Investigation Image Encryption and Image Processing in Power Engineering Industry

Jun Li, Jiao Sheng Li, Yang Yang Pan & Rong Li

Guangdong Provincial Key Laboratory of Quantum Engineering and Quantum Materials, School of Physics and Telecommunication Engineering, South China Normal University, Guangzhou 510006, China

Abstract: A method for image encryption is proposed, which encodes original object image into the encrypted image and then embeds it into host image in our modified interferometer architecture. Several image encryption schemes based on chaotic maps have been proposed. Final encrypted object image is registered as interference patterns, thus the secure information is imperceptible to unauthorized receivers. The method can simultaneously realize image encryption and image hiding at a high speed in pure system. The results of an experiment in which we encrypted a plaintext image optically and then decrypted it numerically demonstrate that our proposed incoherent optical security system is feasible.

[Jun Li, Jiao Sheng Li, Yang Yang Pan & Rong Li. **Investigation Image Encryption and Image Processing in Power Engineering Industry.** *Nat Sci* 2016;14(10):119-123]. ISSN 1545-0740 (print); ISSN 2375-7167 (online). http://www.sciencepub.net/nature. 19. doi:10.7537/marsnsj141016.19.

Keywords: Image Encryption, Image Processing, Power Engineering Industry

1. Introduction

Encryption is the process of encoding messages or information in such a way that only authorized parties can read it. With the increased importance of information security, image security has become increasingly important in many current application areas. In an encryption scheme, the intended communication information or message, referred to as plaintext, is encrypted using an encryption algorithm. The study of image security includes image encryption, image hiding and image watermarking. Image encryption technology has been widely applied to many application areas, such as 3D image encryption, data monitoring, data tracking and confidential data transmission in the military and medical fields, quantum-secured imaging, and quantum-secured surveillance.

It is in principle possible to decrypt the message without possessing the key, but, for a well-designed encryption scheme, large computational resources and skill are required. An authorized recipient can easily decrypt the message with the key provided by the originator to recipients, but not to unauthorized interceptors. In recent years, image security that fully utilizes optical parallel features has become an important research topic; we also have demonstrated the feasibility of optical image hiding and optical image encryption and hiding. These methods may be effective solutions to the future implementation of all-optical systems.

Standards for cryptographic software and hardware to perform encryption are widely available, but successfully using encryption to ensure security may be a challenging problem. A single error in system design or execution can allow successful attacks. Sometimes an adversary can obtain unencrypted information without directly undoing the encryption. However, the large volume of data required for storing or transmitting holograms has been a main limiting factor of optical image security. Many hologram compression schemes have been reported in recent years to solve this problem; however, their effectiveness is limited by the introduction of hologram laser speckling, and the hologram compression is typically performed using electronic means. These signals are then reconstructed from these projections using a process. Simultaneously, CS is combined with other special imaging methods to obtain wider application, such as in quantum imaging, photon counting imaging, the coherent imaging of different wavelengths, and the measurement of electric fields. These features may also be effective solutions for the massive data processing and information security requirements of the Internet of Things (IoT).

The newly developed theory of compressive sensing (CS) provides a new technical approach for hologram compression in the optical domain and captures the non-adaptive linear projections of compressible signals at a rate that is significantly below the rate. Recently, various image encryption methods based on compressive sensing, such as parallel image encryption, image encryption with an Arnold transform and color image encryption, have been proposed. However, these methods relate to digital image encryption; completely optical schemes for image encryption based on compressive sensing have not been discussed. At the receiving terminal, the encrypted image reconstruction is achieved from small amounts of data by an optimization process, and the original image can be decrypted with three reconstructed holograms and the correct keys. The method can be used to perform compressive optical image encryption

in a purely optical system; therefore, it is effective and suitable for secure optical image transmission in future all-optical networks.

Encryption has long been used by military and governments to facilitate secret communication. It is now commonly used in protecting information within many kinds of civilian systems. For example, the Computer Security Institute reported that in 2013, 71% of companies surveyed utilized encryption for some of their data in transit, and 53% utilized encryption for some of their data in storage. This paper proposes a completely optical image encryption method based on compressive sensing. Using a Mach-Zehnder interferometer, an object image is first encrypted to a white-sense stationary noise pattern using a DRPE method in the object beam path. Then, the encrypted image is highly compressed to a signal utilizing the sparsity of the signal in a sparse domain. Moreover, our method utilizes the sparsity of a signal to reconstruct a complete signal from a small sample to overcome the limitation of the large hologram data volumes of 3D images or 3DTV. In addition, our method can overcome the limitations of the precision and costs of traditional sensors, wavelengths and resolution for array imaging based on CS. The principles and numerical simulations are described below.

