Journal of System Simulation

Volume 28 | Issue 9 Article 39

8-14-2020

Private Face Detection Based on Random Sub-images in Cloud

Yuan Peng
1. Beijing Electronic Science and Technology Institute, University, Beijing 100070, China;;2. Xidian University, University, Xi'an 710071, China;

Jin Xin
1. Beijing Electronic Science and Technology Institute, University, Beijing 100070, China;;

Xiaodong Li
1. Beijing Electronic Science and Technology Institute, University, Beijing 100070, China;;

Zhao Geng
1. Beijing Electronic Science and Technology Institute, University, Beijing 100070, China;;

See next page for additional authors

Private Face Detection Based on Random Sub-images in Cloud

Abstract

Abstract: In order to detect faces of terminal face image in the cloud at the same time protect both privacy of data,a method of face images privacy detection based on random sub-Images representation was proposed. *Terminal divided original image into 2 value sub-images weighted sum based on random sub-images generation algorithm and randomly arranges weights of sub-images. Terminal sent sub-images according to the weights of random sequence to the cloud server*. Cloud server detected sub-images with its face detection algorithm. Terminal merges test results based on random sub were exploded. *Two random vectors were leveraged to protect the parameters of the trained face detector and the content of the terminal image. The innovation of this method is that the random sub-images thought is proposed and is applied to the image face detection making privacy face detection achieve in the cloud*.

Keywords

cloud, face detection, privacy, random sub-image, random vectors

Authors

Yuan Peng, Jin Xin, Xiaodong Li, Zhao Geng, Yaming Wu, Mingxin Ma, Yulu Tian, and Yingya Chen

Recommended Citation

Yuan Peng, Jin Xin, Li Xiaodong, Zhao Geng, Wu Yaming, Ma Mingxin, Tian Yulu, Chen Yingya. Private Face Detection Based on Random Sub-images in Cloud[J]. Journal of System Simulation, 2016, 28(9): 2195-2200.

第 28 卷第 9 期 系统仿真学报© Vol. 28 No. 9
2016 年 9 月 Journal of System Simulation Aug., 2016

基于随机子图表示的云环境人脸图像隐秘检测

袁鹏[1,2]，金鑫[1]，李晓东[1]，赵耿[1]，吴亚明[1,2]，马铭鑫[1,2]，田玉露[1]，陈迎亚[1]
(1. 北京电子科技学院，北京 100070；2. 西安电子科技大学，西安 710071)

摘要： 为了在云端服务器中进行终端用户的人脸图像检测的同时能够保护双方的数据隐私，提出了一种基于随机子图表示的人脸图像隐秘检测方法。*终端将原图像根据随机子图产生算法划分为 2 值的子图像加权和，将子图像的权值随机排序，将子图像按照权值随机排列的顺序发给云端服务器。*云端服务器利用其人脸检测算法对子图像进行检测，终端根据随机子图分解合并检测结果。*云端和终端都引入了随机数机制，以保护终端的人脸图像信息和云端的人脸检测算法参数。该方法的创新点是提出了随机子图算法并应用于图像的人脸检测中，使云端隐私保护的人脸检测得以实现。*

关键词： 云端；人脸检测；隐秘；随机子图；随机数
中图分类号：TP319 文献标识码：A 文章编号：1004-731X (2016) 09-2195-06

Private Face Detection Based on Random Sub-images in Cloud

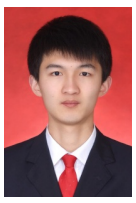
Yuan Peng[1,2], *Jin Xin*[1], *Li Xiaodong*[1], *Zhao Geng*[1], *Wu Yaming*[1,2], *Ma Mingxin*[1,2], *Tian Yulu*[1], *Chen Yingya*[1]
(1. Beijing Electronic Science and Technology Institute, University, Beijing 100070, China; 2. Xidian University, University, Xi'an 710071, China)

