论所提出的一种较为鲁棒的子空间特征提取方法，该算法进行稀疏重构某些样本时，会出现错误学习的情况，即可能会被与该样本不同类的其他样本错误逼近。针对(SPP)算法的问题，2012 年，Tan 等人[2]利用鉴别信息提出了基于鉴别稀疏保持嵌入(Discriminant Sparsity Preserving Embedding, DSPE)的人脸识别算法，该算法通过求解最小二乘问题来更新 SPP 算法的稀疏权重矩阵，得到一个鉴别稀疏矩阵，避免样本的误逼近，提高识别性能。DSPE 算法是一种线性流行学习子空间算法，虽然在 LPP 基础上做了改进，但是在复杂的非约束环境的条件下，DSPE 算法鲁棒性依然不足，同时该算法得到的是人脸图像的线性鉴别稀疏矩阵，而人脸结构在现实中是非刚性的，是非线性结构的。因此本文利用核技术的思想对 DSPE 算法做出了改进，提出了核鉴别稀疏保持嵌入(KDSPE)的算法。KDSPE 算法将原始样本通过非线性映射投影到高维空间中，然后将高维空间的计算转成利用核函数求解内积的问题。KDSPE 作为一个非线性的监督学习方法，不仅获得了图像全局最优低维嵌入，还有效的提取人脸非线性特征，同时在非约束环境下具有较好的鲁棒性。

近年来，随着人脸识别技术和密码学的快速发展，将安全的计算方法应用到传统的人脸识别技术中的研究热度持续上升。文献[3]中提出了一种结合同态加密和不经意传输协议的安全协议实现在云环境下的人脸识别隐秘算法，该方法具体较好的灵活性，可行性，安全性，该算法的人脸特征提取是线性的，同时不能很好的区分真实近邻和伪近邻，此外该算法的安全协议下的通信通道安全性不足。考虑到在高维空间的人脸特征提取，以及在不经意传输协议的使用过程中是否存在对参与者的隐秘信息存在泄露和通信通道的安全性的问题。本文利用同态加密和基于身份加密系统(IBE) [4]的不经意传输协议，提出一种基于核鉴别稀疏表示的隐秘人脸识别方案。终端采集待测样本的数据和数据库的人脸图像数据在安全协议下隐秘对比，从而判断终端采集的人脸数据是否在数据库存在。这里利用 KDSPE 算法得到的核鉴别稀疏矩阵，在安全协议下计算加密后的核鉴别稀疏矩阵的欧式距离来判断是否匹配。这种算法可以在保证不泄露双方信息的前提下进行人脸识别。具体系统要求如下：一种具有实用性，有效性的人脸识别算法 KDSPE。一种是利用同态加密和基于 IBE 的不经意传输协议的算法，这两种算法结合起来的算法可以保证终端和数据库都不会获取双方信息的情况下实现的。

2. 基本知识

2.1. 同态加密算法

同态加密[5]是：对经过同态加密的数据进行处理得到输出，然后对输出进行解密，其结果与未加密的数据处理的输出一样，设加密算法为 $E(\ )$，解密算法为 $D(\ )$。

加法同态性质：存在有效算法 $\oplus$，$E(x+y)=E(x)\oplus E(y)$ 或者 $x+y=D(E(x)\oplus E(y))$ 成立，显然完成 $x+y$ 的计算，无需解密 x，y。

乘法同态性质：存在有效算法 $\otimes$，$E(x\times y)=E(x)\otimes E(y)$ 或者 $x\times y=D(E(x)\otimes E(y))$ 成立，显然完成 $x\times y$ 的计算，无需解密 x，y。

2.2. 基于传统身份加密系统(IBE)的不经意传输协议

基于传统 IBE 的不经意传输协议[6]的描述及步骤：

描述：发送方同意采用不经意传输协议发送它的 n 个秘密信息 $\{m_1,m_2,\cdots,m_n\}$ 的加密信息给接受者，并允许接受者获得其中 k 个秘密信息 $\{m_{\delta_1},m_{\delta_2},\cdots,m_{\delta_k}\}$。