Encryption, by itself, can protect the confidentiality of messages, but other techniques are still needed to protect the integrity and authenticity of a message; for example, verification of a message authentication code (MAC) or a digital signature.

Methods

Digital signature and encryption must be applied to the cipher text when it is created (typically on the same device used to compose the message) to avoid tampering; otherwise any node between the sender and the encryption agent could potentially tamper with it. Encrypting at the time of creation is only secure if the encryption device itself has not been tampered with.

The compressive optical image encryption system is shown in Fig. 1. A laser beam is split into an object beam and a reference beam. The object beam first illuminates an object image that is used for encryption and subsequently passes through two random phase masks P_1 and P_2 to perform the encryption using the DRPE method. Each tillable mirror-pixel can be rotated +11 or −11 degrees from the horizontal to reflect light to or away from an intended target. When the mirror-pixel is in the +12 degree state, more than 93% of the reflected energy can be coupled to the target. Then, the compressive sampling data are obtained by the photodiode detector with the modulation of the encrypted complex light field by the DMD device. Finally, we can acquire the compressed hologram image by a traditional communication channel and subsequently reconstruct it via the specific algorithm. In addition, the original object can be decrypted via an inverse Fresnel transformation with three reconstructed holograms and the correct keys. In the other arm, the reference beam illuminates the piezoelectric transducer mirror, which is capable of phase shifting. Then, the two waves overlap to form an interference pattern in the plane of a Digital Micro mirror Device. The DMD, a semiconductor-based "light switch" array of millions of individually addressable, tillable mirror-pixels, is a reflective spatial light modulator.

Then, we transmit the measurement data and measurement matrix using a conventional channel to the computer, where the image reconstruction and decryption will be performed. For the image signal, because the gradients of most images are sparse, Rudin *et al.* presented a nonlinear total variation (TV) algorithm, which attempts to deny images in an effective manner. Simultaneously, it can enforce a sparsity constraint and reconstruct images well under compressive sensing theory. The concept of constrained TV minimization, which attempts to minimize the gradients of images, originated from the field of compressive sensing in the work by Candes *et al*. the total variation in the image x: the sum of the magnitudes of the gradient. The image can be constructed by solving the convex optimization problem of minimizing the l_1-norm of the image subject to the constraint that the image's DFT matches the measured DFT values. We first adopt two-step iterative shrinkage (TwIST) algorithm to reconstruct the interference wave intensity $\hat{I}_k$ by solving the optimal problem under additive white Gaussian noise in the system.

The null space property (NSP) is a sufficient condition for l_1 convex minimization to obtain the sparsest solution. We are primarily concerned with how well CS can approximate a given signal from a given budget of fixed linear measurements compared to adaptive linear measurements. Therefore, the advantages of using total variation (TV) is that the TV can considerably reduce the under-sampling ratio as well as offer robustness to noise in the data due to the better null space property (NSP). In the traditional approach of using regularize, such as TV, there is a trade-off between data fidelity and image regularity. A group at Duke also developed a TV algorithm to reduce the noise of a compressed hologram and solve the linear inversion problems. In the present work, we are interested in image reconstruction in which the measurement is incomplete. Because of the incompleteness, there will be no unique minimizer of the data-fidelity-objective function, and TV is used to select a unique image out of the set of possible images that agree with the available data.

