目录

在人脸数据库上应用 PCA

1 问题描述

给定了 face 文件夹，其中有 train 和 test 两个文件夹。利用 train 中的人脸数据训练主成分分量，并完成以下练习。

(a) 从 train 文件夹里随意取出一张图片向量 x，将 x 投影到前 K 个主成分中，然后利用这些投影分量来重建人脸 x'，并计算重建误差 $\left\|x'-x\right\|^2$。从 $K=1$ 开始，不断的增加 K。给出重建误差随 K 的增长的收敛曲线。重建误差能否为 0?

(b) 从 test 文件夹里读取文件名 face.jpg 的文件，按照(a)的方式来做。与(a)相比，对于相同的误差阈值，是否需要更大的 K？重建误差能否为 0?

(c) 从 test 文件夹里读取文件名 nonface.jpg 的文件，按照(a)的方式来做。与(b)相比，对于相同的误差阈值，是否需要更大的 K？重建误差能否为 0?

2 算法说明

本次实验主要是利用 PCA 降维提取特征脸，即将人脸投影到特征脸空间。其操作流程如下：

2.1 特征脸构建

1) 将每幅训练图像重排为一列向量 $x_i \in \mathbb{R}^N \quad (i=1,2,\ldots,M)$

2) 计算训练数据的均值，将数据矩阵去中心化

$$\mu = \frac{1}{M}\sum_{i=1}^{M} x_i \tag{1}$$

$$A = \begin{bmatrix} x_1-\mu & x_2-\mu & \cdots & x_M-\mu \end{bmatrix} \tag{2}$$

3) 获取训练数据的协方差阵

$$C = \frac{1}{M-1}AA^T \in \mathbb{R}^{N\times N} \tag{3}$$

4) 对协方差阵 C 进行特征分解，设 C 的特征值分别是 $\lambda_1 \ge \lambda_2 \ge \cdots \ge \lambda_N$，相应的特征向量是 $\xi_1,\xi_2,\cdots,\xi_N$，这 N 个特征向量即为特征脸，它们构成了特征空间的正交基。

2.2 投影与重建

5) 根据(4)式确定要选取的特征值的个数 K（本次实验是探究重建误差与 K 的关系，因此不需要此步操作）

$$\begin{aligned} &\min K \in [1,N] \\ &s.t.\ \frac{\sum_{i=1}^{K}\lambda_i}{\sum_{i=1}^{N}\lambda_i} \ge threshold \end{aligned} \tag{4}$$

6) 根据 K 值，得到投影矩阵

$$P = \begin{bmatrix} \xi_1 & \xi_2 & \cdots & \xi_K \end{bmatrix} \in \mathbb{R}^{N\times K} \tag{5}$$

7) 设 x 是输入图像，将其投影到特征空间，得到图像在特征空间的坐标 y

$$y = P^T\left(x - \bar{x}\right) \in \mathbb{R}^K \tag{6}$$

8) 利用特征脸空间的投影向量对图像进行重构，得到重构图像 x'

$$x' = \bar{x} + Py \tag{7}$$

9) 考察重建误差 $\|x' - x\|^2$

3 结果分析

题中 3 幅不同图片的重建误差随着 K 的变化趋势如图 1 和图 2 所示。其中，图 1 是自然刻度显示，图 2 是将 y 轴取对数后显示，这样方便我们观测 $K \to N$ 时的重建误差。