步骤：首先给出定义，发送者的公私钥对为 S_{pub}/S_{priv}，接受者的公私钥对为 R_{pub}/R_{priv}，发送者任意选取 $d_i\in Z_q^*,i=1,\cdots,n$，计算出 $P_i=d_iS_{pub}$ 作为选择的参照点同步发布出去，其中 $\{\delta_1,\delta_2,\cdots,\delta_k\}\in\{1,2,\cdots,n\}$。

接受者任意选取 k 个数 $a_j \in Z_q^*$，计算出 $V_j = a_j P_{\delta_j}, i = 1,2,\cdots,k$，并发送给发送者，发送者再任意选取随机数 $r \in Z_q^*$，计算出 $U_0 = rS_{pub}$，$U_j = rV_j$，密文 $c_i = m_i \oplus H_1\left(\hat{e}\left(P_i + S_{priv}, S_{pub}\right)^r\right)$，并发给接受者，接受者对接到的数据处理，计算 $W_j = a_j^{-1} U_j$，然后在计算 $m_{\delta_j} = c_{\delta_j} \oplus H_1(g)$，$g = \hat{e}\left(W_j, R_{pub}\right)\hat{e}\left(U_0, R_{priv}\right)$ 恢复出秘密消息 m_{δ_j}。

该协议安全性分析模型：

1) 本文是假设参与者是半诚实的，其中参与者包括发送方和接收方，参与者对数据的访问权限问题：

对发送方的隐私(相对于接收方)，假如接受者是半诚信攻击者，他想获得自己权限以外的数据 m_{n-k}，必须有解密辅助数据 rP_{n-k}，又因为 d_i, r 都是对接受者保密的，所以无法获得 $P_1, P_2, \cdots, P_n$ 之间的关联性，也就是说 rP_i 是 n 个相互独立的辅助数据，没有线性关系。再考虑到椭圆曲线离散对数困难假设问题，通过 $U_j, V_j, rS_{pub}, S_{pub}$ 求解 r, rP_i 是非常困难的。这就证明了基于 IBE 的不经意传输协议能够保证发送方的隐私。

对接受者的隐私(相对于发送方)，因为 a_j 是接受者随机选取的，对发送方是保密的。假设发送方计算出 $V_i d_{\delta_i}^{-1} = a_{\delta_i} S_{pub}$，由于 $a_{\delta_i} \neq a_{\delta_j}$，得 $a_{\delta_i} S_{pub} \neq a_{\delta_j} S_{pub}$，这就保证了接受者的隐私。

对接受者，发送者的隐私(相对于其他攻击者)，在现实环境中存在着各种攻击者，在本文中为了方便研究，我们定义这些攻击者为其他攻击者 A，同时我们只考虑了两种以下情况，假如其他攻击人想获得发送方发给接受者的信息，或者接收方发给发送方的信息。证明如下：

事实 1： A 不知道 a_i 的值，也就不知道 V_i 是由那个 P_i 计算出来的。

事实 2： 计算 $\left(rP_i, R_{priv}\right)$ 或 $\left(r_i, R_{priv}\right)$，必须知道 (r,s)，而这些参数是除发送者外所有人保密的。

事实 3： 即使 A 知道公钥系统的公共参数和截获的数据，计算 (r,s) 也是相当于计算椭圆曲线离散对数问题。

综上所述其他攻击人无法获得密文，这就保证了对接受者，发送者的隐私。

2) 通信通道的安全性：由于基于 IBE 的不经意传输协议充分利用了公钥系统的验证性，不需要提前协商安全通信通道，这就保证了通信通道的安全。

2.3. 基于 IBE 改进方案的不经意传输协议

2001 年，Cocks [7]等人基于二次剩余假设理论提出了第一个实用性的 IBE 方案，2005 年，Boneh [8]等人基于子群判定问题提出了可以对密文进行无限加法运算和一次乘法运算的 BGN 方案，同时利用二次多元多项式的思想重新评估了加密算法。2013 年，Clear 等人[4]基于 Cocks 的方案做出了改进，虽然同态加法的计算性能有所提高，但是只能支持加法同态性质。随后，2016 年，文献[9]基于 Cocks 和 Boneh 的方案提出了具有密文无限加和一次乘法同态性质的新型 IBSHE 方案。

