ISSN 1674-1056
http://cpb.iphy.ac.cn
http://iopscience.iop.org/cpb
中国物理 B
Chinese Physics
中国物理 Chinese Physics B

Phase retrieval algorithm for optical information security

Shi-Qing Wang(王诗晴), Xiang-Feng Meng(孟祥锋), Yu-Rong Wang(王玉荣), Yong-Kai Yin(殷永凯), Xiu-Lun Yang(杨修伦)

Citation: Chin. Phys. B . 2019, 28(8): 084203. **doi:** 10.1088/1674-1056/28/8/084203
Journal homepage: http://cpb.iphy.ac.cn; http://iopscience.iop.org/cpb

What follows is a list of articles you may be interested in

Multiple-image encryption by two-step phase-shifting interferometry and spatial multiplexing of smooth compressed signal

Xue Zhang(张学), Xiangfeng Meng(孟祥锋), Yurong Wang(王玉荣), Xiulun Yang(杨修伦), Yongkai Yin(殷永凯)

Chin. Phys. B . 2018, 27(7): 074205. **doi:** 10.1088/1674-1056/27/7/074205

Implication of two-coupled tri-stable stochastic resonance in weak signal detection

Quan-Quan Li(李泉泉), Xue-Mei Xu(许雪梅), Lin-Zi Yin(尹林子), Yi-Peng Ding(丁一鹏), Jia-Feng Ding(丁家峰), Ke-Hui Sun(孙克辉)

Chin. Phys. B . 2018, 27(3): 034203. **doi:** 10.1088/1674-1056/27/3/034203

Application of optical diffraction method in designing phase plates

Ze-Min Lei(雷泽民), Xiao-Yan Sun(孙晓艳), Feng-Nian Lv(吕凤年), Zhen Zhang(张臻), Xing-Qiang Lu(卢兴强)

Chin. Phys. B . 2016, 25(11): 114201. **doi:** 10.1088/1674-1056/25/11/114201

Image encryption using random sequence generated from generalized information domain

Xia-Yan Zhang(张夏衍), Guo-Ji Zhang(张国基), Xuan Li(李璇), Ya-Zhou Ren(任亚洲), Jie-Hua Wu(伍杰华)

Chin. Phys. B . 2016, 25(5): 054201. **doi:** 10.1088/1674-1056/25/5/054201

A general phase retrieval algorithm based on ptychographicalliterative engine for coherent diffractive imaging

Fu Jian, Li Peng

Chin. Phys. B . 2013, 22(1): 014204. **doi:** 10.1088/1674-1056/22/1/014204

Phase retrieval algorithm for optical information security*

Shi-Qing Wang(王诗晴), Xiang-Feng Meng(孟祥锋), Yu-Rong Wang(王玉荣), Yong-Kai Yin(殷永凯), and Xiu-Lun Yang(杨修伦)†

Department of Optics, School of Information Science and Engineering, and Shandong Provincial Key Laboratory of Laser Technology and Application, Shandong University, Qingdao 266237, China

(Received 9 March 2019; revised manuscript received 16 May 2019; published online 9 July 2019)

As a typical technology for optical encryption, phase retrieval algorithms have been widely used in optical information encryption and authentication systems. This paper presents three applications of two-dimensional (2D) phase retrieval for optical encryption and authentication: first, a hierarchical image encryption system, by which multiple images can be hidden into cascaded multiple phase masks; second, a multilevel image authentication system, which combines (t, n) threshold secret sharing (both t and n are positive integers, and $t \leq n$) and phase retrieval, and provides both high-level and low-level authentication; and finally, a hierarchical multilevel authentication system that combines the secret sharing scheme based on basic vector operations and the phase retrieval, by which more certification images can be encoded into multiple cascaded phase masks of different hierarchical levels. These three phase retrieval algorithms can effectively illustrate phase-retrieval-based optical information security. The principles and features of each phase-retrieval-based optical security method are analyzed and discussed. It is hoped that this review will illustrate the current development of phase retrieval algorithms for optical information security and will also shed light on the future development of phase retrieval algorithms for optical information security.

Keywords: phase retrieval algorithm, authentication system, image encryption

PACS: 42.30.Rx, 42.30.Va, 42.30.Wb, 42.30.Kq **DOI:** 10.1088/1674-1056/28/8/084203

1. Introduction

The security issues of information, especially image information have received increasing attention. Besides traditional image information security,[1,2] optical information security also has a lot of room to develop. Different kinds of optical information processing technologies have been put into application to realize more efficient security systems, such as phase retrieval algorithms, double random phase encoding (DRPE) technique,[3–6] digital holography,[7–9] phase-shifting interferometry,[10–12] ghost imaging,[13–19] aperture movement,[20] and sparse-phase multiplexing.[21]

Phase retrieval is a typical technology for optical encryption and authentication, which usually encodes the information of the secret image into one or several pseudo-random phase masks. This technique was first proposed by Wang *et al.* in 1996.[22] The encryption scheme was based on a $4f$ system, in which the secret image in the output plane was encoded into a phase mask in the Fourier plane by using a modified projection-onto-constraint-sets (POCS) algorithm, while the other phase mask in the input plane was fixed. Situ and Zhang designed a two-phase-encoding-mask security scheme in 2004. In each iteration of their scheme, the phase distributions of both masks would be adjusted simultaneously,[23] which have improved the speed of iteration. Later, they also extended the iterative algorithm from the $4f$ system to the Fresnel domain.[24] From then on, many researches on optical encryption based on the phase retrieval algorithm have been carried out in the Fresnel domain. In 2012, a lensless multiple-image optical encryption scheme based on the cascading modified Gerchberg–Saxton (GS) algorithm in the Fresnel domain was proposed by Huang *et al.*,[25] which increased the encryption capacity while avoiding the crosstalk noise. Chen *et al.* proposed an information authentication scheme based on cascaded iterative phase retrieval algorithm and sparse representation in 2013, in which the concept of nonlinear correlation was used to identify the decoded image when it cannot be identified through directly visual detection.[26] We have also done some work in this field. We first designed a hierarchical image encryption system based on cascaded iterative phase retrieval algorithm in 2007.[27] During 2013 ∼ 2017, several multilevel authentication systems were designed in succession, in which the phase retrieval algorithm was combined with the phase multiplexing or secret sharing algorithms, which made the authentication systems have good information encryption characteristic and security.[28–32] We proposed a secret shared multiple image encryption method based on row scanning compressive ghost imaging and phase retrieval in 2017, which increased data encryption efficiency and realized secret key data sharing.[33]

*Project supported by the National Natural Science Foundation of China (Grant Nos. 61775121, 61605165, 61307003, 61405122, and 11574311), the Key Research and Development Program of Shandong Province, China (Grant No. 2018GGX101002), the Natural Science Foundation of Shandong Province, China (Grant No. ZR2019QF006), and the Fundamental Research Funds of Shandong University, China (Grant No. 2015GN031).

†Corresponding author. E-mail: xlyang@sdu.edu.cn

© 2019 Chinese Physical Society and IOP Publishing Ltd

In this paper, we review the phase retrieval algorithms for optical information security. As a typical technology for optical encryption, the excavation of its application prospect has always been a direction of our efforts. To give readers a sense of our meaningful work in this field, three phase retrieval algorithms for optical encryption and authentication are reviewed here: first, a hierarchical image encryption system, by which multiple images can be hidden into cascaded multiple phase masks; second, a multilevel image authentication system which combines (t, n) threshold secret sharing and phase retrieval, and provides both high-level and low-level authentication; and finally, a hierarchical multilevel authentication system combining secret sharing scheme based on basic vector operations and phase retrieval, by which more certification images could be encoded into multiple cascaded phase masks of different hierarchical levels. These three phase retrieval algorithms can effectively show a picture about phase-retrieval-based optical information security. The principles and features of each phase-retrieval-based optical security method are analyzed and discussed. New ideas, such as single-channel color image encryption, have also revitalized these systems.

2. Phase retrieval algorithms for optical encryption

2.1. Encryption of grayscale images

A schematic diagram of an optical information security system based on the iterative double phase retrieval algorithm in the Fresnel domain is shown in Fig. 1. The encryption process is to find two desired phase distributions by iterative algorithm under the given input and output constraints, and the commonly used phase retrieval algorithms are the modified GS algorithm[34] and POCS algorithm.[35]

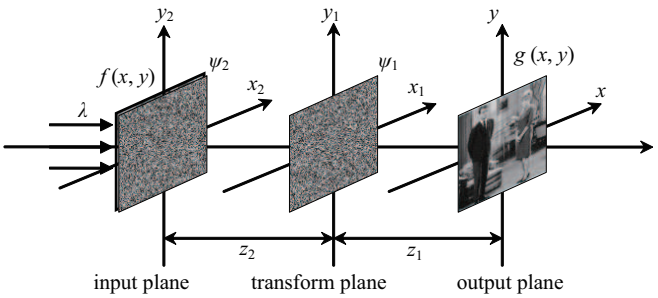


Fig. 1. Schematic diagram of optical information security system based on iterative double phase retrieval algorithm in Fresnel domain.

The two phase masks ψ_1 and ψ_2 whose initial phase values are randomly distributed between 0 and 2π are, respectively, placed in the transform plane (x_1, y_1) and input plane (x_2, y_2), and the secret image $g(x,y)$ is placed in the output plane (x, y). The distance between the transform and the output plane is z_1, and that between the input and the transform plane is z_2. We could place a binary or grayscale image $f(x,y)$ in the input plane clinging to the random phase mask ψ_2 as input amplitude constraint. When illuminating the input plane with an on-axis plane wave of unit amplitude and wavelength λ, after the kth iteration ($k = 1, 2, 3, \ldots$) the complex amplitude U^k in the output plane under the Fresnel approximation can be described as[24,36]

$$U^k(x,y) = \mathrm{FrT}_{z_1}\left(\mathrm{FrT}_{z_2}\left\{f\exp\left[\mathrm{i}\psi_2^k(x_2,y_2)\right]\right\} \times \exp\left[\mathrm{i}\psi_1^k(x_1,y_1)\right]\right), \tag{1}$$

where FrT denotes the Fresnel transform.

Suppose that the distributions of the two phase masks after the k-th iteration are ψ_1^k and ψ_2^k respectively, then in the $(k+1)$-th iteration process they can be described as follows:[27]

$$\psi_1^{k+1}(x_1,y_1) = \arg\left(\frac{\mathrm{IFrT}_{z_1}\left\{g\exp\left[\mathrm{i}\arg\left(U^k\right)\right]\right\}}{\mathrm{FrT}_{z_2}\left[f\exp\left(\mathrm{i}\psi_2^k\right)\right]}\right), \tag{2}$$

$$\psi_2^{k+1}(x_2,y_2) = \arg\left[\frac{\mathrm{IFrT}_{z_2}\left(\mathrm{IFrT}_{z_1}\left\{g\exp\left[\mathrm{i}\arg\left(U^k\right)\right]\right\}\exp\left(-\mathrm{i}\psi_1^{k+1}\right)\right)}{f}\right], \tag{3}$$

in the above expressions, IFrT_z denotes the inverse Fresnel transform and $\arg(\cdot)$ is the phase extraction operator. Or we could also take out the input image $f(x,y)$ and just illuminate the system by the on-axis plane wave, then the f in Eqs. (1)–(3) would be substituted by 1.