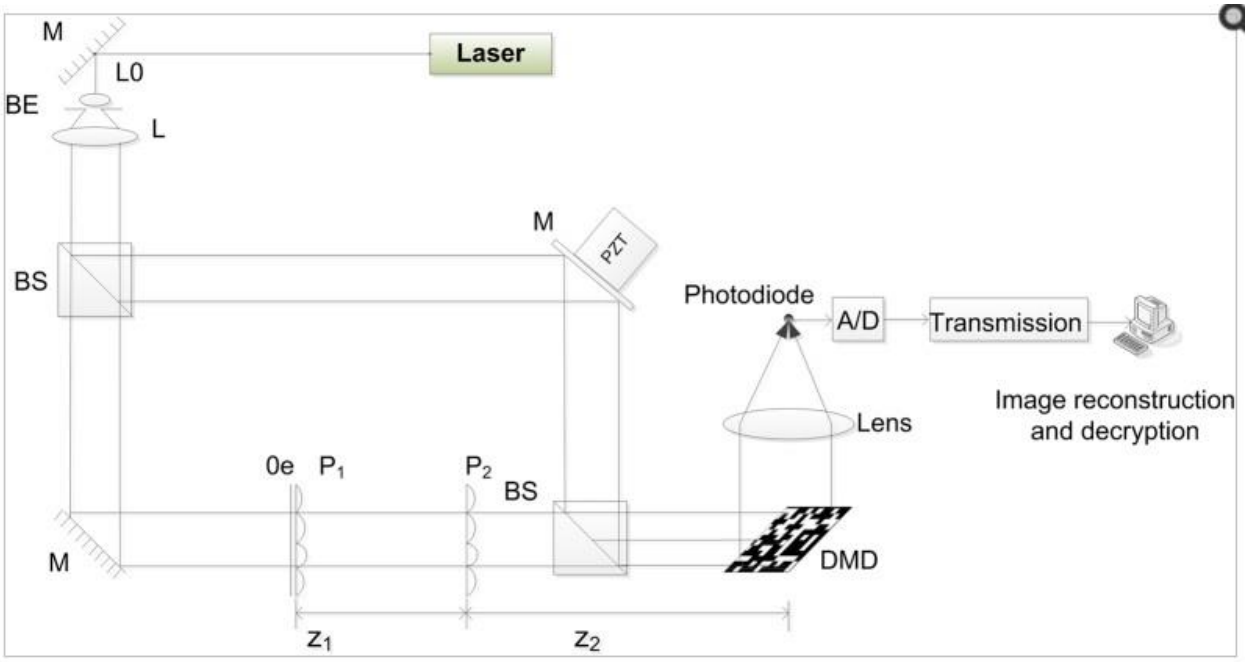

Fig 1. Setup of compressive optical image encryption. BE, beam expander; L, lens; BS, beam splitter; M, mirror; P, random phase plate; PZT, piezoelectric transducer mirror; Oe, object image.

Results

A series of simulations have been performed to verify the feasibility of our proposed method. This section presents a series of results based on the following conditions. The type of central processing unit (CPU) used in the computer simulation is an Intel(R) Core(TM) i7, and the memory of the computer is 6 GB. We used the MATLAB R2009a software package. The measurement matrix size of the DMD used in the computer simulation. The measurement matrix generated by the DMD is random sequences of 0.1. The original object images used in the simulation are shown, all with sizes. The intensity values of the complex amplitude field containing encrypted object information are first modulated by the DMD, and then, once we received the compressed data of the encrypted image in the photodiode detector, we can reconstruct the original image from the compressed and encrypted image using the correct keys and the optical system's parameters. The simulation results for the compressive optical image encryption in a Mach-Zehnder interferometer are shown. After performing compressive optical image encryption on the object images, the three encrypted interferograms containing the secret image information on the DMD plane will be sampled with compressive sensing theory; one of these interferograms is shown the recovered object images from measurements and measurements using our method. The computer simulations show that this compressive optical image encryption method is performed using a completely optical scheme in the Fresnel domain.

Moreover, we investigated the compression feature and the effects of the measurement noises in our method. The computer simulations are shown in Figs. 2. The relations of the sampling rate in the compressive sampling process and the peak signal-to-noise ratio (PSNR) between the original image and the reconstructions are shown in Fig. 2. In this simulation, the measurement noise described in Equation is additive white Gaussian noise with a zero mean and a standard deviation $\sigma = 0.3$. Figures 2 present the relations of the sampling rate in the compressive sampling process and the PSNR for a binary image and gray-level image. The PSNRs clearly increase with increases in the sampling rate. When the sampling rate reaches 26%, the PSNR values are close to or greater than 21 dB. When considering the effects of white Gaussian noise, the relations of the sampling rate and PSNR have the same tendency. It also illustrates the minimum number of measurements that enables a decent image retrieval under different measurement noise conditions. It show the relations of the number of measurements and the standard deviation σ of the additive white Gaussian noise when the PSNR is 18 dB for the binary image and the gray-level image. This shows that the proposed method is effective and exhibits a good performance with a white Gaussian noise in the fully optical domain.