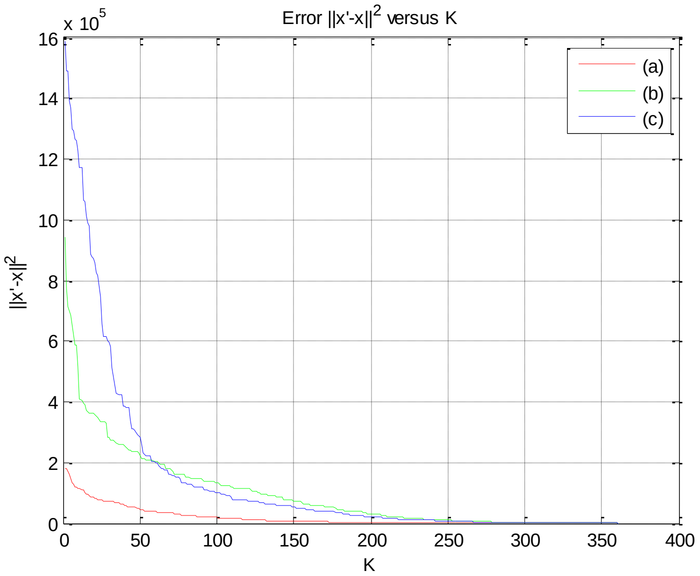

图 1 重建误差随 K 的变化曲线（自然刻度）

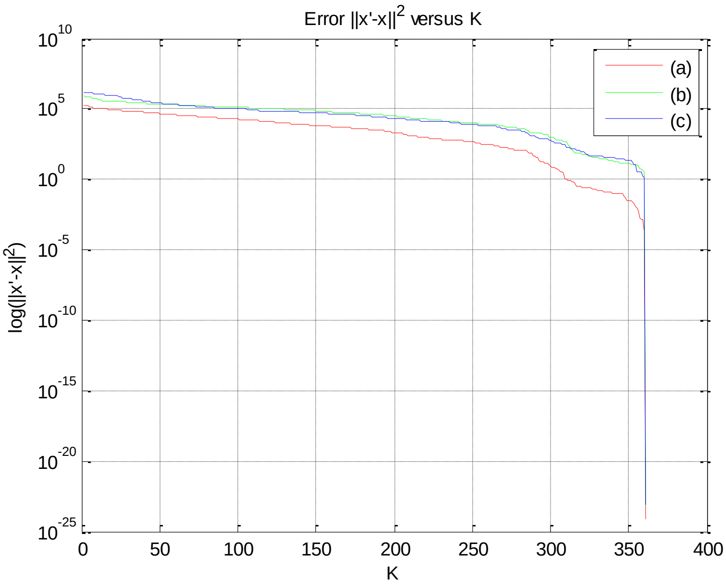

图 2 重建误差随 K 的变化曲线（semilogy）

据此，我们可以对原问题做出如下回答。

3.1 问题回答

(a) 重建误差可以为 0。

(b) 与(a)相比，对于相同的误差阈值，需要更大的 K。重建误差可以为 0。

(c) 与(b)相比，对于相同的误差阈值，需要更大的 K（当 K 值不过大时）。重建误差可以为 0。

3.2 结果分析

对上述结果的分析如下。

3.2.1 曲线变化趋势

无论哪幅图片，随着特征数量 K 的增多，重建误差都逐渐降低，这是因为我们引入了更多的特征维度。尽管被加入的维度对原图的贡献越来越小，但只要其不为 0，我们的重建误差总是逐渐降低的。实际上，协方差矩阵 C 是半正定矩阵，因而其特征值满足 $\lambda_i \geq 0$，即每个维度的加入，总是使得重建越来越好。

3.2.2 相同的误差阈值所需的 K 值

直接从训练图像中选取的人脸图像与训练出的特征脸相似性是最大的，因此其特征值最大的几个特征脸即可对图像进行很好的重建，这在图中变现为(a)曲线始终在最下方，且随着 K 值增加迅速降低。

对于 test 集中的人脸照片，尽管其不是训练特征脸的来源，但由于仍是人脸照片，因此它向特征脸空间投影时，大多数能量仍集中在少数的几个主成分里。所以，随着 K 值增加，其重建误差也迅速降低。但由于毕竟不是训练集中的照片，其重建误差在 K 值较小时仍大于(a)曲线对应的误差，因此，在相同误差阈值条件下，往往需要更大的 K。

对于非人脸图片，由于其与训练集图片特征的差别最大，因此，当 K 值不是很大时其重建误差总是最大的。相比于(b)，在相同误差阈值条件下，往往需要更大的 K。但注意到，当 K 值进一步增大时，(c)的重建误差有可能反而低于(b)的重建误差。我认为这个结果不具有一般意义，因为当 K 值趋近 N 时，重建误差是趋于 0 的。如果不是取自于训练集里的图片，在特征值极小的维度上，其大小往往是不定的。

3.2.3 重建误差可以为 0

无论图像是否人脸，只要当 $K=N$，即我们用所有的特征进行重建，那么重建误差是等于 0 的。根据线性代数的知识，当 $K=N$ 时，向量组 $\begin{bmatrix}\xi_1 & \xi_2 & \cdots & \xi_N\end{bmatrix}$ 构成了特征脸空间中的完备正交基。根据帕塞瓦尔定理，一个信号所含有的能量（功率）恒等于此信号在完备正交函数集中各分量能量（功率）之和。因此，只要用所有的特征维度对图像进行重构，我们是可以保证无误差重建的。

3.2.4 对人脸识别的启示

从图 1 可以看出，当重建特征数 K 较小时，人脸图像和非人脸图像的重建误差是有明显区分的。因此，我们可以设定一个合适的 K 值（比如本实验中取 20-30 比较合适），再设定一个与 K 相配合的能量阈值，如果对前 K 个维度的重建能够达到能量阈值，我们可以判定测试图像是一张人脸。注意到，K 的取值不能过大，否则人脸与非人脸的重建误差没有明显区分，甚至有时还会带来误判。