REPORT DOCUMENTATION PAGE

Form Approved

OMB No. 0704-0188

PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
11-08-2015	Final	18 April 2013 to 17 April 2015

4. TITLE AND SUBTITLE

Securing Information with Complex Optical Encryption Networks

5a. CONTRACT NUMBER

FA2386-13-1-4106

5b. GRANT NUMBER

Grant AOARD-134106

5c. PROGRAM ELEMENT NUMBER

61102F

6. AUTHOR(S)

Prof. Swee Ping Yeo

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

National University of Singapore
#E4-05-45, 4 Engineering Drive 3
Singapore 117583
Singapore

8. PERFORMING ORGANIZATION REPORT NUMBER

N/A

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

AOARD
UNIT 45002
APO AP 96338-5002

10. SPONSOR/MONITOR'S ACRONYM(S)

AFRL/AFOSR/IOA(AOARD)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

AOARD-134106

12. DISTRIBUTION/AVAILABILITY STATEMENT

Distribution A: Approved for public release. Distribution is unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

The research will focus on the underlying theory and methodologies to configure complex optical encryption networks for securing information. The goal is to study/develop the architectures for a number of complex optical encryption networks, and to provide effective and reliable solutions for information security.

15. SUBJECT TERMS

Optical Encryption, Network Security, Network Vulnerability , Multi-dimentional Processing, optoelectronic devices

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Seng Hong, Ph.D.
U	U	U	SAR	14	19b. TELEPHONE NUMBER *(Include area code)* +81 4 2511 2005

Standard Form 298 (Rev. 8/98)
Prescribed by ANSI Std. Z39.18

AOARD Grant 134106

PIs: Swee Ping Yeo and Xudong Chen

National University of Singapore,
Department of Electrical and Computer Engineering,
4 Engineering Drive 3, Singapore 117583, Singapore

Project: Securing Information with Complex Optical Encryption Networks

Period of performance reported: 04/18/2013 - 04/17/2015

1. Summary of the Project

In implementing this research project, several research topics as follows have been conducted:

(1) Nonlinear security system has been designed to withstand the attacks.

(2) 3D-space-based optical signal processing strategies have been introduced to enlarge key space.

(3) Optical encoding principles have been studied and integrated into a large number of different complex optical encryption networks. Arbitrary encoding path in the designed optical encryption networks can be chosen by the sender for securing information.

(4) Various optical setups and principles have been analyzed and sifted for the optical cryptography topology. The combination of different topology types is feasible to create a new and complex topology type for optical cryptography.

(5) A multiple-CCD system has been designed and applied in the complicated optical topology, and an administrator can send the different encrypted information to different receivers in order to confuse the attackers.

Research works have been published as journal or conferences papers. In total, **4 journal papers** have been published, **and 2 conference papers** have been presented. In addition, we have been invited to give **2 talks** related to optical security.

2. Details of the Research Work

Due to the popularization of networking and internet, much research effort is made in the field of information security. Military communication system makes an increasing use of traffic security techniques, which seek to conceal its sender, its receiver and the content of messages. **The research topic in this project** is to establish the underlying theory and methodologies to configure complex optical encryption networks for securing information. **The main objective** is to propose the architectures for a number of complex optical encryption networks so as to provide effective and reliable solutions for information security. **Various novel optical cryptosystems** are developed and integrated into the encoding networks, which are highly desirable for a range of applications, such as defence sector, domestic security sector and immigration control sector. **In the implementation period, we have made some important contributions, and technical details related to several individual encryption strategies in the designed networks are given as follows:**

(2.1) In the first contribution, we have studied optical security using ghost imaging in 3D space (**see Fig.1**). The series of random phase-only masks are sparsified, which are further converted into particle-like distributions placed in 3D space. Our results demonstrate that a larger key space can be generated due to application of 3D space compared with previous works. It is believed that this finding can effectively enlarge application domain of ghost imaging for optical security, and a different research perspective may be opened up for ghost-imaging-based optical encoding.