现给出 Cocks 等人和 Boneh 等人算法的同态性质如下：

设系统的公钥为 (n, G, G_1, e, g, h)，明文 m_1, m_2 分别对应的密文 c_1, c_2，加密计算公式 $c_1 = g^b h^{e_1}, c_2 = g^c h^{e_2}$，得 $c_1 c_2 h^{e_3} = g^{b+c} h^{e_1+e_2+e_3}$。所以它满足同态加性质，由于受到 IBE 公钥密码系统的双线性对性质的限制，加密公式只能进行一次乘法运算，但不影响密文乘法运算后再无限进行加法运算。

本节的工作就是结合具有同态性质的 IBE 改进方案和不经意传输协议设计一个安全计算协议，由于 Cocks 等人和 Boneh 等人的算法是在传统身份加密系统的基础上改进的，所以本节设计的安全协议和 2.2 节的协议设计流程是一致的，主要区别是加密函数计算公式改变了，我们只需证明加密计算的正确性就可以，而 Boneh 等人的 BNG 方案中已经给出证明。同时本节设计的安全协议也符合根据基于传统身份加密系统(IBE)的不经意传输协议安全性分析模型的整体框架。

3. 改进算法

3.1. DSPE 算法

人脸超完备字典为 $X=[X_1,X_2,\cdots,X_C]$， X_i 为属于第 i 类的人脸样本集合。

a) 最小二乘法求解鉴别信息权重：

$$\begin{aligned}&\min_t \left\|x_{ij}-X_i t\right\|_2\\&s.t \quad It=1\end{aligned} \tag{1}$$

其中 $X_i=[x_{i1},x_{i2},\cdots,x_{ik}]\in R^{m\times k}$， I 为全 1 行向量。

b) 人脸样本由鉴别信息权重重构后得到的残差由其它类的所有样本进行稀疏重构：

$$\begin{aligned}&\min_s \|s\|_1\\&s.t \quad \left\|er-\widehat{Xs}\right\|<\varepsilon\\&\quad Is=0\end{aligned} \tag{2}$$

其中 $er=x_{ij}-X_i\tilde{t}=x_{ij}-X\tilde{h}$，超完备字典 $\hat{X}=[X_1,X_2,\cdots,X_C]$，其中 $X_i=O$。

c) 求解鉴别稀疏权重：

设 $\tilde{s}$ 是(2)的最优解，则将 $\tilde{s}$ 中的系数按照不同的类别进行分块，从而得 $\tilde{s}=[\tilde{s}_1,\cdots,\tilde{s}_{i-1},O,\tilde{s}_{i+1},\cdots,\tilde{s}_k]$，再结合(1)的最优解假设是 $\tilde{t}$，则更新后的鉴别稀疏权重设为 $\tilde{d}=\tilde{s}+\tilde{h}=[\tilde{s}_1,\cdots,\tilde{s}_{i-1},\tilde{t},\tilde{s}_{i+1},\cdots,\tilde{s}_k]\in R^n$。

DSPE 的目标函数为：

$$\begin{aligned}&\max_w \quad W^{\mathrm{T}}XMX^{\mathrm{T}}W\\&s.t \quad W^{\mathrm{T}}XX^{\mathrm{T}}W=1\end{aligned} \tag{3}$$

其中 $M=D+D^{\mathrm{T}}-D^{\mathrm{T}}D, D=[\tilde{d}_1,\tilde{d}_2,\cdots,\tilde{d}_n]$。

3.2. 本文 KDSPE 算法

3.2.1. 核稀疏表示

假设原始样本通过非线性映射 Φ 变换到一个高维的特征空间 H 上，则 X 在高维特征空间 H 中的表示为：

$$\Phi(X)=[\Phi(X_1),\Phi(X_2),\Phi(X_3),\cdots,\Phi(X_C)] \tag{4}$$

则高维空间的稀疏表示问题如下：

$$\min_W \|s\|_0 \quad s.t \ \Phi(X)s=\Phi(b) \tag{5}$$

其中 $\Phi(b)$ 是原始空间的一个样本信号 b 映射到高维空间形成的。

考虑到实际环境噪声的影响，一般无法精确重构原始信号，设 ε 是误差容，

(5)常被写成下列形式：

$$\min_W \|s\|_1 \quad s.t \ \left\|\Phi(X)s-\Phi(b)\right\|<\varepsilon \tag{6}$$

