Linear growth of key-space based attack on Fourier plane encryption algorithm

Lingfei Zhang
Supervisor: Thomas Naughton

Maynooth University Department of Computer Science,
Maynooth, Co. Kildare, Ireland

Abstract-
In recent years, several attack algorithms have been proposed against the security of the double random phase encoding (DRPE) system. Because the unique feature of optical image encryption is that an approximate key can be sufficient, heuristic algorithms have been employed to successfully obtain approximate keys with relatively low decryption errors. These attacks were based on the known-plaintext attack in which an attacker can use a single arbitrary pair of plaintext and ciphertext to infer the decryption key. However, the time cost of previous algorithms remains considerably high when the size of plaintext is greater than 128×128 pixels [1-5], because the algorithms are considered subject to the size of the key-space. Also, secure models of encryption [6] can be used to protect against known-plaintext attacks. In this talk, the exponential growth of the key-space with multiple perfect keys in the system will be explained. Then, we propose to convert the growth of the key-space to linear by transforming the multiple perfect keys to one. This admits a greedy algorithm that individually optimises each pixel of the decryption key to estimate the optimal phase-value, which would be infeasible in an exponential key-space situation. Because of the linear key-space, the new algorithm is shown to be more capable of dealing with large inputs (over 128×128 pixels) than any previous algorithms. Moreoever, the decryption error and time cost of the algorithm is predictable. It can be applied to all cases of optical image encryption.

[1] U. Gopinathan, D. S. Monaghan, T. J. Naughton, and J.T. Sheridan, “A known-plaintext heuristic attack on the Fourier plane encryption algorithm,” Opt. Express 14, 3181-3186 (2006).
[2] W. Liu, G. Yang, and H. Xie, “A hybrid heuristic algorithm to improve known-plaintext attack on fourier plane encryption,” Opt. Express 17, 13928–13938 (2009).
[3] X.Peng, P.Zhang, H.Wei, and B.Yu, “Known-plaintext attack on optical encryption based on double random phase keys,” Opt. Lett. 31, 1044-1046, (2006).
[4] X. Peng, H. Wei, and P. Zhang, “Chosen-plaintext attack on lensless double-random phase encoding in the Fresnel domain,” Opt. Lett. 31, 3261-3263 (2006).
[5] Y. Frauel, A. Castro, T. J. Naughton, and B. Javidi, “Resistance of the double random phase encryption against various attacks,” Opt. Express 15, 10253-10265 (2007).
[6] T. J. Naughton, B. M. Hennelly, and T. Dowling, “Introducing secure modes of operation for optical encryption, ”J. Opt. Soc. Amer. A, vol. 25, pp. 2608–261, 2008