Hi 我有跑一些東西,主要做法是如果總共有 T步,我再從 x_T 還原到 x_0 的過程裡比較用 多少比例的攻擊 過的照片做condition 的效果各是如何。檔名裡面的小數點"0.4" or "0.5" 等等 代表 "靠近 x_0 的多少 percent 是用乾淨的image 做 condition",所以 如果總共有100步 0.4 代表 x_9 9~ x_4 0 是用被攻擊過(圖一)的照片當 x_0 0 是用乾淨(圖二)的圖片當 x_0 0 是用乾淨(圖二)的圖片當







下面是結果。但不make sense ,現在的結果是說用越多乾淨的圖片 (小數點越大) 和原圖的distance 就會越遠,我覺得蠻怪的,我再檢查一下我的code。但目前確定(圖三)是連臉都找不到所以有騙過,我再來的work 應該是會在這兩個之間找個平衡。另外一個發現是畫質越低的同樣的比例(小數點一樣的情況下)攻擊會越有效

lmg	Distance	Detect as Same person?
img1_attacked-0.0.jpg (圖一)	0.00051x	Yes
img1_attacked-0.4.jpg	0.00039x	Yes
img1_attacked-0.5.jpg	0.00075x	Yes
img1_attacked-0.6.jpg	0.00094x	Yes
img1_attacked-0.8.jpg	0.00095x	Yes
img1_attacked-0.9.jpg	0.0018x	Yes







img1_attacked-0.4.jpg

img1_attacked-0.6.jpg

img1_attacked-0.9.jpg