因为 $\Phi(X)$ 和 $\Phi(b)$ 都是未知的，根据高维空间中的内积可以用核函数 $K(x,y)$ 求解，对于任意的 x,y，有 $\Phi(x)^{\mathrm{T}}\Phi(y)=K(x,y)$，再根据定理 1，如下：

定理 1：对任意的 $\varepsilon\geq 0$，都存在 $\delta\geq 0$，只要 $\left\|\Phi(X)^{\mathrm{T}}\Phi(X)s-\Phi(X)^{\mathrm{T}}\Phi(b)\right\|\leq\delta$，就一定有

$\left\|\Phi(X)s-\Phi(b)\right\|\le\varepsilon$ 。

(6)的求解问题转换为：

$$\min_{W}\ \|s\|_1 \quad s.t\ \left\|\Phi(X)^{\mathrm{T}}\Phi(X)s-\Phi(X)^{\mathrm{T}}\Phi(b)\right\|\le\delta \tag{7}$$

3.2.2. KDSPE 算法

根据 3.2.1 节的理论介绍，可将(1)，(2)分别表示如下：

$$\min_{t}\ \left\|\Phi(X_i)^{\mathrm{T}}\Phi(x_{ij})-\Phi(X_i)^{\mathrm{T}}\Phi(X_i)t\right\| \quad s.t\ \ It=1 \tag{8}$$

$$\min_{s}\ \|s\|_1 \quad s.t\ \left\|\Phi(\hat{X})^{\mathrm{T}}\Phi(er)-\Phi(\hat{X})^{\mathrm{T}}\Phi(\hat{X})s\right\|\le\delta,\ Is=0 \tag{9}$$

得到的核鉴别稀疏权重设为 $\hat{\tilde{d}}=\hat{\tilde{s}}+\hat{\tilde{h}}=\left[\hat{\tilde{s}}_1,\cdots,\hat{\tilde{s}}_{i-1},\hat{\tilde{t}},\hat{\tilde{s}}_{i+1},\cdots,\hat{\tilde{s}}_k\right]$。

通过 $\hat{\tilde{d}}$ 建立 KDSPE 目标函数：

$$\begin{aligned}&\max_{W}\quad W^{\mathrm{T}}\Phi(X)\hat{M}\Phi(X)^{\mathrm{T}}W\\&s.t\quad\ W^{\mathrm{T}}\Phi(X)\Phi(X)^{\mathrm{T}}W=1\end{aligned} \tag{10}$$

其中 $\hat{M}=\hat{D}+\hat{D}^{\mathrm{T}}-\hat{D}^{\mathrm{T}}\hat{D},\hat{D}=\left[\hat{\tilde{d}}_1,\hat{\tilde{d}}_2,\cdots,\hat{\tilde{d}}_n\right]$

由拉格朗日乘子法的，设：

$$L^{\Phi}(W,\lambda)=W^{\mathrm{T}}\Phi(X)\hat{M}\Phi(X)^{\mathrm{T}}W-\lambda\left(W^{\mathrm{T}}\Phi(X)\Phi(X)^{\mathrm{T}}-1\right) \tag{11}$$

对(11)求导得：

$$\Phi(X)\hat{M}\Phi(X)^{\mathrm{T}}W=\lambda\Phi(X)\Phi(X)^{\mathrm{T}}W \tag{12}$$

设投影向量 $W=\Phi(X)a$ 代入(12)求得前 d 个最大本征值的本征向量 $a_i\left(i=1,2,\cdots,d\right)$，求得映射 $W_{KDSPE}=\left[a_1,a_2,\cdots,a_d\right]$。