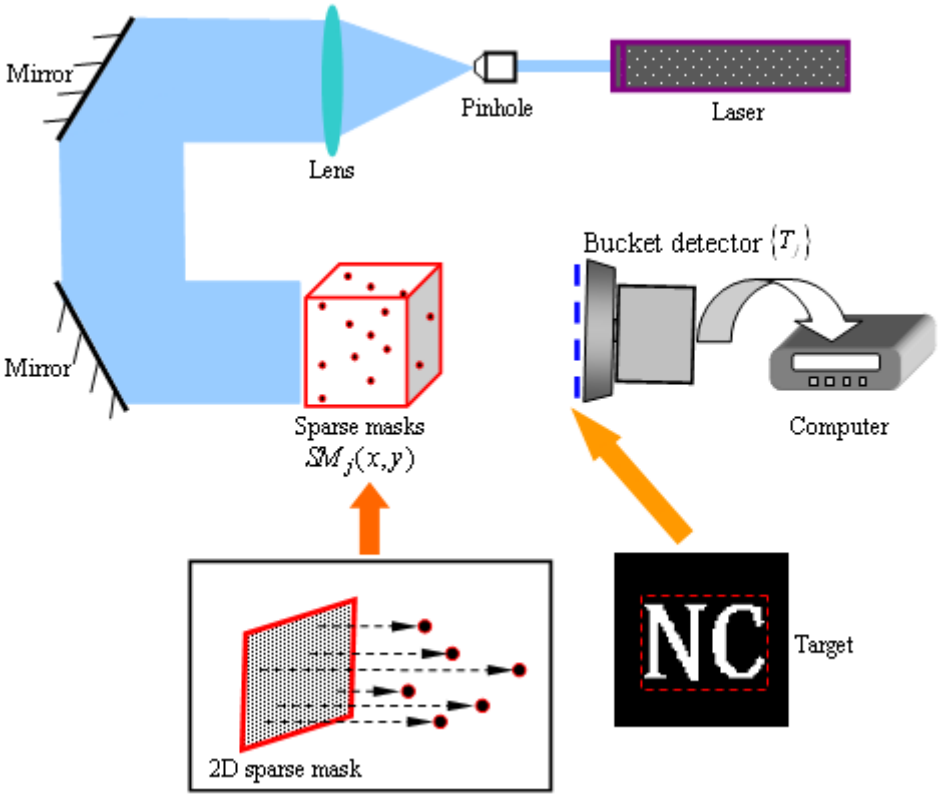

Fig. 1. Optical encoding setup based on ghost imaging. For simplicity, wave propagation at the reference path is virtually computed, and is not shown here.

A series of random 2D phase-only masks (such as **30000**) can be converted into 3D space for enlarging key space of the designed optical cryptosystem, and only some particles are available during the encoding (i.e., sparse strategy). **Single-pixel bucket detector** can record a series of intensity points which serve as ciphertexts, and a series of reference intensity patterns can be correspondingly recorded. The data decoding process is mainly based on correlation principle between the series of intensity points (object arm) and the reference sequence (reference arm). Since the decoded images should be verified by using a nonlinear correlation algorithm without direct observation of the image, an additional security layer can be correspondingly generated. **Figure 2** shows flow chart for illustrating data encoding and decoding process.

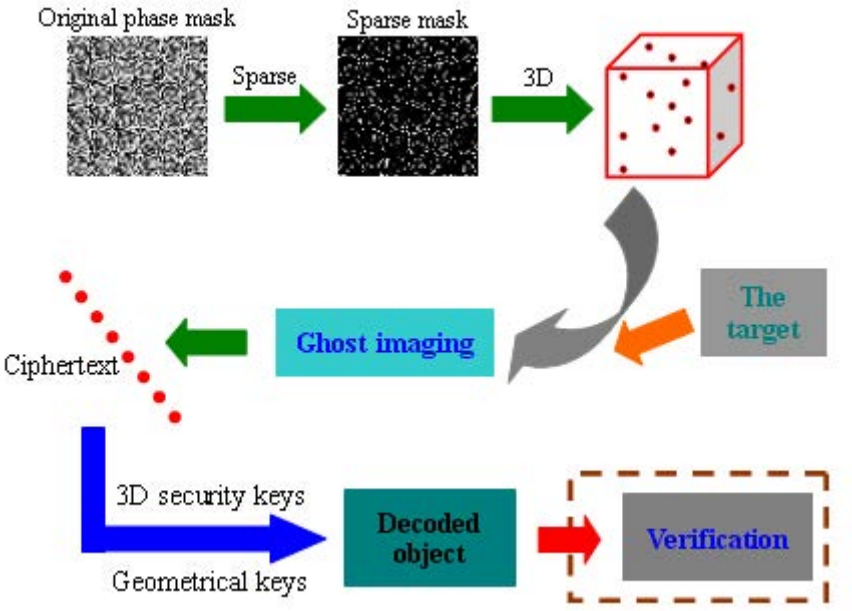

Fig. 2. Flow chart for illustrating data encoding and decoding process.

Figures 3 and 4 show some results based on the developed 3D-ghost-imaging optical security system. Optical verification is applied without direct observation of the plaintext [**see Figs. 3(a) and 3(b)**], which will provide an additional security layer for the optical encoding system. Only one remarkable peak can be observed in **Fig. 3(b)**, which means the correct security keys being employed.

When 2D sectional decryption is implemented, only noisy backgrounds can be obtained and observed as shown in **Figs. 4(c) and 4(d)** [respectively corresponding to **Figs. 4(a) and 4(b)**]. Hence, 3D optical security is realized for generating a larger key space.

