

Report#2

采用DNNL完成卷积层：

Batch Size: 512

Method	Time
DNNL	0.367s
OpenMP	0.499s
Single Thread	0.412s

DNNL表现最好（可能内部优化了并行计算），考虑要不要所有的层都写一个DNNL的版本，但工作量很大，并且自己写的优化一下可能会达到同样的效果。

多线程效果不如单线程的原因肯能有：

- 线程的创建与切换之类的时间开销大于多线程计算的时间开销
- 线程数量没有动态调整，当我设置为CPU核心数的一半时速度快一点。

正在完成加密协议的设计。

目前测试数据是CSV格式的图片，加密方式有两种：

1. 流加密
2. 分组加密

流加密 会泄露图片的大小信息，以及如果一个某个值占绝大多数（比如0，MNIST四周都是黑色），加密后的数据也是某个值占绝大多数。但是流加密的速度快，而且可以很轻松的实现随机读取。

分组加密 对csv加密时，对整个csv执行一次加密是最快的，但是想要实现读取一个Batch时随机读取，就要实现某种方法，可以随机选择部分密文加解密（这一点我还没看，不知道现行的加密方式是否支持）。