Strengths and weaknesses of optical encryption algorithms

Unnikrishnan Gopinathan,[a] David S. Monaghan,[a] Thomas J. Naughton,[b] John T. Sheridan,[a] Bahram Javidi[c]

[a] *Dept. of Electronic and Electrical Engineering, University College Dublin, Belfield, Dublin 4, Ireland*
[b] *Dept. of Computer Science, National University of Ireland Maynooth, County Kildare, Ireland*
[c] *Electrical & Computer Engineering Dept., University of Connecticut, Storrs, CT 06269, USA*

Introduction

Many image encryption algorithms have been proposed over recent years Refs. 1-8, to cite a few. Many of these algorithms can be implemented using optical techniques taking advantage of both the natural two dimensional (2D) imaging capabilities of optics and the parallelisms achievable with optical processing. Optical systems are also capable of encrypting real world 3D objects [9]. The output of an encryption system is complex valued. Digital holographic techniques have been used to record high quality approximations of both the amplitude and phase of complex valued wavefronts output by the optical encryption systems [9,10]. Digital compression techniques have been used to enable efficient storage and transmission of encrypted holographic data over digital communication channels [11,12].

Though many optical encryption techniques have been proposed in the recent years, a systematic analysis of the strengths and weaknesses of these algorithms has not been undertaken yet, to the best of our knowledge. Optical encryption algorithms with all their advantages mentioned above, are yet to undergo rigorous cryptanalysis which many conventional cryptographic algorithms are subjected to. There are instances in the literature when an encryption mechanism is shown to be robust to blind decryption for a limited number of keys in the key space. But this is not sufficient to evaluate the strength of an encryption algorithm. This work attempts to systematically study the strengths of some of the well known image encryption algorithms.

Cryptanalysis of image encryption algorithms

We perform a known-plaintext cryptanalysis on a well-known optical encryption algorithm – the Fourier plane encoding algorithm [2]. This algorithm encodes an image to a stationary white noise by using two statistically independent random phase codes in the input plane and Fourier plane. The image is multiplied by a random phase code. A Fourier transform is performed on this product and multiplied by the second random phase code. A second Fourier transform gives the encrypted image. In known-plaintext cryptanalysis, it is assumed that the attacker is assumed to know the encryption mechanism. The attacker has also access to a pair of plaintext and ciphertext. If the attacker is able to find the key used for a given plaintext-ciphertext pair, then all the security of all the past and future ciphertext which used the same key is compromised. In our analysis, we consider two factors – the error in the decrypted image with a partially-correct encryption key, and the time required to find that key. In many instances, a partial decryption with a certain amount of error may be more desirable than a perfect decryption which would take a greater amount of time. This is especially true in the case of image encryption. We further consider cases where the attacker has a partial knowledge of the plaintext corresponding to a given ciphertext and analyze the security of the algorithm.

Experiments

We did some preliminary experiments to analyze the strength of the Fourier plane encoding algorithm. We used a well known nonlinear optimization algorithm – Simulated Annealing (SA). We chose a 32×32 image shown in Fig. 1(a) as the plaintext and encrypted it using two random phase codes. If the image is real-valued, one needs only the random phase code used in the Fourier plane to decrypt the image. The algorithm starts with an initial guess of the Fourier plane random phase and searches over a key space to

minimize a cost function which is the normalized RMS error between the decrypted image for a given key and the original image. The plot of the time taken to find the key for different errors between the decrypted image and original image is shown in Fig. 1(e). The decrypted image with a normalized RMS error of 0.1 is shown in Fig. 1(b). Fig. 1(d) shows the decrypted image obtained from an image [Fig. 1(c)] encrypted using the same set of keys used for Fig. 1(a).