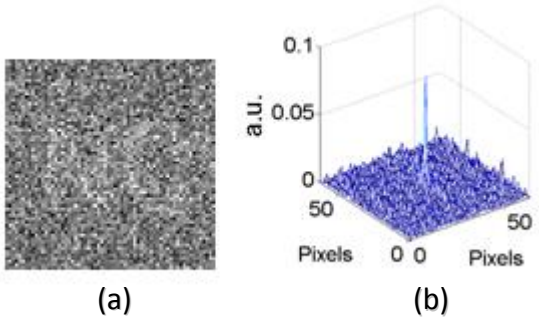

Fig. 3. Optical decoding with correct keys: (a) decoded image, and (b) nonlinear correlation map corresponding to (a).

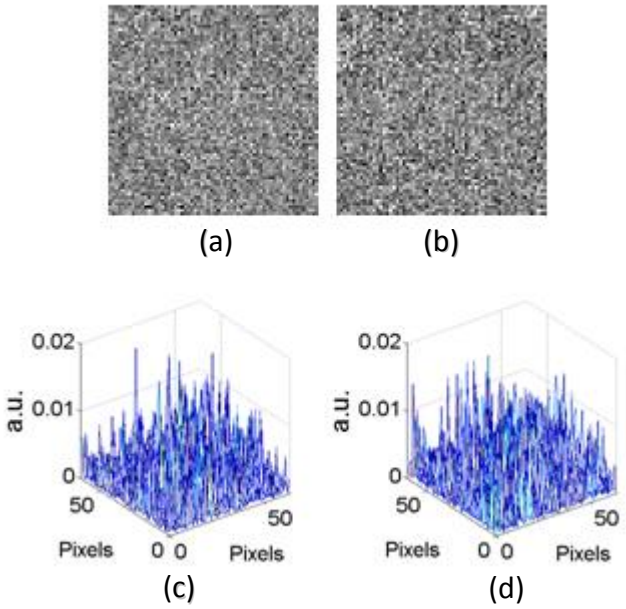

Fig. 4. Sectional decodings: (a) and (b) decoded images by considering only one section, and (c) and (d) nonlinear correlation maps respectively corresponding to (a) and (b).

(2.2) In the second contribution, we have proposed single-path beam-propagation-based imaging via aperture movement for optical encryption (**see Fig. 5**). A series of diffraction intensity patterns (i.e., ciphertexts) are recorded via aperture movement during optical encryption, and an iterative phase retrieval algorithm is correspondingly applied for the decryption. Our results demonstrate that the proposed optical encryption method possesses several significant advantages over the ptychography-based image encoding method. The shape of available illumination region can be flexibly designed and modified through the aperture, and aperture size can be easily changed according to encoding requirement. Overlapping area among neighboring aperture regions can be precisely controlled without the illumination shift during optical encryption, and it is also possible for the sender to control information assignment or distribution for establishing multiple security levels. In addition, when sparse plaintext is used during optical encryption, the proposed scheme can still authenticate the decrypted image without direct observation of plaintext information.

In **Fig. 5**, two random phase-only masks (M1 and M2) are used in the optical path, and an aperture (A) is placed just behind the phase-only mask M1. In practice, different aperture shapes and sizes can be arbitrarily generated and applied during optical encoding, and varied apertures can be easily generated by using amplitude-only spatial light modulator. When the designed aperture is sequentially moved in the transverse domain, a series of diffraction intensity patterns are correspondingly recorded by the CCD camera as the ciphertexts. During data decryption, phase retrieval algorithm is correspondingly developed and applied. If the movable aperture sequentially covers all plaintext regions, the recorded diffraction intensity patterns (i.e., ciphertexts) can provide sufficient information for extracting the full plaintext during the decryption. The sender can also choose to transmit only a few neighboring diffraction intensity patterns for controlling system security, and only small parts of the plaintext will be available to each authorized receiver.

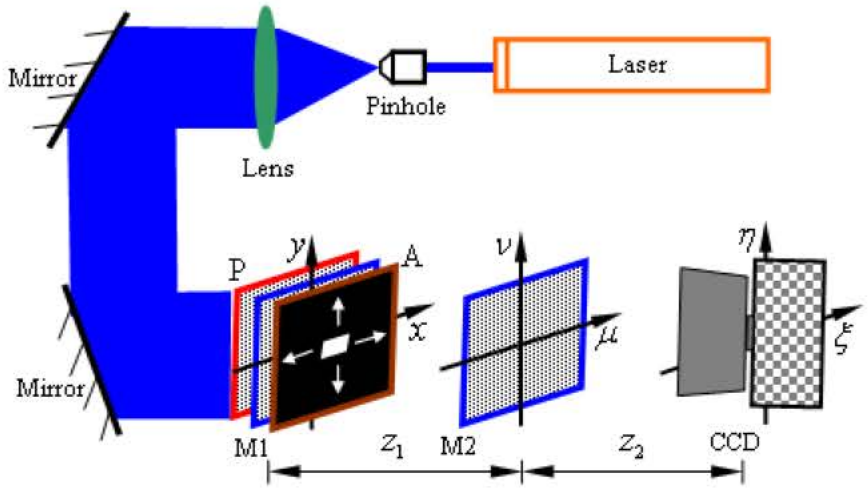

Fig. 5. Schematic experimental setup for the developed optical security system with movable aperture: M, phase-only mask; A, Aperture; P, plaintext; CCD, charge-coupled device.