To evaluate the similarity between the output real amplitude image after the k-th iteration g^k and the original secret image g, the mean square error (MSE) and correlation coefficient (CC) are usually used as a convergence criterion, the iterations are repeated until the MSE is no longer larger than a predefined threshold or the CC is large enough. The MSE and CC are defined as follows:[36–38]

$$\mathrm{MSE} = \frac{1}{N}\sum_{x,y}\left[g^k(x,y) - g(x,y)\right]^2, \tag{4}$$

where N is the number of pixels of the image,

$$\mathrm{CC} = \frac{E\left\{\left[g - E(g)\right]\left[g^k - E\left(g^k\right)\right]\right\}}{\sigma_g\sigma_{g^k}}, \tag{5}$$

where $E\{\}$ denotes the expected value operator, and σ is the standard deviation of the corresponding image.

When the iteration cycle stops, two final phase distributions ψ_1 and ψ_2, located, respectively, in the transform and input plane, are generated, which can be stored as keys of decryption.

In the process of decryption, suppose that the original input image (if any) and the phase masks after iteration are placed at the correct position. Once the system is illuminated by a plane wave of the correct wavelength, the decrypted image will be available on the output plane.[36]

2.2. Encryption of color images

In recent years, the research of efficient color image encryption is in the ascendant.[39] Phase retrieval algorithms can also realize the encryption of color images. Unlike the traditional RGB three-channel encryption, our suggested single-channel encryption scheme for color images uses color filter array (CFA) in the traditional color-imaging scheme.

Color filter array was invented by Bryce Bayer. As can be seen from Fig. 2, the whole Bayer CFA is a series of interval single-color filters placed on each pixel, or in other words, it consists of a series of four lattices of 2×2: one R, one B and two G's. In this way, each channel can obtain a picture with partial value vacancies. Although this leads to the loss of two-thirds of the pixel values, it greatly reduces the amount of information, and the values of these vacancies can be filled by interpolation algorithms.[39] In 2017, Chen *et al.* applied this filter to a diffractive-imaging-based encryption scheme.[40]

Here, we introduce the Bayer CFA into our optical encryption scheme based on phase retrieval algorithm. Comparing with gray image, we need to do pre-processing before putting the color image in the output plane (x, y); *i.e.*, to sample the three-channel color image into the single-channel gray mosaic image by the Bayer CFA, and figure 3(a) depicts this step. After the process of decryption, we need to do post-processing so that the color image can be reconstructed from the gray mosaic image by interpolation algorithm, and figure 3(c) depicts this step.

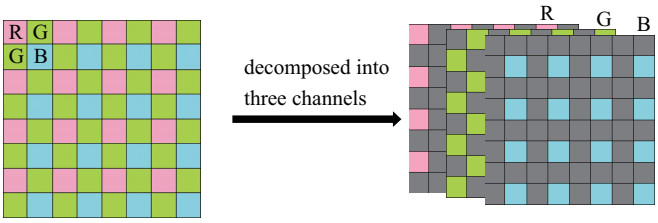


Fig. 2. Bayer color filter array pattern.

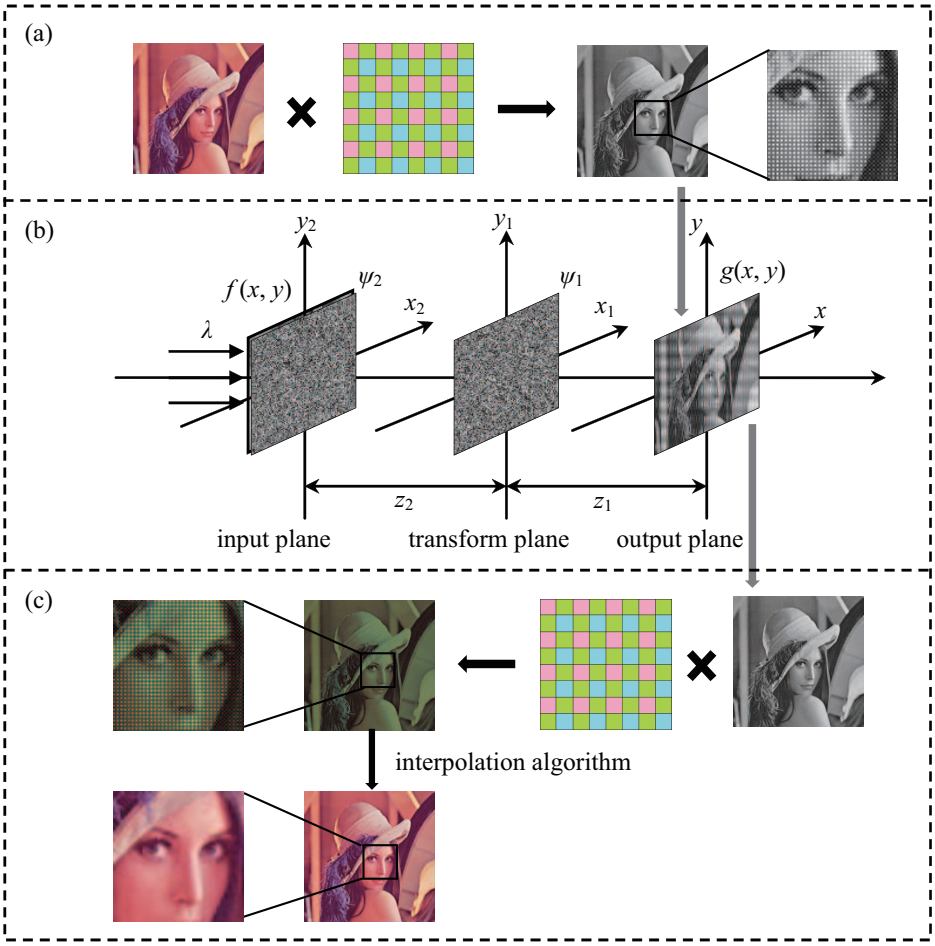


Fig. 3. (a) Pre-processing, (b) schematic diagram of optical information security system based on iterative double phase retrieval algorithm, (c) post-processing.

3. Hierarchical image encryption by using cascaded iterative phase retrieval algorithm[27]

A hierarchical image encryption system based on the cascaded iterative phase retrieval algorithm is presented in this section, which can encrypt the information of different levels into different cascaded phase masks. The use of multiple phase masks makes the convergence rate fast and the construction of hierarchical encryption avoid crosstalk noise. Thus, it can be widely used in hierarchical security authentication.

3.1. Theoretical analysis and description

A schematic diagram of an N-level encryption system by cascaded iterative phase retrieval algorithm is shown in Fig. 4. This system is extended from the optical information security system based on the iterative double phase retrieval algorithm. As shown in Fig. 4, $2N$ cascaded phase masks are used to encrypt and decrypt N secret images. In the k-th iteration, phase masks ψ_{2N} and ψ_{2N-1} are adjusted simultaneously to encrypt the N-th secret image, while the distributions of other phase masks ψ_1–ψ_{2N-2} retain the iteration results of the lower encryption levels.

Suppose that an on-axis plane wave of unit amplitude and wavelength λ illuminates the encryption system, under the premise of Section 2, we can derive that after the k-th iteration ($k = 1, 2, 3, \ldots$), the complex amplitude of N-level output image U_N^k can be described as[27]

$$U_N^k(x,y) = \mathrm{FrT}_{z_1}\{[\cdots \mathrm{FrT}_{z_{2N-2}}(\mathrm{FrT}_{z_{2N-1}}\{\mathrm{FrT}_{z_{2N}}[\exp(\mathrm{i}\psi_{2N}^k)] \times \exp(\mathrm{i}\psi_{2N-1}^k)\}\exp(\mathrm{i}\psi_{2N-2}))\cdots]\exp(\mathrm{i}\psi_1)\}, \quad (6)$$

then in the $(k+1)$-th iteration process, the distribution of phase masks ψ_{2N-1} and ψ_{2N} would be adjusted to

$$\psi_{2N-1}^{k+1} = \arg(\mathrm{IFrT}_{z_{2N-1}}\{[\cdots \mathrm{IFrT}_{z_2}(\mathrm{IFrT}_{z_1}\{g_N \exp[\mathrm{i}\arg(U_N^k)]\}\exp(-\mathrm{i}\psi_1))\cdots]\exp(-\mathrm{i}\psi_{2N-2})\}/\mathrm{FrT}_{z_{2N}}[\exp(\mathrm{i}\psi_{2N}^k)]), \quad (7)$$

$$\psi_{2N}^{k+1} = \arg(\mathrm{IFrT}_{z_{2N}}\{\mathrm{IFrT}_{z_{2N-1}}[(\cdots \mathrm{IFrT}_{z_1}\{g_N \exp[\mathrm{i}\arg(U_N^k)]\}\cdots)\exp(-\mathrm{i}\psi_{2N-2})]\exp(-\mathrm{i}\psi_{2N-1}^{k+1})\}). \quad (8)$$

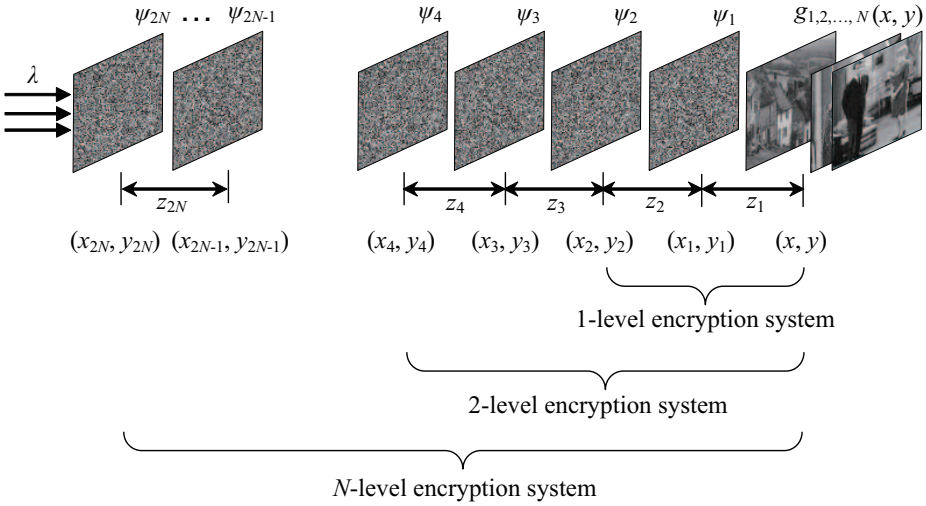


Fig. 4. Schematic diagram of N-level encryption system by cascaded iterative phase retrieval algorithm.