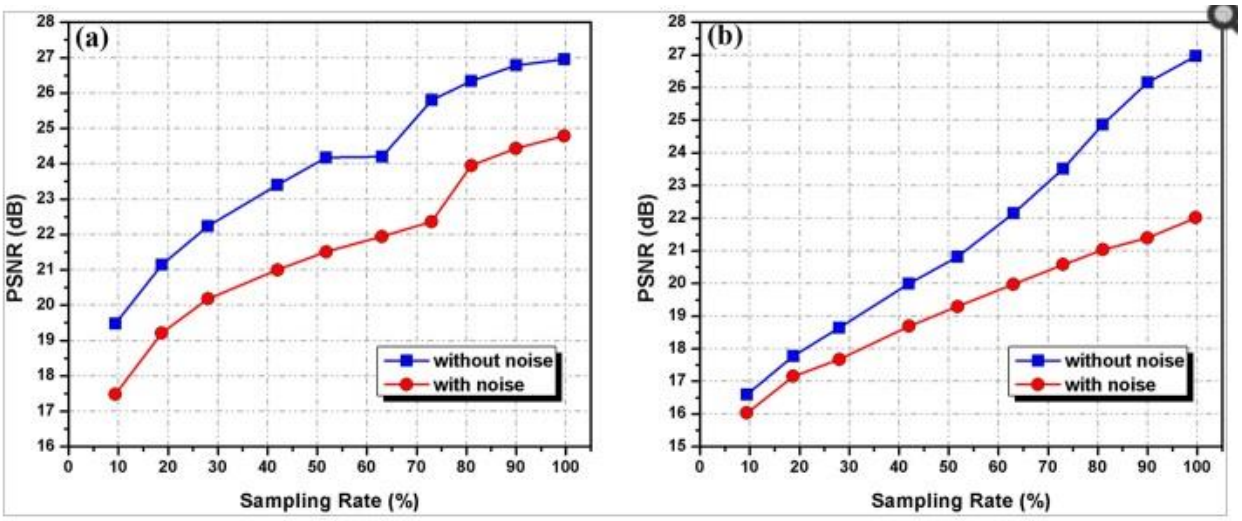

Fig. 2: Relations of the sampling rate and PSNR with measurement noise and without measurement noise. (**a**) Relations of the sampling rate and PSNR between the original binary image and reconstructed images; (**b**) Relations of the sampling rate and PSNR between the gray-level image and reconstructed images.

To further test the vulnerability of the proposed compressive encryption scheme, let us assume that a potential eavesdropper, who knows our reconstruction mechanism, has unauthorized access to a fraction $\Phi$of the key parameters and uses the corresponding measurement matrix to reconstruct the image. It a sequence of object images reconstructed from such a partially recovered key. The encrypted information begins to be retrieved when $\Phi$is as high as 15%, which means that the eavesdropper should capture at least 15% of the measurement matrix numbers.

With an optical image encryption technique and a compressive sensing technique, the method introduces an all-optical solution to sensing the original object, encrypting the object, and compressing the object in the analogue domain, which will present a superior scheme to overcome the limitations of the large holograms data volume for current optical image encryption systems. In addition, the DMD used in the setup of the compressive optical image encryption can perform high-speed measurements; therefore, it is expected to be widely used for 3D object encryption, video secure transmission, real-time video encryption technology and future all-optical networks, such as real-time video security transmission and naked-eye 3D Television. To ensure security against more sophisticated eavesdropping attacks, Alice and Bob might want to synchronously and randomly alter the order of the elements of the key for different objects. The mean square error (MSE) between the original image and reconstructions versus the sampling rate is shown. Clearly, the MSEs are observed to decrease with increases in the sampling rate. This proves that in addition to the keys above, the data of the measurement matrix are also one of the important keys. Therefore, the space of the key is expanded.

In this paper, an optical image encryption technique based on compressive sensing using fully optical means has been proposed. The simulations show that the method can be used to reconstruct the original image well with fewer measurements established by criterion and can be applied to gray-scale images and binary images to perform image encryption and compression in an all-optical system.