In our contribution, three typical apertures [**see Figs. 6(c), 6(d) and 6(e)**] are designed and applied, and in practice a large number of apertures can be arbitrarily designed. Since these apertures can also be considered as security keys, a large key space can be generated. It can be seen in **Fig. 6(g)** that after optical encoding, the input image (P) can be converted into stationary white noise.

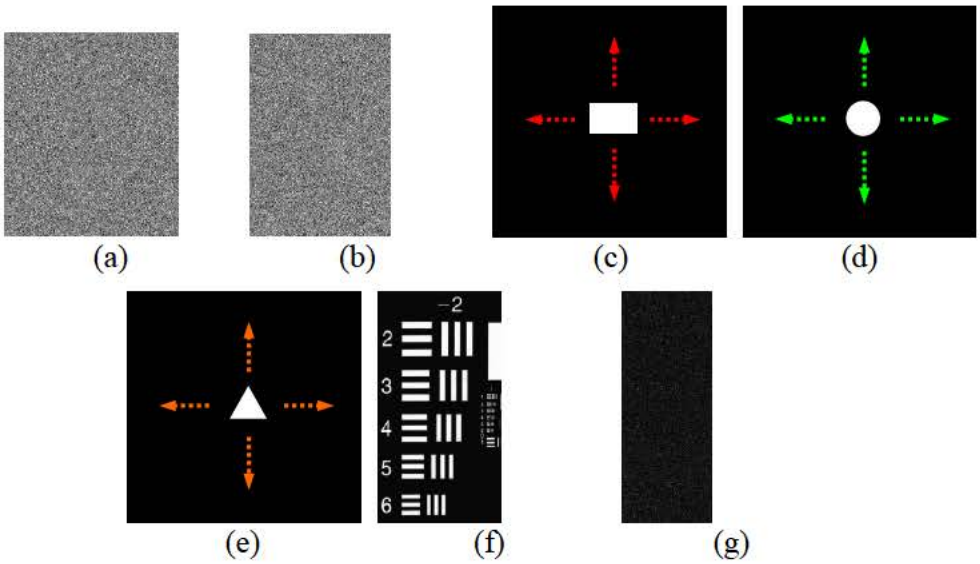

Fig. 6. Phase-only masks (a) M1 and (b) M2; schematic illustration of the movements of (c) rectangle-shaped aperture, (d) circle-shaped aperture, (e) triangle-shaped aperture; (f) an input image (i.e., the plaintext); and (g) one typical diffraction intensity pattern (i.e., ciphertext).

In **Figs. 7, 8 and 9**, different aperture structures are applied during optical encryption, and the corresponding decryption results with correct or wrong keys are demonstrated. It can be seen that a rapid convergence rate can be achieved in the designed phase retrieval algorithm during data decoding. Since the aperture is applied, the whole input image can be flexibly controlled and distributed. For instance, one specific receiver is allowed to access to only some small parts of the input image during digital (or optical) decoding.

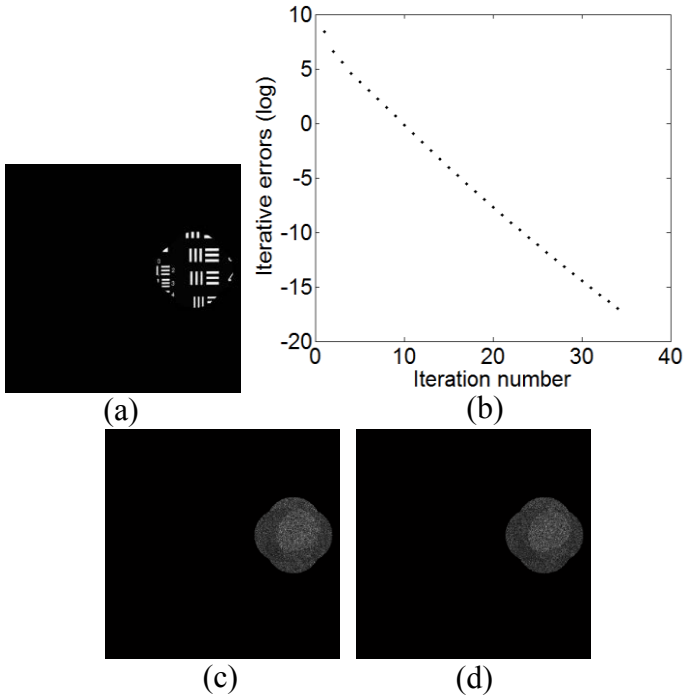

Fig. 7. The circle-shaped aperture and only five neighboring aperture positions: (a) The decrypted image obtained by using correct security keys, (b) a relationship between the number of iterations and iterative errors (with logarithm scale), (c) the decrypted image obtained after 500 iterations using wrong wavelength, and (d) decrypted image obtained after 500 iterations using wrong phase-only mask M2.