When the iteration cycle stops, the resulting phase distribution ψ_{2N-1} and ψ_{2N} together with other phase masks ψ_1–ψ_{2N-2}, can be utilized to retrieve the N-level secret image.

Hierarchical image encryption can classify the information according to the security level, thus it can be opened to users of different privilege levels. The 1-level encryption system is suitable for encrypting low level information, which requires only two keys (ψ_1 and ψ_2). The 2-level encryption system is suitable for encrypting higher level information, which requires four keys ($\psi_1 \sim \psi_4$), and so on. So in the hierarchical image encryption system, users with the highest level of privilege will obtain all the phase masks after each iteration, the cascade order of the phase masks, and the correct geometric parameters, such as wavelength and distance. At the same time, they can decrypt all the secret images. But users with low levels of authority cannot obtain secret images of higher levels.

3.2. Computer simulations and discussion

Taking the 4-level image encryption system for example, the feasibility of the system is verified by computer simulation. Four greyscale images 'Goldhill', 'Peppers', 'Lena', and 'Couple' represent 1st–4th level secret images, and they are shown in Figs. 5(a)–5 (d), respectively. For simplicity, all images used in the simulations have 256×256 pixels, and the resolution of all digital images is 15 μm on each plane. The

distance between all adjacent planes is 108.3 mm. And the wavelength λ is 0.532 μm. Unless otherwise specified, the same settings will be used in the simulations below.

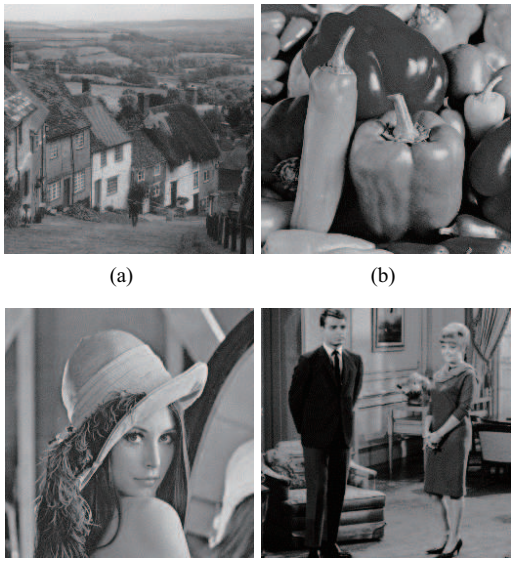


Fig. 5. Four greyscale images: (a) 'Goldhill', (b) 'Peppers', (c) 'Lena', and (d) 'Couple'.

Figure 6 depicts the convergence curves of each level, which show that the iterative algorithm has a good convergence effect. After 200 iterations, the eight phase keys are shown in Fig. 7, and the decrypted images with their corresponding CCs are shown in Table 1. Obviously, the quality of all the decrypted images is very high, and the CCs of them are almost equal to 1. If one tries to use the incorrect keys or the correct keys in wrong order to decrypt the secret images, then they will get nothing useful.

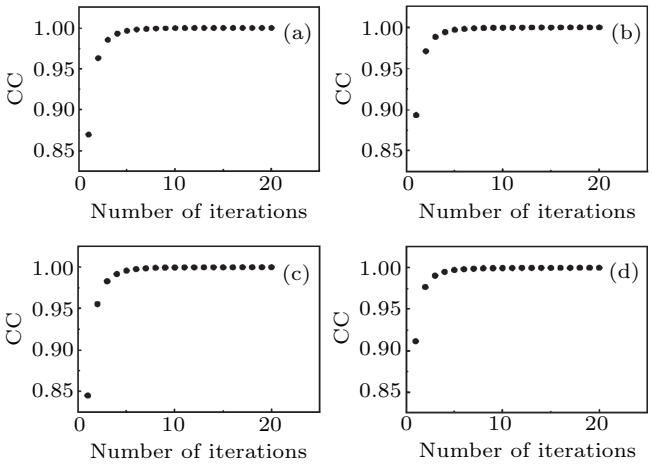


Fig. 6. Convergence curves of (a) 1st level, (b) 2nd level, (c) 3rd level, and (d) 4th level.

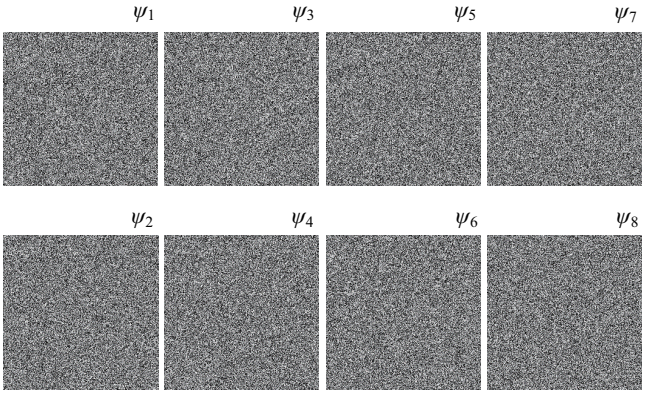


Fig. 7. Resulting eight phase keys after 200 iterations.

Table. 1 Decrypted images with their corresponding CCs.

Decrypted image				
	Goldhill	Peppers	Lena	Couple
CC	1.00000	1.00000	1.00000	0.99999



Fig. 8. Original RGB images ((a) and (c)), and their corresponding decrypted images ((b) and (d)).

To verify the feasibility of color image encryption, we replace the 2nd and 3rd level grayscale secret images 'Peppers' and 'Lena' with RGB images and repeat the simulation. The pre-processing and post-processing steps are added as shown in Section 2. The interpolation algorithm in the post-processing adopts a color demosaicking algorithm using direction similarity in color difference spaces,[39] and the steps of color correction and smoothing are added to obtain more realistic results. The original images and their decrypted images are shown in Fig. 8. The CCs of the two decrypted images are as high as 0.97722 and 0.96035, respectively, which shows that this color image encryption scheme is feasible and effective.

This color image encryption scheme can also be applied to the authentication systems introduced in Sections 4 and 5, because, except for the two steps of pre-processing and post-processing, other processes are exactly the same as grayscale images. To avoid excessive duplication, in the following sections only grayscale images will be used for simulation.

However, it should be noted that the phase retrieval based on the iteration algorithms will theoretically cause slightly information loss. The single-channel encryption scheme for color images we introduced in this paper also sacrifices the amount of information for less computation and storage cost. So this system is not suitable for image encryption scene which pursues the perfect decryption. However, it is very appropriate to apply it to ID card, certificate and other actual authentication systems, which only need a similarity between the decrypted and the original image as a criterion for passing through the systems or not.

4. Multilevel image authentication using shared secret threshold and phase retrieval[29]

Encryption and authentication are two important aspects of modern information security. The role of encryption system is to protect information from illegal intruders, while the role of authentication system is to verify messages.

Widely used in the information security, the (t, n) threshold secret sharing was first proposed by Shamir,[41] by which n participants will share the secret information but no valid information will be available unless at least t ($t \leq n$) participants are gathered. Combining this technique with the phase retrieval algorithm, a splendid multilevel authentication system is presented that can verify the accessibility of the original certification image with different privilege levels in the same system. The security of authentication system is improved to some extent by the addition of low-level authentication and secret sharing algorithm.

4.1. Theoretical analysis and description

4.1.1. Iterative phase retrieval algorithm

The fundamental structure of iterative phases generation is the same as that in Section 2, only without the input constraint.

Putting standard certification image $g(x,y)$ in the output plane, when illuminating the input plane with an on-axis plane wave of unit amplitude and wavelength λ, after the k-th iteration ($k = 1, 2, 3, \ldots$) the complex amplitude U^k in the output plane is[24,36]

$$U^k(x,y) = \mathrm{FrT}_{z_1}\{\mathrm{FrT}_{z_2}\{\exp[\mathrm{i}\,\psi_2^k(x_2,y_2)]\} \times \exp[\mathrm{i}\,\psi_1^k(x_1,y_1)]\}. \quad (9)$$

Suppose that the distributions of the two phase masks after k-th iteration are ψ_1^k and ψ_2^k, respectively, then in the $(k+1)$-th iteration process they can be described as[27]

$$\psi_1^{k+1}(x_1,y_1) = \arg\left(\frac{\mathrm{IFrT}_{z_1}\{g\exp[\mathrm{i}\arg(U^k)]\}}{\mathrm{FrT}_{z_2}[\exp(\mathrm{i}\,\psi_2^k)]}\right), \quad (10)$$

$$\psi_2^{k+1}(x_2,y_2) = \arg[\mathrm{IFrT}_{z_2}(\mathrm{IFrT}_{z_1}\{g\exp[\mathrm{i}\arg(U^k)]\} \times \exp(-\mathrm{i}\,\psi_1^{k+1}))]. \quad (11)$$

4.1.2. (t, n) threshold secret sharing algorithm based on Lagrange interpolating polynomial

The Lagrange interpolating polynomial is the basis of (t, n) threshold secret sharing algorithm. A polynomial f about x of degree $t-1$ is usually written as follows:[42–46]

$$f(x) = y + m_1 x + m_2 x^2 + \cdots + m_{t-1}x^{t-1}, \quad (12)$$

where y is a constant and $m_1, m_2, \ldots, m_{t-1}$ are $t-1$ random numbers.

To determine the t unknowns (that is, to find the unique solution), no less than t equations about x are needed. Thinking of each x_k and the corresponding value $f(x_k)$ satisfying Eq. (9) as a single point $(x_k, f(x_k))$, here k is a random integer within the interval of $[1, n]$, the n points $(x_1, f(x_1))$, $(x_2, f(x_2))$, $\ldots$, $(x_n, f(x_n))$ make up a point group G. In other words, t or more points in G are needed to obtain the value of y and $m_1, m_2, \ldots, m_{t-1}$ in a Lagrange interpolating polynomial of degree $t-1$.

For a secret sharing scheme, y could be viewed as the secret information, and the n points as n participants who hold their information. To retrieve the secret information, using t points from the n points in G we can solve the equation group and obtain the value of y:

$$y = (-1)^{t-1}\left[f(x_1)\frac{x_2x_3\cdots x_t}{(x_1-x_2)(x_1-x_3)\cdots(x_1-x_t)} + f(x_2)\frac{x_1x_3\cdots x_t}{(x_2-x_1)(x_2-x_3)\cdots(x_2-x_t)} + \cdots + f(x_t)\frac{x_1x_2\cdots x_{t-1}}{(x_t-x_2)(x_t-x_3)\cdots(x_t-x_{t-1})}\right]. \quad (13)$$

4.2. System designing process

A flow chart of the system designing is depicted in Fig. 9(a), and the specific implementation steps are as follows.

