New methods for spatial modulation applied in optical data encryption

PhD Theses

Sarkadi Tamás

Supervisor: Dr Koppa Pál

Budapest University of Technology
Department of Atomic Physics
Budapest
2014

Previous researches

Information technologies demand devices with huge data processing and storage capacity. The increasing amount of data enhances the significance of information security systems. Optical techniques are widely used for data transfer and storage, thus optics can serve to encrypt data. Hardware based optical encryption gives an opportunity to improve the security level related to the conventional software based encryption methods. My thesis covers a special area of the optical cryptography, Fourier optical encryption systems [1] applied in page organized holographic data storages.
In this storage the data is organized in a 2D structure called data page. This page modulates a coherent wave front by spatial light modulator. The wave front is Fourier transformed, and recorded in a hologram. The advantage of the page organized system is that huge amount of data can be read in parallel by one hologram reconstruction. Not only efficient data access, but fast data processing is provided. Many important applications can be realized like content addressable memories and information security systems.
The encryption applied in page organized systems uses the principle of the optical Fourier transformation to delocalize the information content of the spatially modulated wave front. In these cryptosystems the Fourier transformed data page is modulated by a random phase mask. The original wave front can be recovered only in case the random phase mask is known, thus the phase mask can be used as encryption key. Optical encryption and holographic storage are widely researched, several institutes and companies take part in their development and practical realizations.
In the Department of Atomic Physics of Budapest University of Technology holographic memories have been studied since 1998. One of the most significant results was that a read-write holographic memory card system was developed [2]. The next purpose was to combine the holographic storage and the Fourier optical encryption. Our research group used random phase modulated reference wave as encryption key at the hologram recording [3]. Studies were made to estimate the security level of the encryption system [4].

Objectives

When I joined to the project of the Department of Atomic Physics of BME, ny goal was to solve the substantial problems of holographic data encryption. I recognized that the security level of the Fourier optical encryption realized by random phase masks is limited. Thus my goal was to enhance the efficiency of the cryptosystem. I considered that the new cryptosystem to be developed must be robust and compatible to the earlier holographic data storage systems, and it must not be much more complicated than the conventional Fourier encryption techniques.
My further goal was to develop a statistical model to describe the Fourier optical cryptosystems, which is applicable for determining the security level of the encryption method.

Investigation methods

I applied both empirical methods and modeling techniques to study the Fourier optical cryptosystems. Model calculations were made in two differential ways. One of these models was based on computer simulation of wave propagation and the other used the principles of statistical optics to describe the random spatially modulated waves.

The computer model is well known from the literature [5]. In this case the wave fronts are sampled, thus the complex amplitude distributions are represented by an array. The wave propagation and the interaction with optical elements can be modeled by transformations effect on the arrays.
In Fourier optical cryptosystems the input wave fronts and the key phase masks have random spatial modulation. Thus the analysis of the system is complicated, because computer simulation has to be applied on huge amount of random data pages in order to estimate the statistical properties of the encryption. To solve this problem I developed the statistical optics model of the Fourier optical cryptosystem, where the complex amplitudes of the random spatial modulations are considered as random variables. In this way the intensity statistics of the output signal can be determined from the mean values and variances of complex amplitude distributions of the input wave and the random key mask. Thus the efficiency of data encryption can be characterized without analyzing wave front propagation.
After the modeling I demonstrated the efficiency of the Fourier optical cryptosystems experimentally too. I made measurements to validate the statistical optics model, and I determined the most important factors influencing the efficiency of the cryptosystem. On this basis I optimized these factors to enhance the security level of the Fourier optical cryptosystems.

References

1. Ph. Refrigier and B. Javidi, „Optical image encryption based on input plane and Fourier plane random encoding”, Optics Letters, **20,** 767-769 (1995)

2. E. Lőrincz, F. Ujhelyi, P. Koppa, A. Kerekes, G. Szarvas, G. Erdei, J. Fodor, Sz. Mike, A. Sütő, P. Várhegyi, P.S. Ramanujam, S. Hvilsted, "*Read/write demonstrator of rewritable holographic memory card system*", WA 0005, poster presentation at Optical Data Storage Topical Meeting, 14 - 17 April 2001 in Santa Fe, New Mexico, USA, in Optical Data Storage 2001. Proc. of SPIE, Vol. **4342**, 566-573 (2002)

3. F. Ujhelyi, M. Lovász, Z. Göröcs, A. Sütő, P. Koppa, G. Erdei, E. Lőrincz, *"Phase coded polarization holographic system demonstration"*, Holography 2005, International Conference on Holography, Varna, Bulgaria, 21-25 May 2005, Congress Center Frederic Joliot-Curie", Proc. of SPIE **6252** 209-213 (2006)

4. T. Ujvári, P. Koppa, M. Lovász, P. Várhegyi, Sz. Sajti, E. Lőrincz, P. Richter, „A secure data storage system based on phase-encoded thin polarization holograms,” Journal of Optics A, **6,** 401-411 (2004)