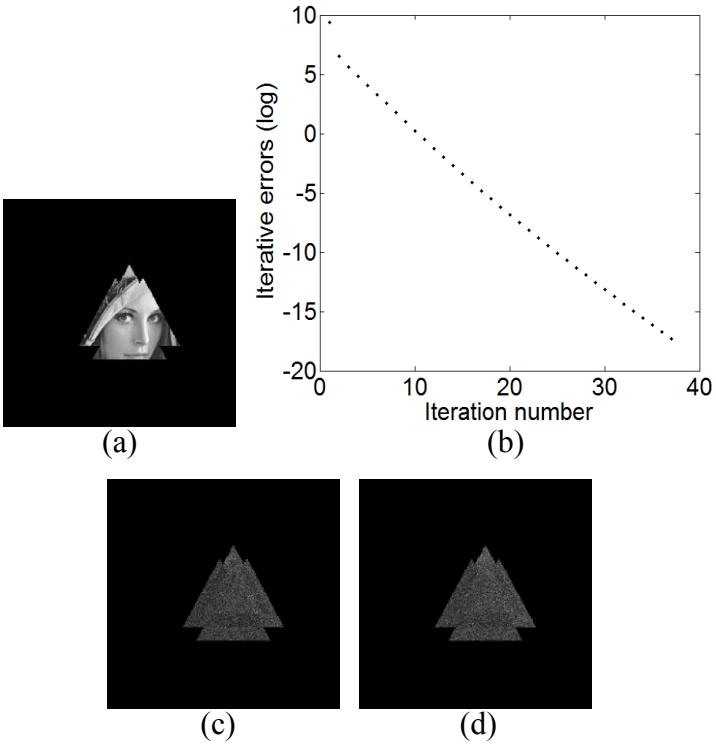

Fig. 8. Triangle-shaped aperture and only five neighboring aperture positions: (a) The decrypted image obtained by using correct security keys, (b) the relationship between the number of iterations and iterative errors with logarithm scale (only 37 iterations are requested), (c) decrypted image obtained after 500 iterations using wrong wavelength, (d) a decrypted image obtained after 500 iterations using wrong phase-only mask M2.

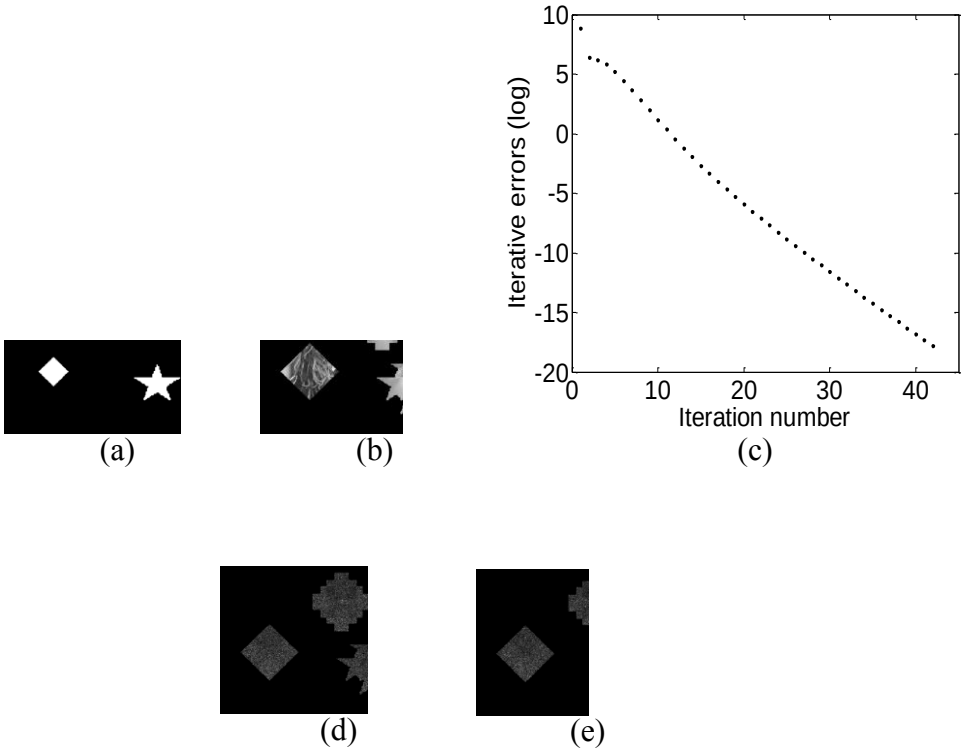

Fig. 9. Aperture array and only five neighboring aperture positions: (a) One simple aperture array, (b) a decrypted image obtained by using correct security keys, (c) a relationship between the number of iterations and iterative errors (with the logarithm scale), (d) a decrypted image obtained after 500 iterations using wrong wavelength, and (e) decrypted image after 500 iterations using wrong phase-only mask M2.

