A universal heuristic attack on double random phase encryption

Lingfei Zhang
(Supervisor: Thomas Naughton)

ABSTRACT-

Optical encryption has potential is cases where visual information needs to be secured and authenticated, and where minor defects in the visible information is tolerable, but where the volumes of information are too great for conventional encryption technologies. This seminar starts with a quick review of optical encryption that indicates the advantages of optical encryption compared with conventional cryptography. Then I introduce a widely cited previously published attack (a simulated annealing heuristic algorithm) on a most common encryption method called double random phase encoding (DRPE). This heuristic algorithm has been shown to successfully find the approximate decryption keys with which to decrypt cipher images with adequate visibility, but the keys obtained perform unsatisfactorily to decrypt other subsequent images encrypted with the original keys. I have proposed a robust modification to the fitness function of the heuristic that strengthens the algorithm for all use cases. I will outline the technique and tests to verify its performance and wide applicability.