


# Optical encryption scheme based on spread spectrum ghost imaging

Jin-Fen Liu(刘进芬), Yue Dong(董玥), Le Wang(王乐), and Sheng-Mei Zhao(赵生妹)

**Citation:**Chin. Phys. B, 2023, 32 (**7**): 074202. DOI: 10.1088/1674-1056/acbf27
Journal homepage: http://cpb.iphy.ac.cn; http://iopscience.iop.org/cpb

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

---

## Deep-learning-based cryptanalysis of two types of nonlinear optical cryptosystems

Xiao-Gang Wang(汪小刚) and Hao-Yu Wei(魏浩宇)
Chin. Phys. B, 2022, 31 (**9**): 094202. DOI: 10.1088/1674-1056/ac6331

## 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)
Chin. Phys. B, 2019, 28 (**8**): 084203. DOI: 10.1088/1674-1056/28/8/084203

## Optical encryption of multiple three-dimensional objects based on multiple interferences and single-pixel digital holography

Ying Wang(王莹), Qi Liu(刘琦), Jun Wang(王君), Qiong-Hua Wang(王琼华)
Chin. Phys. B, 2018, 27 (**3**): 034202. DOI: 10.1088/1674-1056/27/3/034202

## Optical encryption scheme based on ghost imaging with disordered speckles

Yu-dong Zhang(张玉东), Sheng-mei Zhao(赵生妹)
Chin. Phys. B, 2017, 26 (**5**): 054205. DOI: 10.1088/1674-1056/26/5/054205

## An encryption scheme based on phase-shifting digital holography and amplitude-phase disturbance

Hua Li-Li (花丽丽), Xu Ning (徐宁), Yang Geng (杨庚)
Chin. Phys. B, 2014, 23 (**6**): 064201. DOI: 10.1088/1674-1056/23/6/064201

---

# Optical encryption scheme based on spread spectrum ghost imaging

Jin-Fen Liu(刘进芬)[1,2], Yue Dong(董玥)[1], Le Wang(王乐)[1], and Sheng-Mei Zhao(赵生妹)[1,†]

[1] *Institute of Signal Processing and Transmission, Nanjing University of Posts and Telecommunications, Nanjing* 210003, *China*
[2] *NanJing Tech University Pujiang Institute, Nanjing* 211222, *China*

(Received 15 November 2022; revised manuscript received 21 February 2023; accepted manuscript online 27 February 2023)

An optical encryption (OE) scheme based on the spread spectrum ghost imaging (SSGI), named as SSGI-OE, is proposed to obtain a high security with a smaller key. In the scheme, the randomly selected row number of a Hadamard matrix of order $N$ is used as the secure key, and shared with the authorized user, Bob, through a private channel. Each corresponding row vector of the order-$N$ Hadamard matrix is then used as the direct sequence code to modulate a speckle pattern for the ghost imaging system, and an image is encrypted with the help of the SSGI. The measurement results from the bucket detector, named as ciphertext, are then transmitted to Bob through a public channel. The illuminating speckle patterns are also shared with Bob by the public channel. With the correct secure key, Bob could reconstruct the image with the aid of the SSGI system, whereas the unauthorized user, Eve, could not obtain any useful information of the encrypted image. The numerical simulations and experimental results show that the proposed scheme is feasible with a higher security and a smaller key. For the $32 \times 32$ pixels image, the number of bits sent from Alice to Bob by using SSGI-OE ($M = 1024$, $N = 2048$) scheme is only 0.0107 times over a computational ghost imaging optical encryption scheme. When the eavesdropping ratio (ER) is less than 40%, the eavesdropper cannot acquire any information of the encrypted image. The extreme circumstance for the proposed SSGI-OE scheme is also discussed, where the eavesdropper begins to extract the information when ER is up to 15%.