(2.3) In the third contribution, we have investigated optical encryption based on 3D sphere and phase retrieval in gyrator transform domain (**see Figs. 10 and 11**). The plaintext is divided into a series of small quadratic blocks, and each block is considered as a particle. In practical applications, the particles which do not contain plaintext information may not be processed during image encryption, and only valid particles should be considered. The series of particles can be distributed in 3D spheres, and is iteratively encrypted into one phase-only mask based on the phase retrieval algorithm. The results demonstrate that the presented virtual-optics-based cryptosystem is feasible and effective for optical encryption, and the developed optical encryption scheme can achieve the higher security compared with conventional optical encryption methods. It is believed that when the plaintext is simultaneously encrypted into multiple phase-only masks, higher cryptosystem security can be achieved correspondingly.

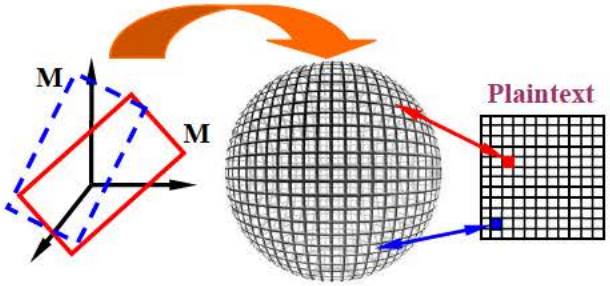

Fig. 10. A schematic illumination of the developed optical encryption method: M, extracted phase-only mask. It is worth noting that phase-only mask M and the coordinate (x,y,z) can be placed inside the 3D sphere for the illustration of the proposed method. The plaintext can also be simultaneously encrypted into multiple phase-only masks.

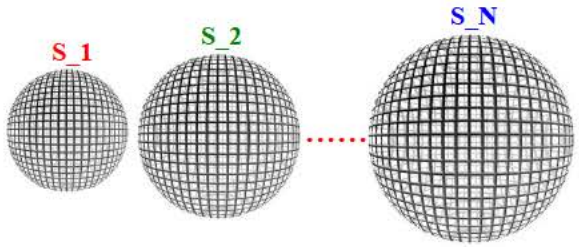

Fig. 11. A schematic illumination of several concentric spheres for the proposed optical encryption method: S, sphere; N, the number of sphere. These transparent spheres can be placed around the same nucellus [i.e., (0,0,0)], and the series of particles (i.e., plaintext) can be randomly distributed in the surface of different concentric spheres.

Figure 12(a) shows a relationship between the number of iterations and iterative errors during optical encryption, and **Fig. 12(b)** shows the corresponding relationship with a logarithm scale. It can be seen in **Figs. 12(a) and 12(b)** that the proposed phase retrieval algorithm can rapidly converge after several iterations. When security keys (such as transform angles) are correct, a decrypted image is extracted in **Fig. 13**. The CC (correlation coefficient) value for **Fig. 13** is 0.8302. Since the plaintext is distributed in 3D spheres, quality of decrypted images could be affected. However, most information about the plaintext can still be observed during image decryption, when security keys are correct. In practice, more neighboring pixels can be combined to generate each particle, which might enhance the quality of decrypted images.

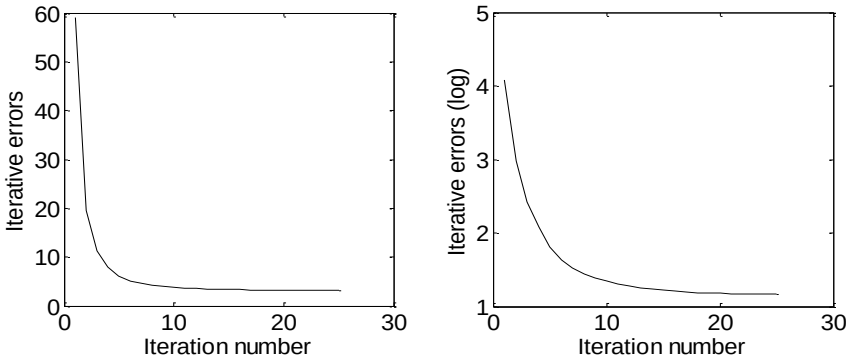

Fig. 12. (a) A relationship between the number of iterations and iterative errors during optical encryption; and (b) a relationship with logarithm scale corresponding to (a).

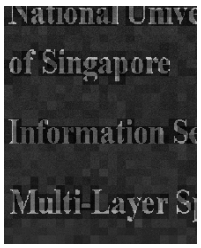

Fig. 13. A decrypted image obtained by using correct security keys.