(i) Encode the standard certification image $g(x,y)$ into two phase masks ψ_1 and ψ_2 by the Fresnel domain iterative phase retrieval algorithm. This step is depicted in Fig. 9(b).

(ii) Store and upload the certification image $g(x,y)$, the geometrical parameters' keys (distances z_1 and z_2, wavelength λ), and the phase ψ_1 to the authentication center when the iterative cycle stops.

(iii) Select n plaintext images as camouflage images.

(iv) Decompose the phase mask ψ_2 in the input plane based on the (t, n) threshold secret sharing algorithm. This step is depicted in Fig. 9(c).

For this multilevel authentication system, each individual pixel value of ψ_2 can be viewed as a separate secret value y in a Lagrange interpolating polynomial f, which is to be divided into n parts. Treating the pixel values at the corresponding positions of the n camouflage images as the unknown variables x_1–x_n, the n corresponding values $f(x_1) \sim f(x_n)$ can be calculated from Eq. (10). It can be considered that this pixel value of ψ_2 is encrypted and divided into n parts. When all the pixel values of ψ_2 are encrypted by this method, n matrices can be obtained, and they are called secret-key-carrier (SKC) images.

(v) Distribute the n SKC images to n different participants of the authentication system to realize secret sharing, with the corresponding camouflage images used as auxiliary tools.

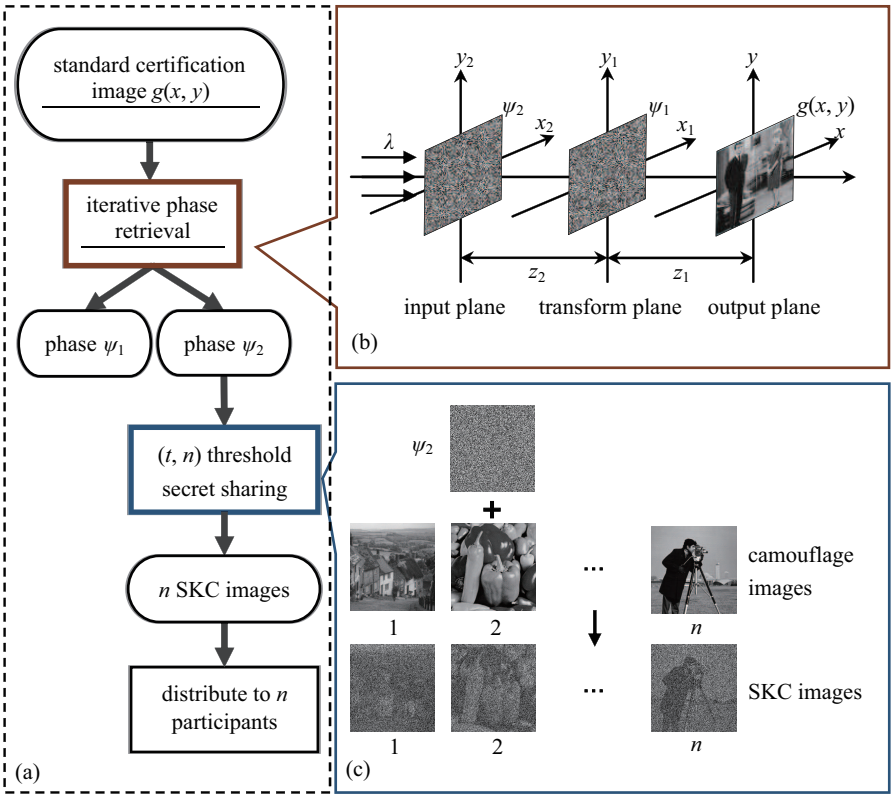


Fig. 9. (a) Flow chart of designing system, (b) schematic diagram of iterative phase retrieval algorithm, and (c) schematic diagram of (t, n) threshold secret sharing algorithm.

4.3. Authentication process

In an authentication system, the level of authentication generally corresponds to the level of privilege. In this image authentication system, the matching degree between decrypted image and the standard certification image determines the the level of authentication. The CC and NCC are the main criteria for determining the privilege level of authenticators. The flow chart of the authentication process is depicted in Fig. 10(a).

4.3.1. High-level authentication

The principle of (t, n) threshold secret-sharing algorithm described in Subsection 4.1.2 shows that only by gathering at least t $(t \leq n)$ authenticators with their SKC images can the phase key ψ_2' be retrieved, and passed by the authentication system. The process of high-level authentication is shown in Fig. 10(b), and the specific implementation steps are as follows.

i) Any t authenticators input their SKC images into the authentication system.

ii) The system recovers phase ψ_2' according to the (t, n) threshold secret sharing algorithm.

iii) With the geometrical keys, the original phase ψ_1 and recovered ψ_2', the authentication center reconstructs the optical path and obtains the reconstructed image g', which is de-

scribed mathematically as

$$g' = \mathrm{abs}(\mathrm{FrT}_{z_1}\{\mathrm{FrT}_{z_2}[\exp(i\psi_2')]\exp(\mathrm{i}\psi_1)\}), \quad (14)$$

where 'abs' denotes the operator for obtaining the real amplitude.

iv) The authentication center calculates the CC between the reconstructed image g' and the standard certification image g. Serving as a criterion for determining the success of high-level authentication, if it is higher than a preset threshold, the authentication is successful, otherwise it means a failure.

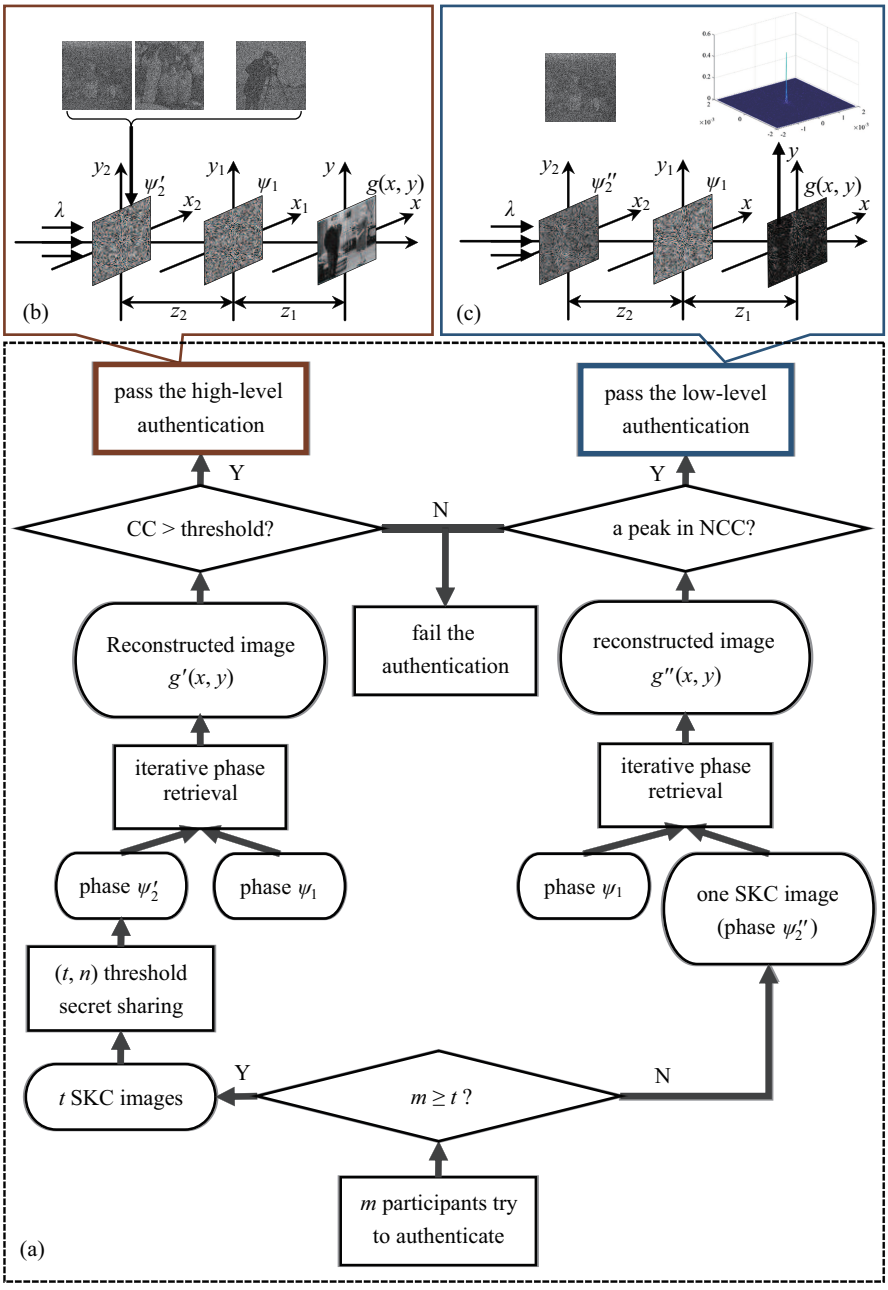


Fig. 10. Flow chart of (a) authentication process, (b) high-level authentication process, and (c) low-level authentication process.

4.3.2. Low-level authentication

We have known that it is impossible to pass the high-level authentication without gathering t ($t \leq n$) participants, while this system provides additional low-level authentication for the correct single authenticator. Nonlinear correlation coefficient (NCC) is introduced as an auxiliary criterion for determining the success of low-level authentication. The NCC is defined as follows:[26,46]

$$\mathrm{NCC}(\xi,\eta) = |\mathrm{IFT}(|\{\mathrm{FT}[g(\xi,\eta)]\}\{\mathrm{FT}[g''(\xi,\eta)]\}|^{\omega-1} \times \{\mathrm{FT}[g(\xi,\eta)]\}\{\mathrm{FT}[g''(\xi,\eta)]\})|^2, \quad (15)$$

where FT and IFT respectively represent the Fourier and inverse Fourier transform, and (ξ, η) is the coordinate of the spectrum transverse plane. The parameter ω defines the strength of the applied nonlinearity whose range is [0.2, 0.4].

The process of low-level authentication is depicted in Fig. 10(c), and the specific implementation steps are as follows.

(I) An authenticator inputs his SKC image into the authentication system.

(II) With the geometrical keys, the original phase ψ_1 and the SKC image treated as ψ_2'', the authentication center reconstructs the optical path and obtains the reconstructed image g''.

(III) Calculate and display the three-dimensional (3D) NCC distribution between g and g''. If there is a peak at the center, the system determines that the low-level authentication is successful. If the NCC distribution is of noise-like pulses, the low-level authentication process fails.