5. Várhegyi Péter, *Új modellek és eszközök a holografikus adattároló rendszerek kutatásában*, PhD értekezés, Budapesti Műszaki és Gazdaságtudományi Egyetem (2005)

Theses

1. I developed the statistical optics model of the Fourier optical cryptosystems, which is applicable to determine the bit error rate of the decrypted data as a function of difference between the encryption and decryption keys without the numerical modeling of the wave propagation. I showed that the orthogonality of key pairs depends not only on the difference between the keys, but on the error correction code applied to recover the decrypted data. The condition of orthogonality is that the probability of reconstruction of a page with wrong key is as small as the probability of failed reconstruction of the page with the right key due to the system noises. Using this orthogonality criterion the volume of the key space and the binary key length of the encryption can be evaluated. [S3,S6]

2. I proved by the statistical optics model of the Fourier optical cryptosystem and by experiments that the security level of Fourier optical cryptosystems can be enhanced by using of phase and amplitude modulated keys, related to the security level provided by the phase-only modulated keys. I showed that the binary key length of the cryptosystem can be maximized by optimally chosen contrast parameter and fill factor of the amplitude key at a given signal to noise ratio of the optical system. I proved that the key length of the Fourier optical cryptosystem can be arbitrarily enhanced by the reduction of noise in case the proposed phase-amplitude keys are used for encryption, in contrast with the conventional phase-only keys, which provides limited key length. [S3]

3. I proposed a data encoding method, to be used in Fourier optical cryptosystems, which is applicable to generate complex modulated input wave fronts. The corresponding pixel of the input image to be encoded is generated by the interference of two neighboring pixels of the complex input wave front. Using the statistical optics model of the cryptosystem I proved that the security level of the encryption can be enhanced in case the ratio of mean intensity of the complex modulated input wave front and the mean intensity of the encoded image is increased. I showed that the key length of the Fourier encryption can be monotonously grown by increasing of the signal to noise ratio of optical system when the proposed complex modulated input wave fronts are used. [S1,S4]

4. I proposed new spatial filters for spatial light modulator systems based on Fourier filtering. These filters are applicable to generate complex modulated wave fronts from appropriately chosen phase only modulated wave fronts. The transmittance distribution of the proposed filters can be determined by the ratio of the power spectral density functions of the complex wave front to be generated and the phase-only modulated input wave of the Fourier filtering system. I showed that difference between the ideal complex modulated wave front and the wave realized by using the proposed filter decreases in case the spatial frequency bandwidth is enhanced, in contrast with the systems known from the literature. [S2,S5]

Relevant publications in the respect of theses

S1 T. Sarkadi, P. Koppa, F. Ujhelyi, J. Reményi, G. Erdei, E. Lőrincz, „Holographic data storage using phase-only data pages," Proceedings of SPIE -Optical and Digital Image Processing, Strasbourg, 7000, paper: 700004, pp: 4-11 (2008)

S2 T. Sarkadi, P. Koppa, „Measurement of the Jones matrix of liquid crystal displays using a common path interferometer," Journal of Optics, 13, 035404 (2011)

S3 T. Sarkadi, P. Koppa, „Quantitative security evaluation of optical encryption using hybrid phase- and amplitude modulated keys," Applied Optics, 51, 745-750 (2012)

S4 T. Sarkadi, P. Koppa, „Optical encryption using pseudorandom complex spatial modulation," Applied Optics, 51, 8068-8073 (2012)

S5 T. Sarkadi, Á. Kettinger, P. Koppa, „Spatial filters for complex wavefront modulation," Applied Optics, 52, 5449-5454 (2013)

S6 T. Sarkadi, P. Koppa, „Improved data pages for an interference-based cryptosystem," Applied Optics, 53, 798-805 (2014)

Other publications

S7 T. Sarkadi, P. Koppa, „Fourier optical cryptosystem using complex spatial modulation," Physica Scripta, T162, 014051. (2014)

S8 Z. Göröcs, G. Erdei, T. Sarkadi, F. Ujhelyi, J. Remenyi, P. Koppa, E. Lorincz, „Hybrid multinary modulation using a phase modulating spatial light modulator and a low-pass spatial filter," Optics Letters, 32, 2336-2338 (2007)

S9 Z. Göröcs, G. Erdei, T. Sarkadi, F. Ujhelyi, J. Reményi, P. Koppa, E. Lőrincz, „Application of a phase-SLM and low-pass Fourier filtering to generate spatial patterns simultaneously modulated in phase and amplitude," International Quantum Electronics Conference, Munich, paper: 4386047, (2007)

S10 P. Koppa, T. Sarkadi, F. Ujhelyi, J. Remenyi, G. Erdei, E. Lorincz, „Optical encryption and encrypted holographic storage using phase-only data pages," Proceedings of SPIE, Optics and Photonics in Security and Defence Conferences, Optics and Photonics for Counter-Terrorism and Crime-Fighting. Florence, 6741, pp: 74101-74108, (2007)

S11 Z. Göröcs, T. Sarkadi, G. Erdei, P. Koppa, „Hologram positioning servo for phase-encoded holographic data storage systems," Applied Optics, 49, 611-618 (2010)