**Keywords:** optical encryption, ghost imaging, spread spectrum, correlated imaging

**PACS:** 42.30.–d, 42.30.Wb, 42.30.Va **DOI:** 10.1088/1674-1056/acbf27

## 1. Introduction

With the rapid development of the informatization of human society, information security is becoming more and more important. To meet the sever challenge, researchers have proposed a variety of encryption techniques successively. They mainly include computer encryption,[1] quantum encryption,[2–5] and optical encryption.[6,7] As a promising encryption method, optical encryption has a lot of advantages, such as high-speed operation and possibility of hiding data in multiple dimensions (like phase, wavelength, spatial frequency, or polarization), which recently attracts interests from more and more researchers.

In a different context, ghost imaging (GI),[8–21] as an intriguing optical technique, has been receiving considerable current attention since Pittman *et al.* proposed an optical imaging by using two-photon quantum entanglement in 1995.[8] In 2002, Bennink[9] provided an experimental demonstration of ghost imaging using a classical source which opened a new avenue to obtain higher resolution images in optically harsh or noisy environments. In ghost imaging, there are two optical beams. One beam, called the signal beam, illuminates an object and then is detected by a bucket detector without any spatial resolution. The other beam, named as the reference beam, is detected by a high spatial resolution detector, such as a charge coupled device (CCD). The information of the object can be retrieved by correlating the intensities detected by the two detectors. In 2008, Shapiro proposed an architecture, named as computational ghost imaging (CGI) to simplify the system of ghost imaging, in which only the signal beam was needed and the reference beam was calculated offline.[22] This offline computational ghost imaging scheme makes the application of ghost imaging in optical encryption field possible.[23–38] For instance, Clemente *et al.* proposed a computational ghost imaging optical encryption (CGI-OE) scheme based on the concepts of CGI in 2010,[23] in which the information of an object is encrypted into the intensities of signal light. In 2012, Tanha *et al.* proposed a gray and a color optical encryption scheme to improve the security and develop the application.[24] Then we presented a quick response (QR) coded compressive ghost imaging optical encryption scheme (QR-CGI-OE), where the computational GI technique, QR code, and compressive sensing technique were adopted in the scheme.[25] In addition, we proposed another optical encryption scheme based on ghost imaging system with disordered speckles to obtain a higher security with a small key in 2017.[26] Later, according to the stealth effect of the phase object in the ghost imaging, Kang *et al.* proposed an optical encryption method based on compressive ghost imaging and public key cryptography in 2018,[27] which solved the key distribution problem of ghost imaging encryption, and reduced the additional cost of establishing security channels. In 2019, a novel information encryption scheme[28]

[†]Corresponding author. E-mail: zhaosm@njupt.edu.cn

© 2023 Chinese Physical Society and IOP Publishing Ltd 

was presented based on the customized data container, where the primary information can be recovered completely from the ciphertext encrypted with computational ghost imaging. In 2020, we also proposed an optical encryption scheme based on ghost imaging with fractional Fourier transform (FrFT), which could dramatically reduce the number of bits of the key transferred between authorized users comparing to the existing optical encryption schemes based on CGI.[29] Recently, Zheng *et al.* proposed an inverse computational GI scheme,[35] in which bucket signals are firstly selected and then random patterns are calculated correspondingly. This scheme provided an opportunity to combine with other cryptographies, and enriched the GI-based encryption process.

It can be believed that the optical encryption schemes based on CGI have dramatically reduced the number of the bits required to transmit the object information to a remote party because the encryption of the object image is not a complex valued matrix but simply an intensity vector. However, the prepared random speckle patterns, commonly selected as the secure key in most existing optical encryption schemes based on CGI, have to be transmitted to the authorized user in a private channel, and the amount of the secure key is large due to the recovery algorithm of computational GI technique. Hence, the corresponding key distribution becomes a severe task in the realizations of the existing optical encryption schemes based on CGI. It is a promising direction to develop a secure encryption with a little key distribution.