4.4. Computer simulations and discussion

Taking (3, 5) threshold secret sharing algorithm for example, the feasibility and performance of the system are verified by computer simulation. The original certification image and the phase distribution (ψ_1 and ψ_2) generated by phase retrieval algorithm after 200 iterations are, respectively, depicted in Figs. 11(a)–11(c). Five pre-selected grayscale camouflage images 'Goldhill', 'Peppers', 'Airplane', 'Baboon', and 'Cameraman' are depicted in Fig. 12(a), the corresponding SKC images of which are calculated by the method mentioned in Subsection 4.1.2 and shown in Fig. 12(b).

We first test the high-level authentication. As the criterion of the high-level authentication, the threshold of the CC between the recovered image g' and the standard certification image g is set to be 0.90. Three correct SKC images are randomly selected in order to retrieve the phase key ψ_2'. The simulation result is shown in Fig. 13(a), and the CC is as high as 0.99452, which means that the high-level authentication is successful.

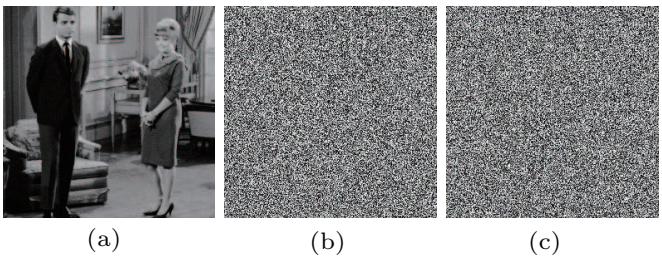


Fig. 11. (a) Original certification image, ((b) and (c)) two phase distributions (ψ_1 and ψ_2) iteratively generated by phase retrieval algorithm after 200 iterations.

We further test the low-level authentication. The parameter ω in NCC is set to be 0.4. A correct SKC image is randomly selected as retrieved phase key ψ_2'', and the CC between the final recovered image and the standard certification is 0.30885, which cannot pass the high-level authentications. However, the NCC distribution is shown in Fig. 13(b), in which the remarkable peak can be observed. This means that the low-level authentication is successful.

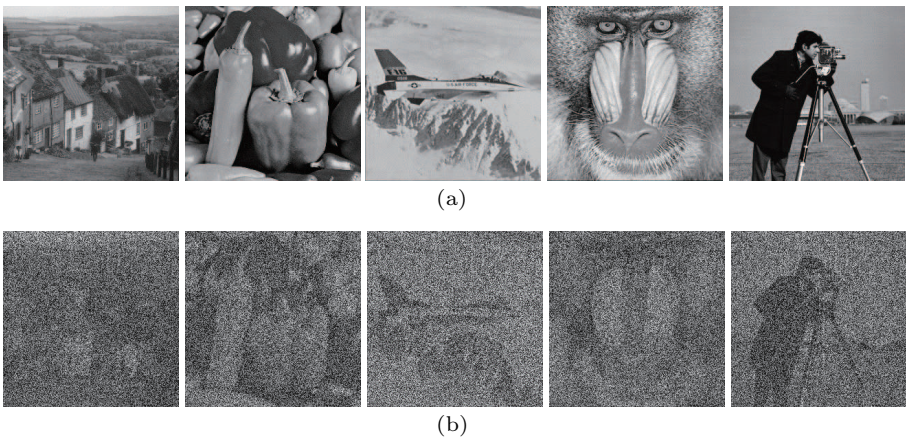


Fig. 12. (a) Five meaningful camouflage images pre-selected. (b) Corresponding SKC images.

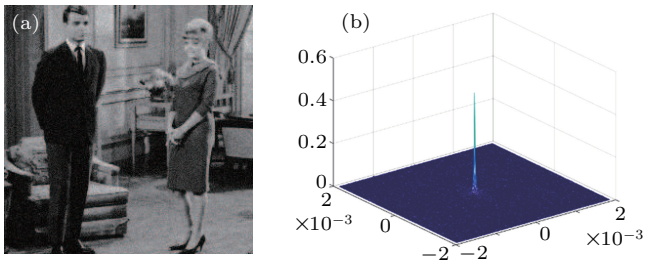


Fig. 13. (a) Simulated result in high-level authentication, and (b) NCC distribution of retrieved image in low-level authentication and corresponding standard certification image.

If any SKC images involved in the authentication process are incorrect, then neither the high-level nor low-level authentications will pass, no clear certification will be recovered in the output plane and no remarkable peak will be generated in the NCC distribution either.[29]

But this system is not perfect. Besides the limitations mentioned in Subsection 3.2, the main shortcoming is the large space cost. Every participant in the authentication system needs a camouflage image as an auxiliary tool besides the SKC image held as the key, which means that the authenti-

cation center needs a large space to store camouflage image database.

5. Hierarchical multilevel authentication system for multiple-image based on phase retrieval and basic vector operations[32]

Basic vector operations were first applied to optical encryption by Deng *et al.* in 2015.[47] The authors designed a (2, n) threshold secret sharing scheme based on basic vector operations and coherence superposition, but only binary images are suitable for their scheme. The system introduced in this section improves Deng's method and combines basic vector operations with phase retrieval algorithm, and present a kind of hierarchical multilevel authentication system, so that both binary and grayscale images are suitable for this authentication system (color images are also applicable to the system by using the single-channel encryption scheme introduced in Subsection 2.2), and the same system can provide multiple privileges, each privilege can also provide multiple levels.

5.1. Theoretical analysis and description

5.1.1. Iterative phase retrieval algorithm

The fundamental structure of hierarchical image encryption based on phase retrieval is similar to that in Section 3. But only one phase mask is updated for each level of encryption, except for the 1-level encryption.

As shown in Fig. 14, for the N-level ($N>1$) encryption, a total of $N+1$ cascaded phase masks ψ_0–ψ_N are involved in encrypting it. In the encryption process, phase masks ψ_0–ψ_{N-1} retain the iteration results of the preceding authentication levels, while a new phase mask ψ_N at plane (x_N, y_N) is added to encode the N-level certification image $g_N(x,y)$ located in the output plane, and the phase distribution of which will be adjusted in each iteration. After the k-th iteration ($k=1, 2, 3, \ldots$), the complex amplitude U^k in the output plane is[27]

$$U_N^k(x,y) = \mathrm{FrT}_{z_0}\{\mathrm{FrT}_{z_1}[(\cdots \mathrm{FrT}_{z_{N-1}}\{\mathrm{FrT}_{z_N}[\exp(\mathrm{i}\psi_N^k)] \times \exp(\mathrm{i}\psi_{N-1})\}\cdots)\exp(\mathrm{i}\psi_1)]\exp(\mathrm{i}\psi_0)\}. \quad (16)$$

Then, in the $(k+1)$-th iteration process, the distribution of phase mask ψ_N will be adjusted to

$$\psi_N^{k+1} = \arg(\mathrm{IFrT}_{z_N}\{[\cdots \mathrm{IFrT}_{z_1}(\mathrm{IFrT}_{z_0}\{g_N \exp[\mathrm{i}\arg(U_N^k)]\} \times \exp(-\mathrm{i}\psi_0))\cdots]\exp(-\mathrm{i}\psi_{N-1})\}). \quad (17)$$

As for the 1-level encryption, phase masks ψ_0 and ψ_1 are adjusted simultaneously in each iteration, so in the k-th step ($k=1, 2, 3, \ldots$) iteration, the output image can be mathematically expressed as[27]

$$U_1^k(x,y) = \mathrm{FrT}_{z_0}\{\mathrm{FrT}_{z_1}[\exp(\mathrm{i}\psi_1^k)]\exp(\mathrm{i}\psi_0^k)\}. \quad (18)$$

Then, in the $(k+1)$-th iteration process, the distribution of phase masks ψ_0 and ψ_1 would be adjusted respectively to[27]

$$\psi_0^{k+1} = \arg[\frac{\mathrm{IFrT}_{z_0}(g_1\{\exp[\mathrm{i}\arg(U_1^k)]\})}{\mathrm{FrT}_{z_1}[\exp(\mathrm{i}\psi_1^k)]}], \quad (19)$$

$$\psi_1^{k+1} = \arg\left[\mathrm{IFrT}_{z_1}(\mathrm{IFrT}_{z_0}\{g_1 \exp[\mathrm{i}\arg(U_1^k)]\} \times \exp(-\mathrm{i}\psi_0^{k+1}))\right]. \quad (20)$$

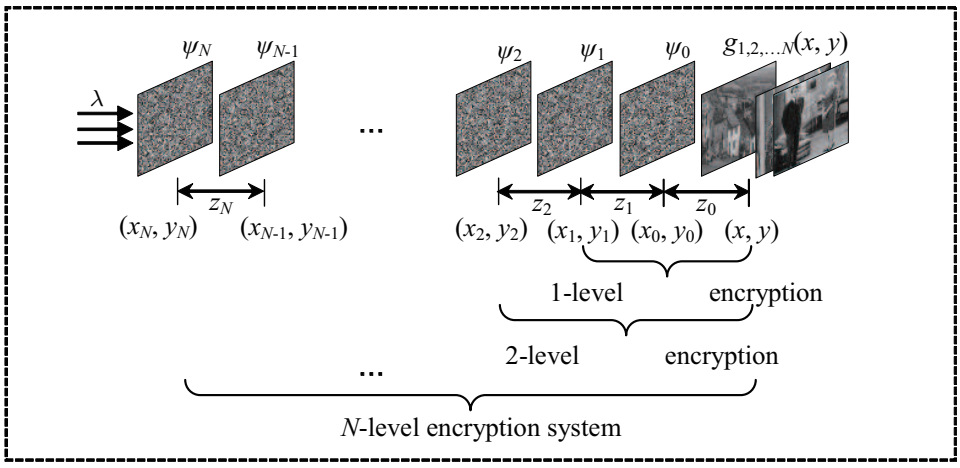


Fig. 14. Schematic diagram of iterative phase retrieval encoding in designing N-level authentication system.

