A novel attack on the Fourier plane encryption algorithm

Lingfei Zhang
Supervisor: Thomas Naughton

Computer Science Department
National University of Ireland Maynooth

Abstract: In this paper, a novel attack on double random phase encoding (DRPE) is proposed, that finds the symmetric encryption keys to decrypt a known plaintext-ciphertext pair. Since the image-based encryption keys are so large in optical encryption, it is common for keys to be reused for different messages. We propose a greedy strategy that optimizes the phase of each pixel of the Fourier domain mask individually to find the lowest decryption error. We show that the approach is significantly more efficient that previously published heuristic approaches. We justify why this counter-intuitive approach works with only a single pass through the sequence of pixels in the key. We present a technique to significantly speed up the search for the approximately optimal phase value of each pixel (from linear search to approximately logarithmic search) through utilising the cyclic response of pixels in encryption key phase masks.

Key word: known-plaintext attack, double random phase encoding (DRPE)