Abstract: In order to detect faces of terminal face image in the cloud at the same time protect both privacy of data,a method of face images privacy detection based on random sub-Images representation was proposed. *Terminal divided original image into 2 value sub-images weighted sum based on random sub-images generation algorithm and randomly arranges weights of sub-images. Terminal sent sub-images according to the weights of random sequence to the cloud server*. Cloud server detected sub-images with its face detection algorithm. Terminal merges test results based on random sub were exploded. *Two random vectors were leveraged to protect the parameters of the trained face detector and the content of the terminal image. The innovation of this method is that the random sub-images thought is proposed and is applied to the image face detection making privacy face detection achieve in the cloud.*

Keywords: cloud; face detection; privacy; random sub-image; random vectors

引言

随着云计算、移动互联网、社交网络等技术的发展，云端的计算和存储能力日益强大，与此同时监控摄像头泛滥导致图像视频数量迅速增加。众所周知，图像视频的处理需要强大的计算能力。因此，越来越多的图像视频处理在云端完成，然而图像视频的隐私内容也被暴露在云端。终端利用云端强大的计算能力和机器视觉算法进行图像的检测、识别、视频前景提取，但有些图像视频涉及个人隐私，终端并不希望图像视频隐私暴露在云端。同时，强大的可视媒体文件分析云服务会花费云服务提供商许多财力物力。他们当然也不愿意泄露自己辛辛苦苦训练的模型的参数或者是受版权保护的算法细节。



收稿日期：2016-05-31 修回日期：2016-07-11；
基金项目：国家自然科学基金(61170037, 61402021)，中央高校基本科研业务(2015XSYJ25)，国家档案局科技计划(2015-B-10)，虚拟现实技术与系统国家重点实验室开放课题(BUAA-VR-16KF-09)；
作者简介：袁鹏(1992-)男，宁夏石嘴山，硕士，研究方向为人脸检测、信息安全。

传统保护图像隐私的一种方法是在从终端传送到服务器端时对图像进行加密，到云端解密图像得到原始图像，然后对原始图像进行操作，然而这种方法有时并不能满足要求。例如一个云服务中心通过 web 网站提供人脸检测的功能，终端也许会对该服务感兴趣，但是它拒绝泄露图像信息即使是对提供服务的云端，终端也许是不想让云端获得图像隐私内容，也许是担心云端被病毒攻击泄露了图像内容。

为了具体描述本文的算法，假设一个视频监控场景，Alice(终端)拥有监控摄像头和 Bob 拥有一个正在运行人脸检测算法的云端服务器。在假设的场景中，Alice 和 Bob 之间按照一个约定协议进行数据交换，从而使 Alice 可以得到其敏感监控图像集里人脸的位置，但是不能获得 Bob 的人脸检测算法的任何参数，而 Bob 无法学习到终端敏感图像集的任何信息。

本文提出了一种基于随机子图表示的人脸图像隐秘检测算法，我们将一幅图像随机分成 256 幅 0、1 像素基准图像，每张基准图像的权值只有客户端知晓。基准图像被随机发送到服务端。服务端从基准图像中什么都复原不出来。用两个随机向量来保护人脸检测的参数。此算法使得整图的处理速度大幅提升。实验结果显示我们的方法比传统的盲处理方法快很多，并且理论上造成信息泄露的风险很低。

人脸检测是指在输入图像中确定所有人脸(如果存在)的位置与大小。人脸检测系统的输入是可能包含人脸的图像，输出是关于图像中是否存在人脸以及人脸的数目、位置、尺度等信息的参数化描述。目前人脸检测算法模型很多，如 ANN 模型、SVM 模型、Adaboost 模型等。Viola&Jones 人脸检测算法[1]利用 Adaboost 模型，其在速度、鲁棒性与精度的综合性能上是最优的[2]，所以本文采用的人脸检测算法是 Viola&Jones 人脸检测算法。