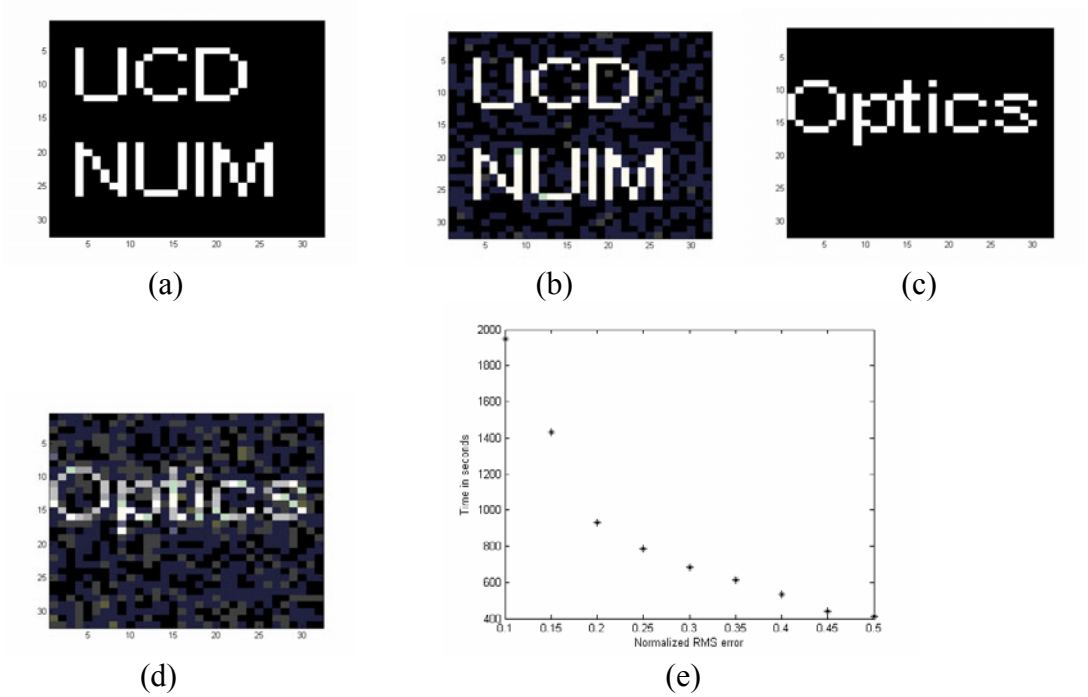

Fig. 1(a) Original image used to find the key and (b) the decrypted image with an RMS error of 0.1 with the keys obtained using SA (c) a different image encrypted using the same set of keys (d) decrypted image using the key used in the previous case (e) plot showing time to find encryption key for different errors.

References

1. B. Javidi and J. L. Horner, "Optical pattern recognition for validation and security verification," Opt. Eng. **33**, 1752–1756, 1994.
2. Ph. Réfrégier and B. Javidi, "Optical image encryption based on input plane and Fourier plane random encoding", Opt. Lett., Vol. **20**, 767-769, 1995.
3. L. G. Neto and Y. Sheng, "Optical implementation of image encryption using random phase encoding," Opt. Eng. **35**, 2459–2463, 1996.
4. O. Matoba and B. Javidi, "Encrypted optical memory system using three-dimensional keys in the Fresnel domain," Opt. Lett. **24**, 762–764, 1999.
5. P. C. Mogensen and J. Glückstad, "Phase-only optical encryption," Opt. Lett. **25**, 566–568, 2000.
6. G. Unnikrishnan, J. Joseph and K. Singh, "Optical encryption by double-random phase encoding in the fractional Fourier domain", Opt. Lett., Vol. **25**, 887-889, 2000.
7. B. M. Hennelly and J. T. Sheridan, "Optical image encryption by random shifting in fractional Fourier domains" Opt. Lett., Vol. **28**, 269-271, 2003.
8. B. M. Hennelly, J. T. Sheridan, "Random Phase and Jigsaw Encryption in the Fresnel Domain", Opt. Eng., Vol. **43**, 2233-2238, 2004.
9. E. Tajahuerce, B. Javidi, "Encrypting three-dimensional information with digital holography", Appl. Opt., **39** 6595-6601, 2000.
10. B. Javidi, T. Nomura, "Securing information by use of digital holography ", Opt. Lett. **25**, 28-30, 2000.
11. T. J. Naughton, Y. Frauel, B. Javidi, E. Tajahuerce, "Compression of Digital Holograms for Three-Dimensional Object Reconstruction and Recognition" Appl. Opt., Vol. **41**, 4124-4132, 2002.
12. T. J. Naughton, B. Javidi, "Compression of encrypted three-dimensional objects using digital holography," Opt. Eng., Vol. 43, 2233-2238, 2004.