3.3. 本文加密方案

3.3.1. 核鉴别稀疏矩阵欧式距离算法

通过 KDSPE 得到的核鉴别稀疏权重，计算两矩阵的欧氏距离来判断人脸相似性。两个 n 维向量 $a\left(x_{11},x_{12},\cdots,x_{1n}\right)$ 与 $b\left(x_{21},x_{22},\cdots,x_{2n}\right)$ 的欧式距离：

$$d_{12}=\sqrt{\sum_{k=1}^{n}\left(x_{1,k}-x_{2,k}\right)^2} \tag{13}$$

训练人脸字典的训练样本建立为 20 个人 5 张不同的人脸图像，经过图像预处理(这里取 18 个像素值)，得到这样一个矩阵：每列代表一个图像的所有像素：

$$\begin{bmatrix}b_{11}&b_{21}&\cdots&b_{100,1}\\b_{12}&b_{22}&\cdots&b_{100,2}\\\vdots&\vdots&\ddots&\vdots\\b_{1,18}&b_{2,18}&\cdots&b_{100,18}\end{bmatrix} \tag{14}$$

经过标准化得到一个 18×200 的标准化人脸字典矩阵。设两个不同的测试样本 b_1 和 b_2，由公式(8)，(9)分别得到相应的核鉴别稀疏矩阵：

$$\hat{\tilde{d}}_1=\left[\hat{\tilde{s}}_{1,1},\cdots,\hat{\tilde{s}}_{1,i-1},\hat{\tilde{t}}_1,\hat{\tilde{s}}_{1,i+1},\cdots,\hat{\tilde{s}}_{1,k}\right]$$
$$\hat{\tilde{d}}_2=\left[\hat{\tilde{s}}_{2,1},\cdots,\hat{\tilde{s}}_{2,i-1},\hat{\tilde{t}}_2,\hat{\tilde{s}}_{2,i+1},\cdots,\hat{\tilde{s}}_{2,k}\right],\quad k=200 \tag{15}$$

利用(15)计算两个矩阵的欧式距离：

$$\sqrt{\sum_{k=1}^{n}\left(\hat{\tilde{s}}_{1,k}-\hat{\tilde{s}}_{2,k}\right)^2+\left(\hat{\tilde{t}}_1-\hat{\tilde{t}}_2\right)^2},\ k\neq i,n=200 \tag{16}$$

3.3.2. 基于核鉴别稀疏表示的隐秘人脸识别方案

加密方案准备工作：为了方便同态加密的计算，在这里我们根据(13)式可以重新定义核稀疏矩阵的欧式距离为：

$$d_{12}^2=\sum_{k=1}^{n}\left(x_{1,k}-x_{2,k}\right)^2 \tag{17}$$

由公式(15)，(16)，(17)可知欧式距离的最大数量级为 10^5，并设 $d_{\max}=10^5$，我们对 2.2 节介绍的允许接受者获得其中 k 个秘密信息进行 k 赋值为 1，然后设 200 对公钥对等分 $d_{\max}$，每份 500，这样构造出 1-out-of-200 的不经意传输协议，发送者是服务器，它的输出是 $X_0,\cdots,X_{n-1}$。接收者是终端，它的输入是欧式距离 d_E。我们设协议映射规则为如果 $(d_E)\bmod(d_{\max})$ 小于阈值 t_i，则 X_i 等于 1 表示匹配，否则等于 0 表示不匹配，其中 $d_E\in\left[500\cdot i,500\cdot(i+1)\right]$。