5.1.2. Secret sharing algorithm based on basic vector operations[47–50]

Vector $\boldsymbol{G}_1$ which can be viewed as a position vector in a 2D Cartesian coordinate system, is shown in Fig. 15. Assuming the modulus of $\boldsymbol{G}_1$ is G and the argument θ_1, then $\boldsymbol{G}_1$ can be written as $G\exp(\mathrm{i}\theta_1)$. $\boldsymbol{Z}_0$ is a unit vector, whose argument θ_0 can be selected randomly. Based on the rule of basic vector decomposition, the subtraction vector $\boldsymbol{Z}_1$ of $\boldsymbol{G}_1$ and $\boldsymbol{Z}_0$, can be expressed as[32]

$$\boldsymbol{Z}_1 = \boldsymbol{G}_1 - \boldsymbol{Z}_0 = G\exp(\mathrm{i}\theta_1) - \exp(\mathrm{i}\theta_0). \quad (21)$$

Rotate $\boldsymbol{G}_1$ around the origin in the coordinate system, a new vector $\boldsymbol{G}_2$ can be generated, whose modulus is the same as $\boldsymbol{G}_1$ and argument is θ_2, which can be denoted as $G\exp(\mathrm{i}\theta_2)$. The $\boldsymbol{G}_2$ can also be seen as the sum vector of $\boldsymbol{Z}_2$ and $\boldsymbol{Z}_0$ as shown in Fig. 15, which can be described as

$$\boldsymbol{G}_2 = G\exp(\mathrm{i}\theta_2) = \boldsymbol{Z}_2 + \boldsymbol{Z}_0, \tag{22}$$

repeating a similar process for n ($n = 1, 2, 3, \ldots$) iterations, a series of vectors

$$\begin{aligned}
\boldsymbol{G}_1 &= G\exp(\mathrm{i}\theta_1) = \boldsymbol{Z}_1 + \boldsymbol{Z}_0,\\
\boldsymbol{G}_2 &= G\exp(\mathrm{i}\theta_2) = \boldsymbol{Z}_2 + \boldsymbol{Z}_0,\\
\boldsymbol{G}_3 &= G\exp(\mathrm{i}\theta_3) = \boldsymbol{Z}_3 + \boldsymbol{Z}_0,\\
&\vdots\\
\boldsymbol{G}_\mathrm{n} &= G\exp(\mathrm{i}\theta_n) = \boldsymbol{Z}_\mathrm{n} + \boldsymbol{Z}_0,
\end{aligned} \tag{23}$$

can be generated, where θ_i ($i = 1, 2, \ldots, n$) are the corresponding arguments, $\boldsymbol{Z}_i$ ($i = 1, 2, \ldots, n$) are the corresponding subtraction vectors of $\boldsymbol{G}_i$ ($i = 1, 2, \ldots, n$) and $\boldsymbol{Z}_0$.

For a secret sharing scheme, the modulus G could be viewed as the secret information. With preselected θ_1–θ_n and $\boldsymbol{Z}_0$, it is easy to calculate corresponding $\boldsymbol{Z}_1$–$\boldsymbol{Z}_n$ and divide them into two parts: amplitude and phase. These information constitutes n pairs of keys, which could be distributed to n different participants to realize the secret sharing.

When reconstructing the secret information G, at least two pairs of keys are needed. For example, the recovery procedure with $\boldsymbol{Z}_j$ and $\boldsymbol{Z}_k$ ($j, k = 1, 2, \ldots, n$, $j \neq k$) can be mathematically expressed as[32]

$$\begin{aligned}
|\boldsymbol{G}_j - \boldsymbol{G}_k|^2 &= |\boldsymbol{Z}_j - \boldsymbol{Z}_k|^2\\
&= |G\exp(\mathrm{i}\theta_j) - G\exp(\mathrm{i}\theta_k)|^2\\
&= 2G[1 - \cos(\theta_j - \theta_k)].
\end{aligned} \tag{24}$$

Deduced from Eq. (19), the result can be expressed as

$$G = \frac{|\boldsymbol{Z}_j - \boldsymbol{Z}_k|^2}{2[1 - \cos(\theta_j - \theta_k)]}. \tag{25}$$

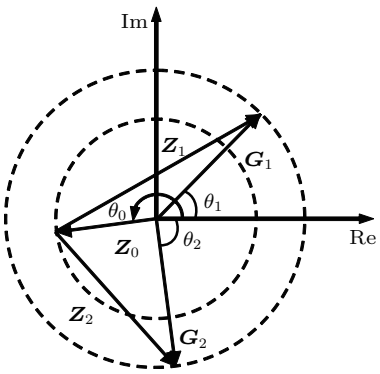


Fig. 15. Schematic diagram of basic vector operation.

The coefficient $(1/2)[1 - \cos(\theta_j - \theta_k)]$ is a constant which has little effect on the result, especially in image encryption, which might be negligible as the resulted pixel numbers are usually normalized in the end.

5.2. System designing process

The flow chart of the integrated system designing process is depicted in Fig. 16. The specific implementation steps are as follows.

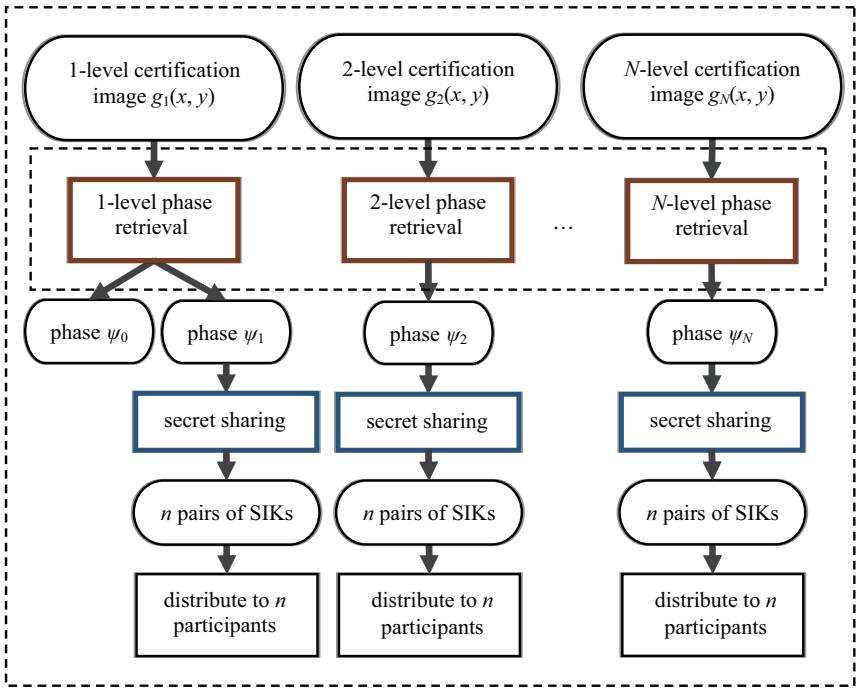


Fig. 16. Flow chart of integrated system designing process.

I) Encode the certification images $g_{1,2,\ldots,N}(x,y)$ into phase masks ψ_0–ψ_N by the N-level iterative phase retrieval algorithm. This step is depicted in Fig. 14.

II) Store and upload the certification images $g_{1,2,\ldots,N}(x,y)$, the geometrical parameters keys (distances $z_1 \sim z_2$, wavelength λ), and phase information ψ_0 in the authentication center database.

III) Randomly select $\theta_1 \sim \theta_n$ and Z_0.

IV) Split phase masks ψ_1–ψ_N according to the secret sharing algorithm based on the basic vector operations.

The strategy of secret sharing in the system is similar to that described in Section 4, each individual pixel value of ψ_1–ψ_N can be viewed as modulus G. Therefore, any one of the phase masks ψ_1–ψ_N can be encrypted into n pairs of shadow images keys (SIKs), and each pair of SIKs consists of an amplitude-type SIK and a phase-type SIK. This step is depicted in Fig. 17.

V) Distribute the n pairs of SIKs at each level of the system to n different participants to realize secret sharing.

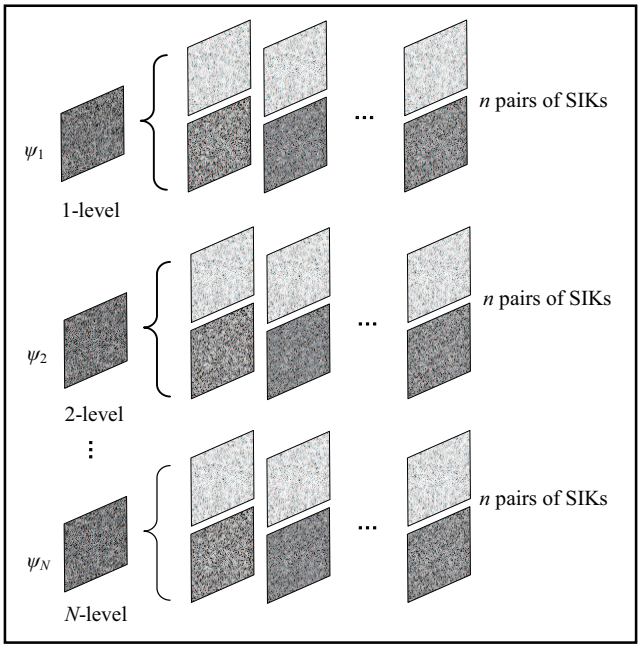


Fig. 17. Schematic diagram of secret sharing in designing N-level authentication system.

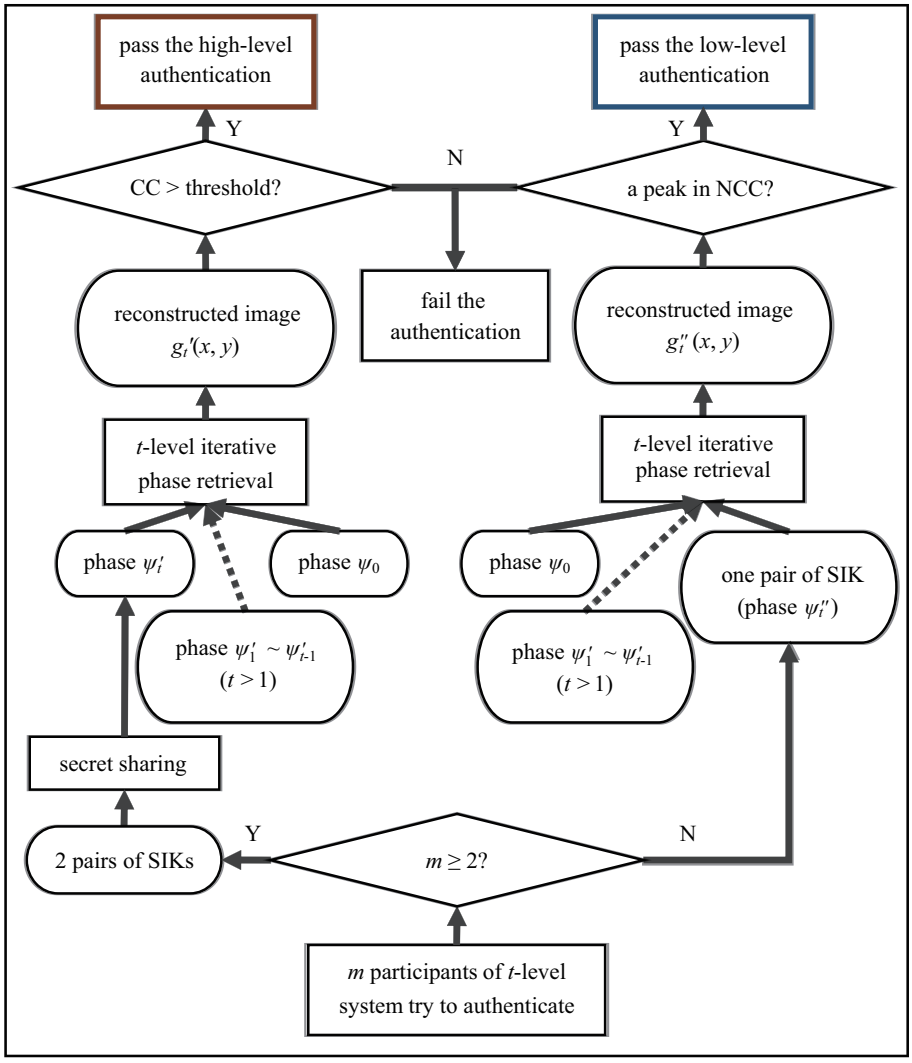


Fig. 18. Flow chart of authentication process.