随着监控摄像头的泛滥，引发了人们对隐私泄露的担忧，这一问题应该被解决。2006 年 Shai Avidan and Moshe Butman 在《Blind Vision》上提出了一种把安全多方计算协议[3]应用到 Viola & Jones 人脸检测算法实现的一种基于不经意传输的人脸图像隐秘检测算法[4]。该算法使用的加密工具是不经意传输协议(OT)[5]，用 OT 构造 Secure Dot Product、Secure Millionaire 安全协议，利用这些安全协议构造了 Secure Classifier 协议达到人脸图像隐秘检测的目的。Secure Classifier 协议主要问题是大量的加解密计算和没有利用积分图像加速人脸检测，严重影响基于不经意传输的人脸图像隐秘检测算法的计算速度。论文的实验部分指出：一个 24×24 的检测窗口被检测需要几分钟，一幅 240×320 的图片大约有 150 000 个检测窗口，所以检测一幅 240×320 的图片需要花费大量的时间，这样检测一幅图片花费的代价太高。综上所述，基于不经意传输的人脸图像隐秘检测算法并不是很理想。

在那之后，Avidan 和 Butman 提出了一系列机器学习技术，可以被认为是不需要加密的解决盲视人脸检测的方法。然而他们方法的副作用是会泄露一定量的可控信息。

最近 Bost 提出了基于加密数据的机器学习分类方法。他们构建了三个主要的分类协议来满足隐私保护限制：超平面决策，朴素贝叶斯，决策树。他们重点关注提供一系列通用分类器和构造构件来建造更复杂的分类器。

很多研究者都研究盲视问题，主要都是朝着加密的方向。然而我们的目标是使得盲视朝着不损失安全性能的非加密方向努力。

1 Viola&Jones 人脸检测算法

Viola&Jones 人脸检测算法是一种基于积分图、Adaboost 学习算法和级联检测器的方法，具有鲁棒性强、检测率高等特点。这种方法首先采用一种被称为“积分图”的方法快速地计算出大量的简单 Haar 特征，再用 Adaboost 学习算法[6-7]从一个较大的特征集中选出少量关键的分类能力较强的特征构造出一系列弱分类器，而后通过线性组合将

这些弱分类器组合构成一个强分类器，最后通过 Cascade 级联算法将多个强分类器合成为一个更加复杂的人脸检测器。

1.1 矩形特征

矩形特征也叫类 Haar 特征，能有效区别人脸与非人脸，最初的类 Haar 特征是由 Papageorgiiou 提出的。在 Viola&Jones 人脸检测系统中，每个弱分类器都是图像一个特征值的判断。矩形特征对一些简单的图形结构，如边缘、线段，比较敏感，但是其只能描述特定走向(水平、垂直、对角)的结构，因此比较粗略。脸部一些特征能够由矩形特征简单地描绘，例如，通常眼睛要比脸颊颜色更深；鼻梁两侧要比鼻梁颜色要深；嘴巴要比周围颜色更深。

1.2 Viola&Jones 人脸检测分类器

对于一个 24×24 的检测器，其内部的矩形特征数量超过 18 000 个，必须用 Adaboost 学习算法甄选合适的矩形特征。现在已经有了简单的特征，还需要一些简单的分类器。为了能使得这些分类器足够的简单，把分类器和这些矩形特征进行一一对应。亦即每个分类器就由一个特征值来决定。于是得到如下的简单分类器原型：

$$h_j(x)=\begin{cases}0 & \text{if } p_j f_j(x) < p_j\theta_j \\ 1 & \text{otherwise}\end{cases} \tag{1}$$

式中：f 为特征值，θ 为阈值，p 指示不等号的方向，x 代表一个检测子窗口。对于每一个特征 f，训练一个弱分类器 $H(x, f, p, \theta)$就是确定 f 的最优阈值。