总体方案具体设计步骤：

1) 终端发送人脸图像的核稀疏矩阵 $\hat{\tilde{d}}=\left[\hat{\tilde{s}}_1,\cdots,\hat{\tilde{s}}_{i-1},\hat{\tilde{t}},\hat{\tilde{s}}_{i+1},\cdots,\hat{\tilde{s}}_k\right]$ 每一位的同态加密结果和每一位的平方值 $\hat{\tilde{d}}^2=\left[\hat{\tilde{s}}_1^2,\cdots,\hat{\tilde{s}}_{i-1}^2,\hat{\tilde{t}}^2,\hat{\tilde{s}}_{i+1}^2,\cdots,\hat{\tilde{s}}_k^2\right]$ 的加密结果。服务器接收到的同态加密后的数据分别就是：$\left\{E_{pk}\left(\hat{\tilde{s}}_1\right),\cdots,E_{pk}\left(\hat{\tilde{s}}_{i-1}\right),E_{pk}\left(\hat{\tilde{t}}\right),E_{pk}\left(\hat{\tilde{s}}_{i+1}\right),\cdots,E_{pk}\left(\hat{\tilde{s}}_k\right)\right\}$ 和 $\left\{E_{pk}\left(\hat{\tilde{s}}_1^2\right),\cdots,E_{pk}\left(\hat{\tilde{s}}_{i-1}^2\right),E_{pk}\left(\hat{\tilde{t}}^2\right),E_{pk}\left(\hat{\tilde{s}}_{i+1}^2\right),\cdots,E_{pk}\left(\hat{\tilde{s}}_k^2\right)\right\}$，对于服务器里数据库的每一个人脸图像的核稀疏矩阵 $\hat{\tilde{d}}^i\in\left\{\hat{\tilde{d}}^1,\cdots,\hat{\tilde{d}}^N\right\}$ 做出以上同样的操作。

2) 服务器进行欧式距离的计算，针对向量中的每一位 j，为了方便计算设 $\hat{\tilde{d}}_j$ 代表获得的核稀疏矩阵里的向量，$\hat{\tilde{d}}_j^i$ 代表数据库里的每一个人脸图像的核稀疏矩阵里的向量。设 $v_j=\left(\hat{\tilde{d}}_j-\hat{\tilde{d}}_j^i\right)^2$，计算出每一位的加密后的距离 $E_{pk}\left(v_j\right)$。然后利用同态加密的加法特性计算出总的加密距离 $E_{pk}\left(d_E\right)=\sum_1^k E_{pk}\left(v_j\right)$。

3) 服务器将计算出的 $E_{pk}\left(d_E\right)$，发给终端，终端收到后进行解密，双方通过 1-out-of-200 不经意传输协议映射规则来进行匹配。

4. 实验结果

在 AR，FERET，CMU-PIE 这三个人脸库分别取 20 个人 5 张不同的 100 张人脸图像，针对每个库进行 10 次重复测试，然后取测试数据的平均值，以下给出 DSPE(主要成分分析方法降维)和 KDSPE(核函数为高斯核函数)在 AR，FERET，CMU-PIE 这三个人脸库的人脸识别率数据对比，如表 1 所示。

对于 AR 的 100 张图像，随机取出 10 张图像放在电脑终端，然后把这 100 张的图像存到服务器的数据库里建立数据集。然后进行数据测试，终端的 10 张图像里每张图像测试出一个匹配率，然后对这 10 条数据进行均值化，作为 AR 人脸库匹配率，同理对于 FERET，CMU-PIE 也是做同样的操作，KDSPE 的欧式距离算法和 KDSPE 结合基于 IBE 公钥系统的不经意传输协议加密的欧式距离算法在数据库样本库上的匹配正确率的数据对比，如表 2 所示。

为了对比本文的加密算法和未加密算法的系统运行时间，单位是秒，测试数据分别是来自 AR，FERET，CMU-PIE 人脸库的 100 张图像里的 10 张图像，分别对属于各个库的 10 张图像进行系统匹配运行时间进行测试，最终的测试数据取 10 条数据的平均值，如图 1 所示。

5. 本文特点与总结

特点：本文研究了传统的人脸特征提取算法，利用核函数的技巧，提出了一种非线性流行学习子空间 KDSPE 算法；本文用核稀疏表示的人脸特征向量长度远远小于传统的图像块提取方法表示的向量长度。大大减少了算法的计算复杂度，提高了运行效率。同时，利用 IBE 公钥系统来构造不经意传输协议，引用一种改进的 IBE 方案使其满足同态加密性质，这样就可以在服务器端实现安全计算。

总结：本文基于图像子空间和稀疏表示的 DSPE 算法，同时结合核稀疏的理论，提出了 KDSPE 算法，考虑到算法安全问题，结合同态加密和基于 IBE 的不经意传输协议，设计了一种隐秘安全的人脸识别算

Table 1. Comparison of recognition rate of two face recognition algorithms
表 1. 两种人脸识别算法的识别率的对比