It is worth noting that in this system the distribution of privileges is in order of security level from low to high, This means that authenticators at higher levels of the authentication system will possess all phase keys at lower levels, they can access the information from lower levels if they want, but they cannot pass the high-level authentication at their own level of the system.

5.3. Authentication process

The authentication process of this hierarchical multilevel authentication system is similar in principle to that of the system introduced in Section 4. The CC and NCC are also used as the main criteria for determining the privilege level of authenticators. We take the t-level ($t = 1, 2, \ldots, N$) system for example to illustrate the authentication process, and the flow chart is depicted in Fig. 18.

5.3.1. High-level authentication

The principle of the secret sharing algorithm based on basic vector operations mentioned in Subsection 5.1.2 shows that for any level of the system, only by gathering at least two participants with their SIKs will the high-level authentication be passed. The process of high-level authentication is shown in Fig. 19, and the specific implementation steps of authenticating the t-level ($t = 1, 2, \ldots, N$) system are as follows.

1) Any two authenticators input their SIKs into the authentication system.

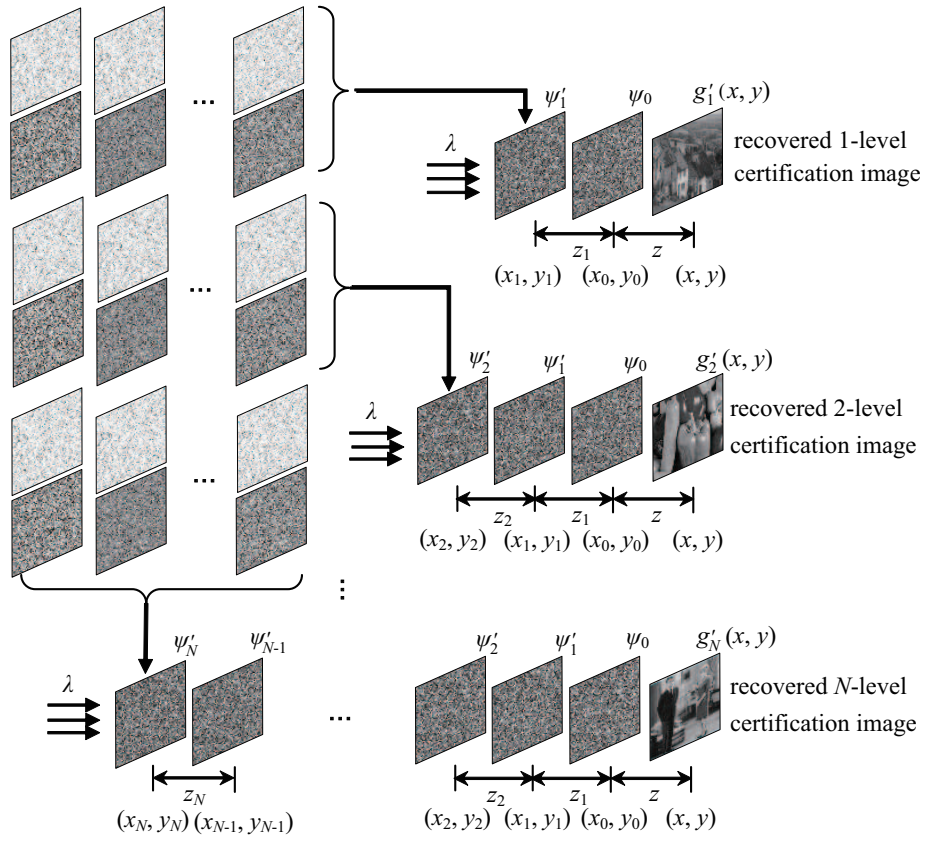


Fig. 19. High-level authentication process.

2) The system recovers phase ψ_t' according to the secret sharing algorithm based on basic vector operations.

3) With the geometrical keys, the original phase ψ_0, phase ψ_1'–ψ_{t-1}' (if $t > 1$) and recovered ψ_t', the authentication center reconstructs the optical path and obtains the reconstructed image g_t'.

As described above, to recover all the N certification images, the higher level authenticators should possess phase keys of all lower levels of the authentication system. The higher the level of authentication system is, the more keys are required.

4) The authentication center calculate the CC between the reconstructed image g_t' and the standard certification image g_t. If it is higher than a preset threshold, the authentication is successful, otherwise it means a failure.

5.3.2. Low-level authentication

The process of low-level authentication is depicted in Fig. 20, and the specific implementation steps of authenticating the t-level ($t = 1, 2, \ldots, N$) system are as follows.

a) An authenticator inputs his pair of SIK into the authentication system.

b) With the geometrical keys, the original phase ψ_0, phase $\psi_1' \sim \psi_{t-1}'$ (if $t > 1$), and ψ_2'' which is recovered from only one pair of SIK, the authentication center reconstructs the optical path and obtains the reconstructed image g_t''.

c) Calculate and display the 3D NCC distribution between g_t and g_t''. If there is a peak in the center, the system determines that the low-level authentication is successful. If not, the low-level authentication process fails.

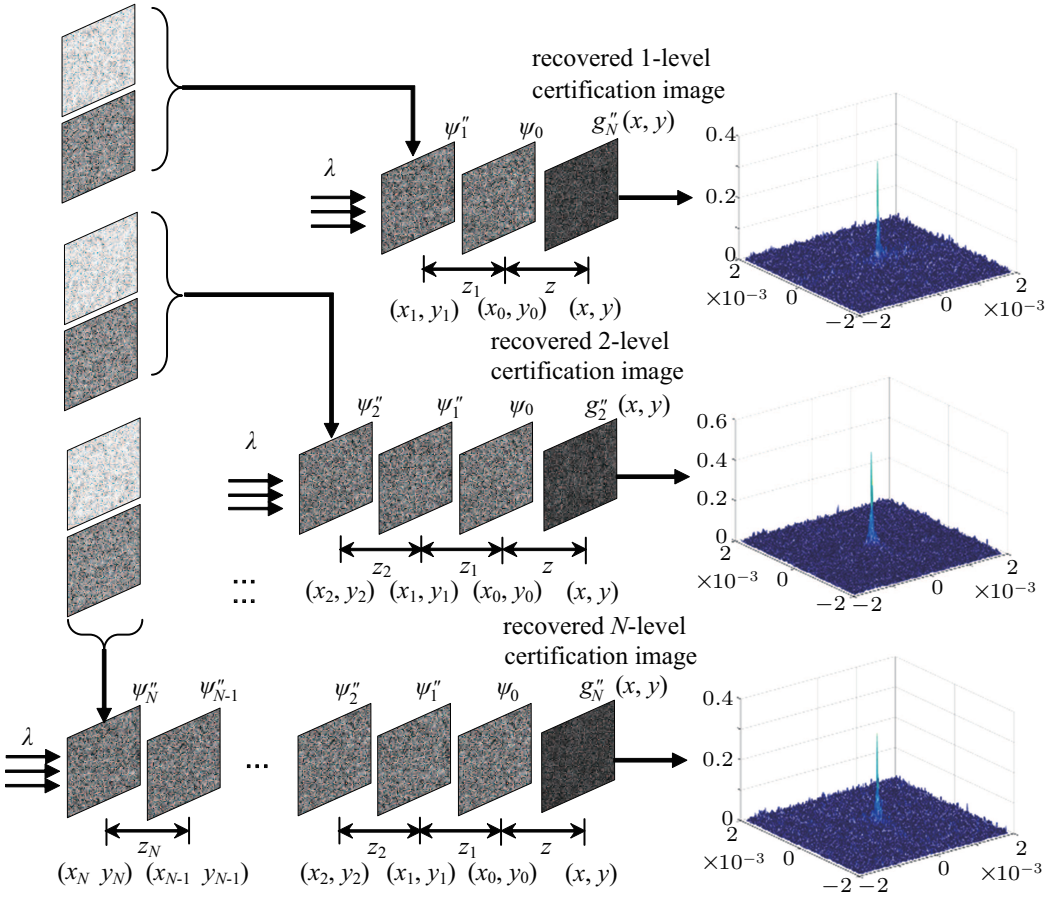


Fig. 20. Low-level authentication process.

5.4. Computer simulations and discussion

Taking the 4-level image encryption system for example, the feasibility and performance of the system are verified by computer simulation. We use the four greyscale images 'Goldhill', 'Peppers', 'Lena' and 'Couple' as standard certification images, and they are respectively depicted in Figs. 5(a)–5(d). To realize the secret sharing algorithm by basic vector operations, one random phase mask $\arg(\boldsymbol{Z}_0)$ and four initial random phase masks ψ_0–ψ_4 for designing the $1^{st} \sim 4^{th}$ level authentication systems have also been selected beforehand. After 500 iterations, phase distributions ψ_1–ψ_4 iteratively generated are shown in Fig. 21. Then each iteratively generated phase key is encrypted into 4 pairs of SIKs and distributed to four different participants based on the secret sharing algorithm by the basic vector operations mentioned in Subsection 5.1.2. Because all the SIKs split from ψ_1–ψ_4 are similar, here we just take 1-level authentication system for example to show the four pairs of SIKs split from phase key ψ_1, and they are illustrated in Fig. 22.

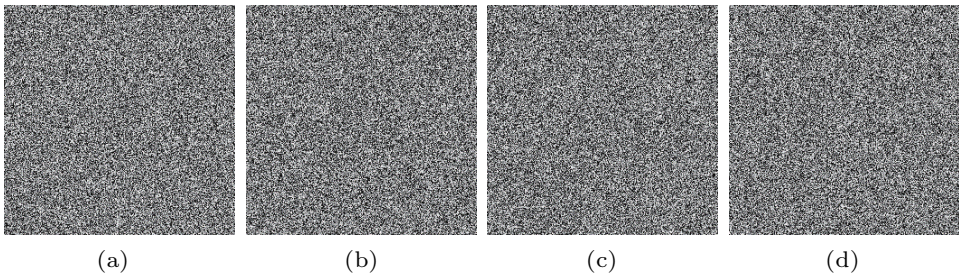


Fig. 21. Phase distributions (ψ_1–ψ_4) iteratively generated by the phase retrieval algorithm after 500 iterations.