AdaBoost 学习算法用于选择特征和训练分类器，给定一组正负样本及特征，训练出这些特征各自的弱分类器，选择一些分类能力较强的弱分类器，将这些弱分类器组合成一个更加复杂、分类能力更强的强分类器。算法的关键是当分类器正确分类时，减少样本的权值，当分类错误时，增加样本的权值，让学习算法能够在后面的学习中对比较困难的样本进行训练，最后得到一个检测率较高的强分类器。强分类器的函数形式如公式(2)所示：

$$H(x)=sign\left(\sum_{n=1}^{N}h_n(x)\right)3 \tag{2}$$

其中，$h_n(x)$是弱分类器函数形式如公式(3)所示：

$$h_n(x)=\begin{cases}\alpha_n & x^T y_n > \theta_n \\ \beta_n & \text{otherwise}\end{cases} \tag{3}$$

其中 x 为图像向量，y 为矩形的权值，θ 为弱分类器的阈值，α 和 β 是利用 Adaboost 学习算法训练出来的，N 是强分类器里包含的弱分类器的个数。

2 基于随机子图表示的人脸图像隐秘检测

2.1 随机子图产生算法

在基于随机子图表示的人脸图像隐秘检测算法中，Alice 首先按照随机子图产生算法将原始图像 X(m 行，n 列)划分为 2 值的子图像加权和，然后把子图像的权值随机排序，将子图像按权值随机排列的顺序发给 Bob。随机子图产生见算法 1，示意图如图 1 所示。

算法 1：随机子图产生算法

输入：图像 X(s 行，t 列)

输出：256 幅 2 值的子图像

1、将输入图像转化为每个像素为 0~255 的二维矩阵；

2、Alice 创建 256 幅子图像 SM_r，每个子图像有 s 行和 t 列，这些子图的像素初始化为 0，第 r 幅子图像 SM_r 的权值为 $Q[r]=r$，其中 r 的取值范围为 0~255；

3、对于图像 X 中的每一个像素 $X[i,j]$，Alice 都做如下子过程，直到 $X[i, j]$为 0。

(1) 产生一个随机数 r，r 的取值范围 $X[i, j]/2 < r \leqslant X[i, j]$，设置权值为 r 的子图像的 $SM_r[i, j]$点像素值为 1；