Since the plaintext is divided into a series of particles distributed in the 3D spheres, the series of transform angles can be considered as principal key. In addition, any decryption with one single transform angle cannot visually render information about the plaintext. **Figures 14(a)–14(c)** show decrypted images when only one single transform angle of $\pi/9$, $\pi/4$ and $\pi/3$ is directly applied during the decryption, respectively. Only one sectional decryption is conducted for each case in **Figs. 14(a)–14(c)**. The CC (correlation coefficient) values for **Figs. 14(a)–14(c)** are 0.0092, 0.0315 and 0.0214, respectively. It can be seen in **Figs. 14(a)–14(c)** that when only one single transform angle is used during image decryption, no information about the plaintext can be extracted. One significant advantage of the proposed method is that the plaintext is distributed in the 3D spheres, and the series of random transform angles can be employed as principal key. When the series of transform angles is wrong during image decryption, a decrypted image with CC value of 0.0133 is obtained in **Fig. 14(d)**. It can be seen in **Fig. 14(d)** that no information about the plaintext can be obtained during image decryption, when security key is wrong.

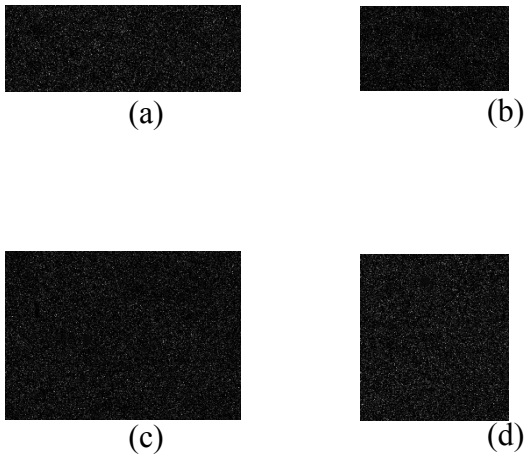

Fig. 14. Decrypted images directly using one single transform angle of (a) $\pi/9$, (b) $\pi/4$ and (c) $\pi/3$; and (d) a decrypted image obtained by using wrong transform angles. One sectional decryption is conducted for (a)-(c).

(2.4) In the fourth contribution, we have proposed a new method using iterative phase retrieval for simultaneously generating two phase-only masks with silhouette removal in the interference-based optical encryption **(see the setup in Fig. 15)**. The two phase-only masks are alternately updated during the iterations, and no any one of phase-only masks is always fixed during the encoding. In our studies, it has been found that only a few iterations are required in the proposed phase retrieval algorithm, and no additional keys (or masks) or complementary strategies are required for silhouette removal. Our studies demonstrate that the proposed method is feasible and effective, and silhouette problem inherent in interference-based optical encryption system is fully resolved rather than partially suppressed. It can be expected that the proposed method can provide a new and effective alternative for interference-based optical encryption.

In this contribution, both phase-only masks M1 and M2 are iteratively extracted, and are alternately updated during the iterations. **Figures 16(a) and 16(b)** show the extracted phase-only masks M1 and M2 by using the proposed method, respectively. It can be seen in **Figs. 16(a) and 16(b)** that the input image has been fully encoded, and plaintext information cannot be observed after the encoding. To illustrate the iterative process, a relationship between the number of iterations and CC (correlation coefficient) values is shown in **Fig. 17**. It can be seen in **Fig. 17** that a rapid convergence rate can be achieved in the proposed phase retrieval algorithm, and only a few iterations **(i.e., 15)** are required to satisfy the threshold. When all security keys and phase-only masks are correct, a decrypted image is obtained as shown in **Fig. 18(a)**. The CC value for **Fig. 18(a)** is 0.9992, which means the input image being accurately retrieved. When only the extracted phase-only mask M1 is used during the decryption, a decrypted image with CC value of -0.0491 is obtained as shown in **Fig. 18(b)**. When only the extracted phase-only mask M2 is used during the decryption, a decrypted image with CC value of -0.0029 is obtained as shown in **Fig. 18(c)**. It can be seen in **Figs. 18(b) and 18(c)** that silhouette problem is fully resolved by using the proposed method.

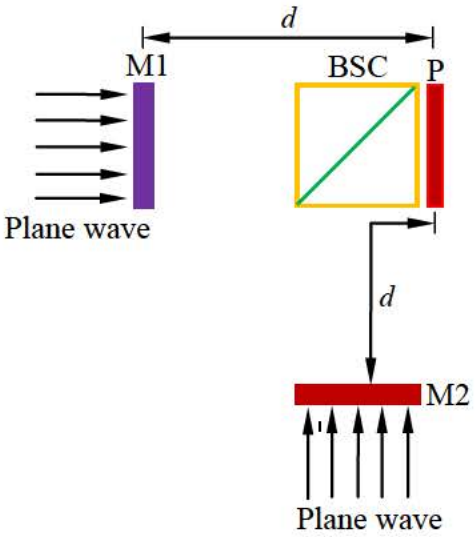

Fig.15. A schematic setup for interference-based optical encryption: M, phase-only mask; BSC, beam splitter cube; P, plaintext (an input image); d, axial distance.