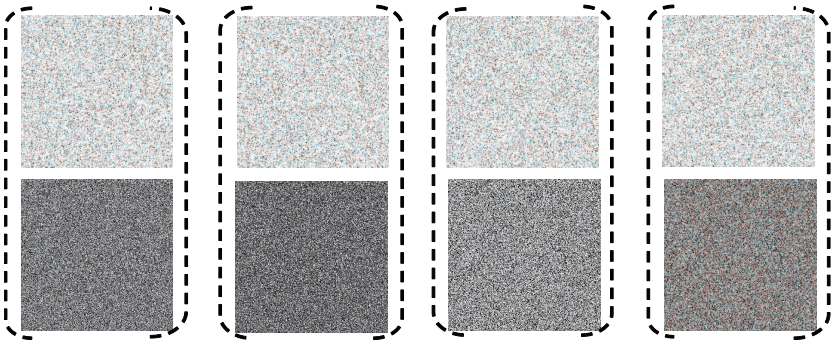


Fig. 22. Four pairs of SIKs split from phase information ψ_1.

We first test the high-level authentication. The threshold of the CC between the recovered image and the standard certification image is set to 0.90. We randomly select two pairs of SIKs at each level to retrieve the phase key ψ_1'–ψ_4'. Based on the process mentioned in Subsection 5.3.1, the simulation results of high-level authentication and their corresponding CCs are shown in Table 2. It is obvious that the high-level authentication of all the 4 security levels of the system are successful.

We further test the low-level authentication. The parameter ω in NCC is set to be 0.4. Only one pair of SIKs is randomly selected at each level of the authentication systems to retrieve the phase key ψ_1''–ψ_4''. The CCs between the final recovered images and the standard certification images are 0.11136, 0.10358, 0.08863, and 0.11368, respectively, none of which can pass the high-level authentications. However, the NCC distributions of them are shown in Figs. 23(a)–23(d), in which the remarkable peaks can be observed. This means that the low-level authentication is successful.

Table. 2 Four simulated results of high-level authentication and their corresponding CCs.

Recovered image				
	Goldhill	Peppers	Lena	Couple
CC	1.00000	0.99895	0.99813	0.99807

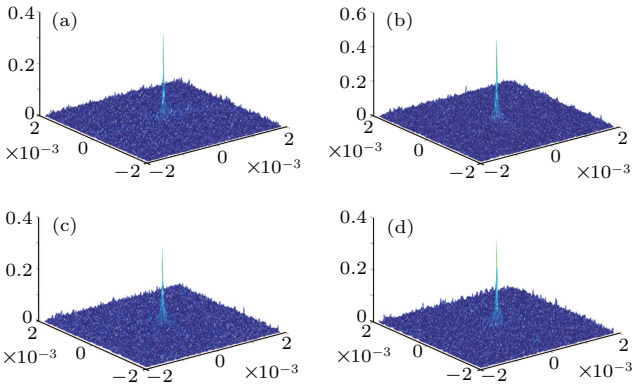


Fig. 23. NCC distributions of final retrieved images in low-level authentication and their corresponding standard certification images.

If any SIKs involved at each level of the authentication process are incorrect, both the high-level and the low-level authentications will be not passed, that is, no clear certification images will be recovered and no remarkable peaks will be generated in the NCC distributions.[32]

The secret sharing algorithm in this system is different from that in Section 4. Because θ_1–θ_n and Z_0 used for secret sharing are randomly selected, and they are not needed for subsequent image restoration in high-level authentication, this saves space for storing them. Compared with Section 3, the reduction of phase masks in the phase retrieval also saves storage space. These advantages contribute to the formation of the hierarchical multilevel authentication system. However, the secret sharing algorithm based on basic vector operations is actually a kind of (2, n) threshold secret sharing algorithm. In other words, no matter how large the value of n is, only two authenticators are needed to realize the high-level authentication, which lacks flexibility to some extent.

We also test the authentication time. The time cost of the high-level authentication of the 1st–4th level system are 0.07 s, 0.08 s, 0.09 s and 0.10 s, respectively. Both theoretical

description and simulation results show that with the increase of the level of authentication system, the authentication time increases. The authentication time of the 4th level system already exceeds 0.10 s. Time cost may be a future improvement of the system.

6. Conclusions

In this paper, we review the phase retrieval algorithms for optical information security, including optical encryption and authentication. Three typical phase retrieval algorithms are presented and discussed, and theoretical principles and application examples are correspondingly demonstrated for each phase-retrieval-based optical information security. The three phase retrieval algorithms reviewed here can effectively show a picture about phase-retrieval-based optical information security. Significant advantages of each phase-retrieval-based optical information security system are analyzed. It is hoped that this review will provide a picture of the current developments of phase retrieval algorithms for optical information security and will also shed light on the future developments of phase retrieval algorithms for optical information security.

References

[1] Zhang X P, Guo R, Chen H W, Zhao Z M and Wang J Y 2018 *Chin. Phys. B* **27** 080701
[2] Wang X Y, Wang Y, Wang S W, Zhang Y Q and Wu X J 2018 *Chin. Phys. B* **27** 110502
[3] Javidi B, Carnicer A, Yamaguchi M et al 2016 *J. Opt.* **18** 083001
[4] Chen W 2016 *IEEE Photon. J.* **8** 1
[5] Wang X G, Chen W and Chen X D 2015 *Opt. Express* **23** 6239
[6] Li T and Shi Y S 2016 *Chin. Phys. Lett.* **33** 014206
[7] Chen W 2018 *Appl. Opt.* **57** 1196
[8] Chen W 2017 *Appl. Opt.* **56** 9126
[9] Chen W and Chen X D 2016 *Appl. Opt.* **55** 6740
[10] Meng X F, Cai L Z, Xu X F, Yang X L, Shen X X, Dong G Y and Wang Y R 2006 *Opt. Lett.* **31** 1414
[11] Meng X F, Cai L Z, Wang Y R, Yang X L, Xu X F, Dong G Y and Shen X X 2009 *Opt. Laser Eng.* **47** 96
[12] Zhang X, Meng X F, Wang Y R, Yang X L and Yin Y K 2018 *Chin. Phys. B* **27** 074205
[13] Chen W 2017 *Opt. Express* **25** 16509
[14] Chen W 2016 *IEEE Photon. Technol. Lett.* **28** 1932
[15] Chen W 2016 *IEEE Photon. Technol. Lett.* **28** 540
[16] Chen W and Chen X D 2015 *Europhys. Lett.* **110** 44002
[17] Chen W and Chen X D 2014 *Appl. Phys. Lett.* **104** 251109
[18] Chen W and Chen X D 2013 *Opt. Lett.* **38** 546
[19] Chen W and Chen X D 2013 *Appl. Phys. Lett.* **103** 221106
[20] Chen W, Situ G H and Chen X D 2013 *Opt. Express* **21** 24680
[21] Chen W 2015 *Appl. Opt.* **54** 10711
[22] Wang R K, Watson I A and Chatwin C R 1996 *Opt. Eng.* **35** 2464
[23] Situ G H, Zhang J J, Zhang Y and Zhao Z S 2004 *J. Optoelectron. Laser* **15** 341 (in Chinese)
[24] Situ G H and Zhang J J 2004 *Opt. Commun.* **232** 115
[25] Huang J J, Hwang H E, Chen C Y and Chen C M 2012 *Appl. Opt.* **51** 2388
[26] Chen W, Chen X D, Stern A and Javidi B 2013 *IEEE. Photon. J.* **5** 6900113
[27] Meng X F, Cai L Z, Wang Y R, Yang X L, Xu X F, Dong G Y, Shen X X, Zhang H and Cheng X C 2007 *J. Opt. A-Pure Appl. Opt.* **9** 1070
[28] Fan D S, Meng X F, Wang Y R, Yang X L, Peng X, He W Q, Dong G Y and Chen H Y 2013 *Appl. Opt.* **52** 5645
[29] Pan X M, Meng X F, Wang Y R, Yang X L, Peng X, He W Q, Dong G Y, Chen and H Y 2014 *J. Mod. Opt.* **61** 1470
[30] Fan D S, Meng X F, Wang Y R, Yang X L, Pan X M, Peng X, He W Q, Dong G Y and Chen H Y 2015 *Appl. Opt.* **54** 3204
[31] Pan X M, Meng X F, Wang Y R, Yang X L, Peng X, He W Q, Dong G Y and Chen H Y 2016 *J. Mod. Opt.* **63** 632
[32] Li X Y, Meng X F, Yin Y K, Yang X L, Wang Y R, Peng X, He W Q, Pan X M, Dong G Y and Chen H Y 2017 *Opt. Laser Eng.* **89** 59
[33] Li X Y, Meng X F, Wang Y R, Yang X L, Yin Y K, Peng X, He W Q, Dong G Y and Chen H Y 2017 *Opt. Laser Eng.* **96** 7
[34] Fienup J R 1982 *Appl. Opt.* **21** 2758
[35] Rosen J 1993 *Opt. Lett.* **18** 1183
[36] Meng X F, Cai L Z, Yang X L, Shen X X and Dong G Y 2006 *Appl. Opt.* **45** 3289
[37] He M Z, Cai L Z, Liu Q, Wang X C and Meng X F 2005 *Opt. Commun.* **247** 29
[38] Chang H T, Lu W C and Kuo C J 2002 *Appl. Opt.* **41** 4825
[39] Liu Z Y, Xia T C and Wang J B 2018 *Chin. Phys. B* **27** 030502
[40] Yuk C K M, Au O C, Li R Y M and Lam S Y 2007 *IEEE International Symposium on Circuits & Systems*, May 27–30, 2007, New Orleans, LA, USA, p. 4
[41] Chen Y, Liu Q, Wang J and Wang Q H 2017 *Opt. Eng.* **56** 123106
[42] Shamir A 1979 *Commun. ACM* **22** 612
[43] Lin C C and Tsai W H 2004 *J. Syst. Software* **73** 405
[44] Liu Z J, Ahmad M A and Liu S T 2008 *Opt. Commun.* **281** 5322
[45] Islam N, Puech W, Hayat K and Brouzet R 2011 *Opt. Commun.* **284** 4412
[46] Chen W, Javidi B, Chen and X 2014 *Adv. Opt. Photon.* **6** 120
[47] Deng X P, Wen W, Mi X W and Long X W 2015 *Opt. Commun.* **341** 22
[48] Wang X G and Zhao D M 2011 *Opt. Commun.* **284** 945
[49] Chen L F, Liu J Y, Wen J S, Mao H D, Ge F and Zhao D M 2015 *Opt. Commun.* **338** 110
[50] Chen L F, Liu J Y, Wen J S, Gao X, Mao H D, Shi X Y and Qu Q L 2015 *Opt. Laser Technol.* **69** 80