(2) 重置 $X[i,j]=X[i, j]-r$，然后转到过程(1)，直到 $X[i, j]=0$；

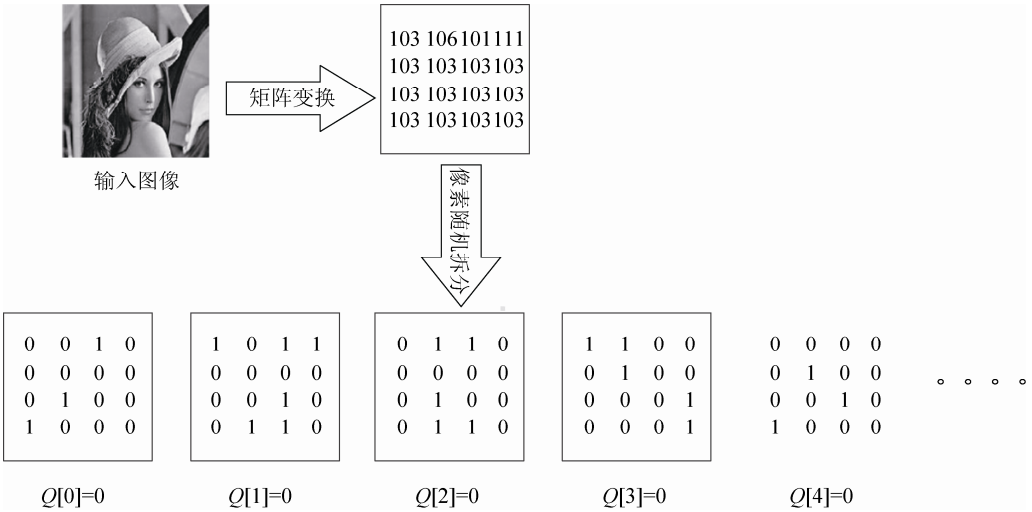


图 1 随机子图产生示意图

2.2 基于随机子图表示的人脸图像隐秘检测算法

基于随机子图表示的人脸图像隐秘检测算法就是让 Alice 把图像通过随机子图产生算法将原图像随机生成 256 张 2 值的子图像，然后把子图像的权值随机排序，将子图像按权值随机排列的顺序发给 Bob。Bob 对子图像进行检测，Alice 根据随机子图分解合并检测结果。最终 Alice 得到图像中是否存在人脸，如果存在人脸，得到人脸位置。基于随机子图表示的人脸图像隐秘检测(简称 RS 算法)见算法 2，示意图如图 2 所示。本文中的基于随机子图表示的人脸图像隐秘检测算法的描述以一个强分类器为例。

算法 2：RS 算法

输入：

①Alice 输入图像 $X(s$ 行，t 列)

② Bob 具有以下形式的强分类器: $H(x)=sign(\sum_{n=1}^{N}h_n(x))$

其中: $h_j(x)=\begin{cases}0 & \text{if } p_j f_j(x)<p_j\theta_j\\ 1 & \text{otherwise}\end{cases}$

输出：

①Alice 只知道 $H(x)$的检测结果，不知道 $H(x)$的任何参数

②Bob 只知道 $H(x)$的检测结果，不知道图像 X 的任何信息

1、Alice 利用上述子图的生成算法将原始图像 X 划分为 2 值的子图像加权和；

2、Alice 将权值集合 $Q\{0,1,2,...,255\}$ 随机重新排列得到集合 Q'，并将子图像 SM 按 Q'集合的顺序重新排列得到 SM_r'，把重新排列子图像 SM_r' 发送给 Bob；

3、Bob 根据子图像 SM_r' 的大小，计算出 M 个检测窗口。

4、对于 m=1,2,…,M 个检测窗口，Alice 和 Bob 进行以下子步骤：

(1) 对于每一个检测窗口，256 幅子图要通过 n=1,2,…,N 个弱分类器进行检测，Alice 和 Bob 进行以下子步骤：

(a) 对于每一幅子图像 SM_r'，其向量表示为 $\boldsymbol{sm_r}$。每一个弱分类器的特征权值向量为 $\boldsymbol{y_n}$，Bob 生成 n 个随机数 $b_1,b_2,\ldots,b_N$，全为正值。Bob 计算当前窗口下的每一个弱分类器 $\boldsymbol{y_n}$ 的特征值 $F_r(n)=sm_r^T * y_n * b_n$，将 256 幅子图的特征值 $F_r(n)$ 发送给 Alice；

(b) Alice 生成随机数向量 $a_k,(k=1,2,...,10)$，并随机选取第 i 项将其置为 1，Alice 收到子图的特征值 $F_r(n)$后，计算弱分类器通过原始图像 X 特征值 $F_{r,k}(n)=\sum_{r=0}^{255}F_r(n)*Q'(r)*a_k$；

(c) Alice 将 $F_{r,k}(n)$发送给 Bob，Bob 比较 $F_{r,k}(n)$

和弱分类器的阈值 $b_n*\theta_n$ 的大小，$F_{r,k}(n)>b_n*\theta_n$ 则保存为 1，否则为 0。得到一个 0，1 向量 $\boldsymbol{c_k}$。

(d) Bob 将 $\boldsymbol{c_k}$ 发送给 Alice，Alice 将第 i 项的值返回给 Bob，若 Bob 接收的返回值为 1，则存储为 α_n，否则 Bob 存储 β_n，Bob 将最后结果存储在 S_n。

(2) Bob 比较 S_n 和强分类器的阈值 stage_threshold 的大小，若 $S_n >$ stage_threshold，则该检测窗口被认为是正值，否则该检测窗口为负值。若检测窗口为正值则记录检测窗口的位置。