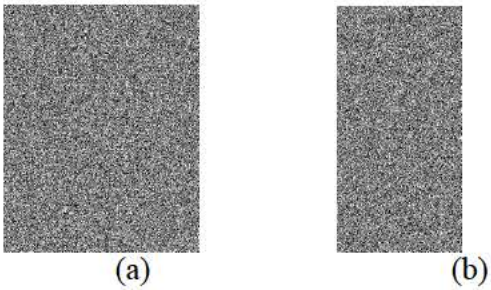

Fig. 16. Phase-only masks (a) M1 and (b) M2 extracted by using the proposed method.

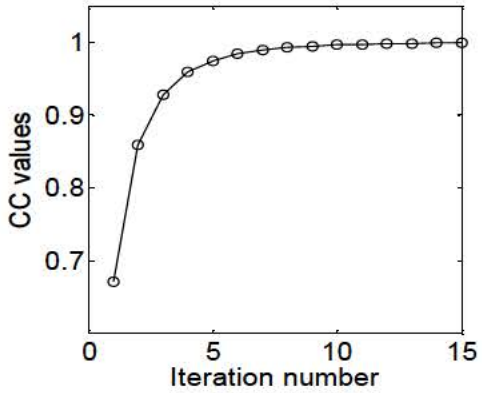

Fig. 17. A relationship between the number of iterations and CC (correlation coefficient) values during image encryption based on the proposed method.

(a) (b) (c)

Fig. 18. (a) A decrypted image obtained when all security keys and phase-only masks are correct, (b) a decrypted image obtained when only the extracted phase-only mask M1 is used during the decryption, and (c) a decrypted image obtained when only the extracted phase-only mask M2 is used during the decryption.

3. Impact of the Research Work

It is expected that optical encryption can attract more and more attention in various sectors (such as defence and security), due to its inherent nature of optical signal processing, i.e., parallel processing, high speed, high security, high flexibility and multi-dimensional capabilities. Compared with electronic cryptography, **unique characteristics of optical encryption** are briefly illustrated as follows:

(a) Optical instruments have parallel-processing and high-speed capabilities. In addition to software platform, optical hardware provides an effective alternative in practical applications.

(b) Higher security can be achieved in the optical encryption systems. Information or materials can be encrypted or hidden in multiple dimensions, such as phase, intensity and light polarization.

(c) Since the sophisticated optoelectronic devices and systems should be analyzed before the retrieval, any hostile hacker will need to possess multi-disciplinary scientific background (such as optics, mathematics, computer, and information theory) and conduct a laborious process of decoding the information (whether in the form of data or images). In other words, before an attacker can even begin a laborious process of decoding, he/she has to gain access to the sophisticated optoelectronic principles and systems where he/she needs to process the information. However, in the military applications, most military information requires **timeliness especially during the war or military conflict**, and the decoded information (**such as commands**) will become invalid to the attacker after a long decoding period.

In practical applications, important or sensitive information/materials (**such as operational plans and military maps in defence sector**) can be encoded by using different optical encoding strategies selected from the designed complex optical encryption networks. Either optical or digital (virtual optics) approach can be used to implement the designed optical encryption method, which can provide high flexibility for defence applications. We believe that optical encryption can open up a new research perspective for information security (i.e., data storage and transmission), and provide a new and powerful alternative for protecting military information in defense sector, such as Air Force.

Publications:

Journal Papers

[1] Wen Chen and Xudong Chen, “Ghost imaging for three-dimensional optical security,” Applied Physics Letters, vol. 103, 221106 (4pp), 2013.

[2] Wen Chen, Guohai Situ, and Xudong Chen, “High-flexibility optical encryption via aperture movement,” Optics Express, vol. 21, 24680–24691, 2013.

[3] Xiaogang Wang, Wen Chen, and Xudong Chen, “Fractional Fourier domain optical image hiding using phase retrieval algorithm based on iterative nonlinear double random phase encoding,” Optics Express, vol. 22, 22981–22995, 2014.

[4] Wen Chen and Xudong Chen, "Iterative phase retrieval for simultaneously generating two phase-only masks with silhouette removal in interference-based optical encryption," Optics Communications, vol. 331, 133–138, 2014.

Conference Papers

[5] Wen Chen and Xudong Chen, “Optical encryption based on 3-D sphere and phase retrieval in gyrator transform domain,” IEEE TENCON 2013, October 22–25 2013, Xi'an, China.

[6] Wen Chen and Xudong Chen, “Single-pixel optical imaging with compressed reference intensity patterns,” SPIE conference, International Conference on Experimental Mechanics (icEM2014) 15–17 Nov. 2014, Singapore.

Invited Talks

[7] Our team member was invited by School of Optical and Electronic Information in Huazhong University of Science and Technology (HUST), WuHan City, China, to present an invited talk called “Information Secured by Optics,” in 2014 East Lake International Forum for Outstanding Overseas Young Scholars, Dec. 28th–30th, 2014.

[8] Our team member was invited by the organization committee of "International Symposium on 3D Imaging, Metrology, and Data Security" to present a topic of "Optical information encryption and authentication based on ghost imaging" in September 26th–29th, 2015 at Shenzhen, China.