References

1. Tanha M., Kheradmand R. & Ahmadi-Kandjani S. Gray-scale and color optical encryption based on computational ghost imaging. Appl. Phys. Lett. 101, 101108 (2012).
2. Malik M., Magana-Loaiza O. S. & Boyd R. W. Quantum-secured imaging. Appl Phys Lett. 101, 241103 (2012).
3. Bishop C. A., Humble T. S., Bennink R. S. & Williams B. P. Quantum-Secured Surveillance Based on Mach-Zehnder Interferometry. arXiv preprint arXiv :1303.6701 (2013).
4. Clemente P., Durán V., Tajahuerce E. & Lancis J. Optical encryption based on computational ghost imaging. Opt. Lett. 35, 2391–2393 (2010).
5. Jun L., Tao Z., Qing-zhi L. & Rong L. Double-image encryption on joint transform correlator using two-step-only quadrature phase-shifting digital holography. Opt. Commun. 285, 1704–1709 (2012).
6. Jun L., Jiaosheng L., Yangyang P. & Rong L. Optical image hiding with a modified Mach-Zehnder interferometer. Opt Laser Eng. 55, 258–261 (2014).

7. Jun L., Jiaosheng L., Yangyang P. & Rong L. Optical image encryption and hiding based on a modified Mach-Zehnder interferometer. Opt. Express. 22, 4849–4860 (2014).
8. Patten R. E. *et al.* Speckle photography: mixed domain fractional Fourier motion detection. Opt Lett. 31, 32–34 (2006).
9. Magana-Loaiza O. S., Howland G. A., Malik M., Howell J. C. & Boyd R. W. Compressive object tracking using entangled photons. Appl. Phys. Lett. 102, 231104 (2013).
10. Sun B. *et al.* 3D Computational Imaging with Single-Pixel Detectors. Science. 340, 844–847 (2013).
11. Clemente P. *et al.* Compressive holography with a single-pixel detector. Opt. Lett. 38, 2524–2527 (2013).
12. Jun L., Yuping W., Rong L. & Yaqin L. Coherent single-detector 3D imaging system. Proceedings of the SPIE - The International Society for Opt Eng. 8913, 891303 (891304 pp.)-891303 (891304 pp.) (2013).
13. Li J. *et al.* Two-step Holographic Imaging Method based on Single-pixel Compressive Imaging. J Opt Soc Korea. 18, 146–150 (2014).
14. Katz O., Bromberg Y. & Silberberg Y. Compressive ghost imaging. Appl. Phys. Lett. 95, 131110 (2009).
15. Assmann M. & Bayer M. Compressive adaptive computational ghost imaging. Sci. Rep.-uk 3, (2013).
16. Howland G. A., Lum D. J., Ware M. R. & Howell J. C. Photon counting compressive depth mapping. Opt. Express. 21, 23822–23837 (2013).
17. Chapman H. N. & Nugent K. A. Coherent lensless X-ray imaging. Nat. Photonics. 4, 833–839 (2010).
18. Howland G. A., Schneeloch J., Lum D. J. & Howell J. C. Simultaneous Measurement of Complementary Observables with Compressive Sensing. Phys. rev. let. 112, 253602 (2014).
19. Mirhosseini M., Magana-Loaiza O. S., Rafsanjani S. M. H. & Boyd R. W. Compressive Direct Measurement of the Quantum Wave Function. Phys. rev. let. 113, 090402 (2014).
20. Zorzi M., Gluhak A., Lange S. & Bassi A. from today's intranet of things to a future Internet of things: a wireless and mobility related view. Ieee Wirel Commun. 17, 44–51 (2010).
21. Huang R., Rhee K. H. & Uchida S. A parallel image encryption method based on compressive sensing. Multime Tools Appl. 72, 71–93 (2014).
22. Chen W., Quan C. & Tay C. J. Optical color image encryption based on Arnold transform and interference method. Opt. Commun. 282, 3680–3685 (2009).
23. Lu P., Xu Z., Lu X. & Liu X. Digital image information encryption based on Compressive Sensing and double random-phase encoding technique. Optik. 124, 2514–2518 (2013).
24. Liu X., Cao Y., Lu P., Lu X. & Li Y. Optical image encryption technique based on compressed sensing and Arnold transformation. Optik. 124, 6590–6593 (2013).
25. Aidi Z., Nanrun Z. & Lihua G. Color Image Encryption Algorithm Combining Compressive Sensing with Arnold Transform. J Comput. 8, 2857–2863 (2013).

9/23/2016