方法	AR	FERET	CMU-PIE
DSPE	80.3	89.5	95.8
KDSPE(本文算法）	91.3	95.7	97.4

Table 2. Comparison of matching accuracy of KDSPE and unencrypted KDSPE algorithm
表 2. KDSPE 和未加密 KDSPE 算法的匹配正确率%的对比

方法	AR	FERET	CMU-PIE
KDSPE 欧式距离(本文算法)	84.55	82.63	90.21
加密 KDSPE 欧式距离(本文算法)	83.94	85.33	91.35

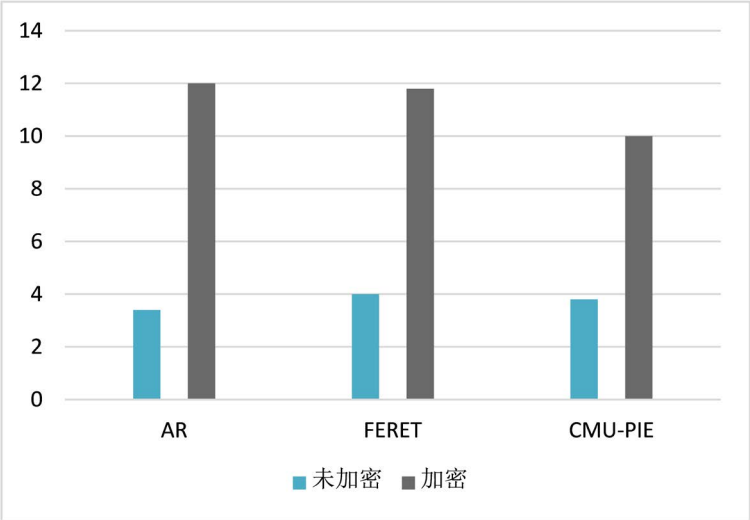

Figure 1. Comparison of the running time between the encryption algorithm KDSPE euclidian distance and the unencrypted KDSPE euclidian distance algorithm
图 1. 加密算法 KDSPE 欧式距离和未加密 KDSPE 欧式距离算法运行时间对比

法，通过对本文算法的数学推导，可行性分析，安全性分析，实验结果分析认为该算法具有识别率高，实用性强的优点，但是本文算法在时间效率问题存在一些问题，使得算法有些不太灵活。

参考文献

[1] Qiao, L.S., Chen, S.C. and Tan, X.Y. (2010) Sparsity Preserving Projections with Applications to Face Recognition. *Pattern Recognition*, **43**, 331-341. https://doi.org/10.1016/j.patcog.2009.05.005

[2] 谭延琪. 基于稀疏表示和子空间的人脸识别方法研究[D]: [硕士学位论文]. 苏州: 苏州大学, 2012.

[3] 刘妍, 金鑫, 赵耿, 等. 基于稀疏表示的云环境中人脸图像隐秘识别方法[J]. 系统仿真学报, 2015, 27(10): 2291-2298.

[4] Clear, M., Hughes, A. and Tewari, H. (2013) Homomorphic Encryption with Access Policies: Characterization and New Constructions. *International Conference on Cryptology in Africa*, **7918**, 61-87.

[5] 陈志伟, 杜敏, 杨亚涛, 等. 基于 RSA 和 Paillier 的同态云计算方案[J]. 计算机工程, 2013(7): 35-39.

[6] 李顺东, 徐彦蛟. 不经意传输协议的研究[D]: [硕士学位论文]. 西安: 陕西师范大学, 2014.

[7] Cocks, C. (2001) An Identity-Based Encryption Based on Quadratic Residues. *Proceedings of International Conference on Cryptography and Coding*, **2260**, 360-363.

[8] Boneh, D., Goh, E.J. and Nissim, K. (2005) Evaluating 2-DNF Formulas on Ciphertexts. *LNCS*, **3378**, 325-342. https://doi.org/10.1007/978-3-540-30576-7_18

[9] 戴晓明, 张薇, 郑志恒, 等. BGN-型类同态 IBE 方案的构造与分析[J]. 计算机应用与软件, 2016: 311-312.