5、把所有正的检测窗口的位置返回给 Alice，得到所有人脸的位置。

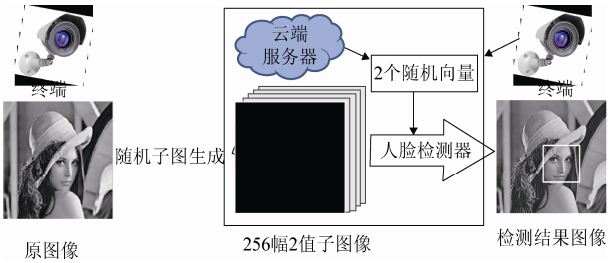


图 2 基于随机子图表示的人脸图像隐秘检测示意图

该算法双方是安全的，从以下两个方面分析：

—从 Alice 到 Bob：

步骤 2 中，Alice 将 255 幅随机重拍的子图发给 Bob，Bob 只知道子图像 SM'_r，不知道每张子图的权值 Q'，完全猜到图像信息的概率是 1/255!，Bob 很难恢复原图像。

步骤 4(1)中(b)、(c)、(d)3 个连续的步骤中，Alice 将 $F_{r,k}(n)$ 发送给 Bob，因为引入了 10 个随机数，Bob 得到 10 个不同的 $F_{r,k}(n)$ 与阈值进行比较得到 c_k 发回给 Alice，Alice 将对应第 i 项的 0 或 1 值给 Bob，因此 Bob 能猜到正确的 $F_{r,k}(n)$ 值的概率取决于 c_k 中 0 或者 1 的个数，设 q_i 为 c_k 中第 i 项值对应 0 或 1 的个数，则 Bob 能正确猜出 $Q'(r)$ 的概率为 $(1/q_i)^{C_N^{255}}$。所以 Bob 很难恢复原图像。

—从 Alice 到 Bob：

对于所有的步骤，因为对于特征值 y_n 和阈值 θ_n 始终带有随机数 b_n，Alice 不能获得关于特征值 y_n 和阈值 θ_n 的任何信息。

算法复杂度：

该协议的复杂度为该协议的复杂度是 $O(MNLK)$，其中 M 是子图像的个数，N 是弱分类器的个数，L 是测试图像向量的 X 的维数，K 为随机数的 a_k 的个数。

3 实验结果

本文把 Viola&Jones 人脸检测器改成隐秘的人脸检测器。在这个过程中仍然可以利用积分图，但需要计算 256 幅子图像的积分图，计算 256 幅子图像的特征值。该 Viola&Jones 人脸检测器包含了 22 级的强分类器的级联，其中每一个强分类器可以被表示为公式(1)的强分类器，允许每一个级联后作出判断，这样可以缩短检测时间。实验环境为 64 位 Windows7 操作系统，内存为 8G，处理器为 3.5 GHz AMD A10 Pro-7800 R7，12compute Cores 4C+8G。VS2012+OpenCV2.4.3 +OpenSSL-1.0.1c 平台。

1、检测准确率实验

检测准确率实验使用 OpenCV 自带的 haarcascade_frontalface_alt.xml 文件用来加载分类器，图像测试集是 LFW 和 CMU 人脸图库的 100 幅图片。检测图像为 100*100，共有 104 张人脸，正确检测出 92 个人脸，检测准确率为 88.46%，漏检人脸 12 个，漏检率为 11.54%，

基于随机子图表示的人脸安全检测算法检测结果如下表 1 所示，可以看出 RS 算法和 V&J 算法人脸检测正确率相同。这说明 RS 算法在理论和实验上都不会影响人脸检测的正确率。

表 1 算法检测结果

检测算法	人脸数/个	准确检测/个	漏检数	准确率/%	漏检率
V&J	104	92	12	88.46	11.54
RS	104	92	12	88.46	11.54

2、检测时间实验

检测时间实验使用 OpenCV 自带的 haarcascade_frontalface_alt.xml 文件用来加载分类器，图像测试集是 LFW 和 CMU 人脸图库的 80 幅

图片，大小为 90*90、100*100、110*110、120*120、144*144、196*196、260*196、300*300 的图像各 10 幅，共 80 幅图像。测试这 80 幅图的检测时间，分别求出每种图像大小的 10 幅图检测时间的平均值，得到 8 种不同大小的检测时间。从表 2 可以看出，随着图像的增大，随机子图的生成时间和 RS 算法的检测时间也在增大。这说明随机子图的生成和基于随机子图表示的人脸图像隐秘检测算法的计算量和图像大小有直接关系。

表 2 检测时间

图像大小	运行时间	
	随机子图像的生成时间/s	RS 算法检测时间/s
90*90	0.392	80.324
100*100	0.432	146.193
110*110	0.451	187.612
120*120	0.468	247.324
144*144	0.496	375.081
196*196	0.535	931.803
260*196	0.611	1 271.071
300*300	0.698	2 788.582

3、3 种人脸检测算法时间比较实验

本实验使用 OpenCV 自带的 haarcascade_frontalface_alt.xml 文件用来加载分类器，图像测试集是 LFW 和 CMU 人脸图库的 50 幅大小为 100*100 的图。分别测试 Viola&Jones 人脸检测算法(简称 VJ 算法)、基于不经意传输的人脸安全检测算法(简称 OT 算法)、基于随机子图表示的人脸安全检测算法(简称 RS 算法)检测 50 幅的程序运行时间，并分别求其平均值。从表 3 可以看出 RS 算法的优势。与 OT 算法相比，RS 算法处理速度更快，在保证终端和服务器双方的隐私数据安全性的情况下，RS 算法将运行时间大大缩短。RS 算法是一个高效安全的算法。

表 3 各个算法时间对比

测算算法	VJ	RS	OT
检测时间/s	0.38	147.135	几个小时

4 结论

本文通过将随机子图算法应用于 Viola&Jones 人脸检测算法，使云端人脸图像隐秘检测得以实现。通过对其安全性、复杂度、效率和实验结果的分析，该算法具有简单灵活、实用性强、性能较高等优点。该算法较《Blind Vision》的人脸图像隐秘检测算法检测速率已经有了质的提升，但还是不能达到实时检测。我们打算继续研究随机子图算法，并将其应用到其他的人脸检测模型。开发新的方法，使隐秘的人脸检测更快速。

参考文献:

[1] Paul Viola, Jones M J. Robust Real-Time Face Detection [J]. International Journal of Computer Vision, (S0920-5691), 2004, 57(2): 137-154.

[2] Tassa T. Generalized oblivious transfer by secret sharing [J]. Designs Codes & Cryptography (S0925-1022), 2011, 58(1): 11-21.

[3] Wang T. A review of the Study of Secure Multi-party Computation [J]. Information Security & Technology (S1674-9456), 2014 (5): 41-44.

[4] Avidan S, Butman M. Blind Vision [C]// Proc. of the 9th European Conf. on Computer Vision. Germany: Springer Berlin Heidelberg, 2006: 1-13.

[5] Shai Avidan, Moshe Butman. Efficient Methods for Privacy Preserving Face Detection[C]// Proceedings of the Twentieth Annual Conference on Neural Information Processing Systems. Vancouver, British Columbia, Canada, Publisher: MIT Press, 2006: 57-64.

[6] 张文科, 杨勇, 杨宇. 安全多方计算研究 [J]. 信息安全与通信保密, 2014 (1): 97-99. DOI:10.3969/j.issn. 1009-8054.2014.01.027.

[7] Yuta Nakashima, Noboru Babaguchi, Fan J. Intended human object detection for automatically protecting privacy in mobile video surveillance [J]. Multimedia Systems (S0942-4962), 2012, 18(2): 157-173. DOI: 10.1007/ s00530-011-0244-y.