In this paper, we propose a novel secure optical encryption scheme, named as SSGI-OE, based on spread spectrum ghost imaging,[39] which is a promising technique in optical security because it has a great potential in protection against eavesdropping. In the scheme, Alice firstly generates a large Hadamard matrix of order $N$, and randomly selects $M$ $(M<N)$ rows' numbers of the generated Hadamard matrix as the secure key and distributes them to Bob in a private channel. Alice extracts $M$ corresponding row vectors of the generated Hadamard matrix and regards them as the direct sequence codes. With the help of the spread spectrum ghost imaging system, the measurement results from the bucket detector, called ciphertext, are obtained. Later, Alice transmits $M$ speckle patterns and the ciphertext to Bob by a public channel. The unauthorized user, Eve, cannot reconstruct the image of the object because the correlations between the measurement results and the speckle patterns are destroyed. On the contrary, the authorized user, Bob, could despread the measurement results by the received key, and retrieve the image of the object with the theory of SSGI. The feasibility and security of the proposed optical encryption scheme are discussed by simulations and experiments.

This paper is organized as follows. In Section 2, we present the schematic setup of the SSGI-OE scheme, and give the theoretical analysis of the proposed scheme. In Section 3, we provide the numerical and experimental results to demonstrate the proposed scheme. Finally, we draw our conclusion in Section 4.

## 2. Theory

### 2.1. Theoretical method

Figure 1 shows the schematic diagram of the proposed SSGI-OE scheme, where $\{\mathrm{Row}_k\}_{k=1}^{M}$ are rows' numbers randomly chosen from $N$ order Hadamard matrix, and $M$ is the number of the selected row vectors. These rows' numbers are the secure key in the scheme, and transmitted to Bob by a private channel. Alice takes the resultant row vectors of the generated Hadamard matrix as the direct sequence codes $\{\varphi_k(t)\}_{k=1}^{M}$ to modulate the speckle patterns $\{I_k(x,y)\}_{k=1}^{M}$. The $k$th direct sequence code is used to modulate the $k$th speckle pattern. $N$ is the length of each direct sequence code. Then these speckle patterns are modulated by a spatial modulator, such as a spatial light modulator (SLM) or digital micro-mirror device (DMD), to obtain the temporal-spatial speckle patterns $\{P_k(x,y,t)\}_{k=1}^{M}$.

$$P_k(x,y,t)=I_k(x,y)\varphi_k(t), \tag{1}$$

where $I_k(x,y)$ is the intensity distribution of the $k$th speckle pattern, and the direct sequence code $\varphi_k(t)$, which is an orthogonal walsh hadamard code, should satisfy

$$\int_T \varphi_k(t)\varphi_{k'}(t)\,\mathrm{d}t=\begin{cases}1, & \text{if} \quad k=k',\\ 0, & \text{otherwise},\end{cases} \tag{2}$$

where $T$ is the duration of a speckle pattern.

Later, these speckle patterns illuminate the object directly, and a bucket detector is used to collect the total light intensities transmitted through the object, denoted as $B_k(t)$,

$$\begin{aligned} B_k(t) &= \int_A P_k(x,y,t)T(x,y)\,\mathrm{d}x\mathrm{d}y\\ &= \int_A I_k(x,y)\varphi_k(t)T(x,y)\,\mathrm{d}x\mathrm{d}y\\ &= \varphi_k(t)\int_A I_k(x,y)T(x,y)\,\mathrm{d}x\mathrm{d}y, \end{aligned} \tag{3}$$

where $T(x,y)$ is the transmission function of the object, $A$ is the illuminated region by $P_k(x,y,t)$. This operation is repeated $M$ times for $M$ different temporal-spatial speckle pattern $P_k(x,y,t)$, and obtains $M$ bucket detection signals $\{B_k(t)\}_{k=1}^{M}$. Then a summation of each bucket detection signal, $\sum_{k=1}^{M}B_k(t)$, which is called ciphertext, is transmitted in a public channel.

$$\begin{aligned} \sum_{k=1}^{M}B_k(t) &= \sum_{k=1}^{M}\varphi_k(t)\int_A I_k(x,y)T(x,y)\,\mathrm{d}x\mathrm{d}y\\ &= \sum_{k=1}^{M}B_k\varphi_k(t), \end{aligned} \tag{4}$$

where $B_k=\int_A I_k(x,y)T(x,y)\,\mathrm{d}x\mathrm{d}y$.

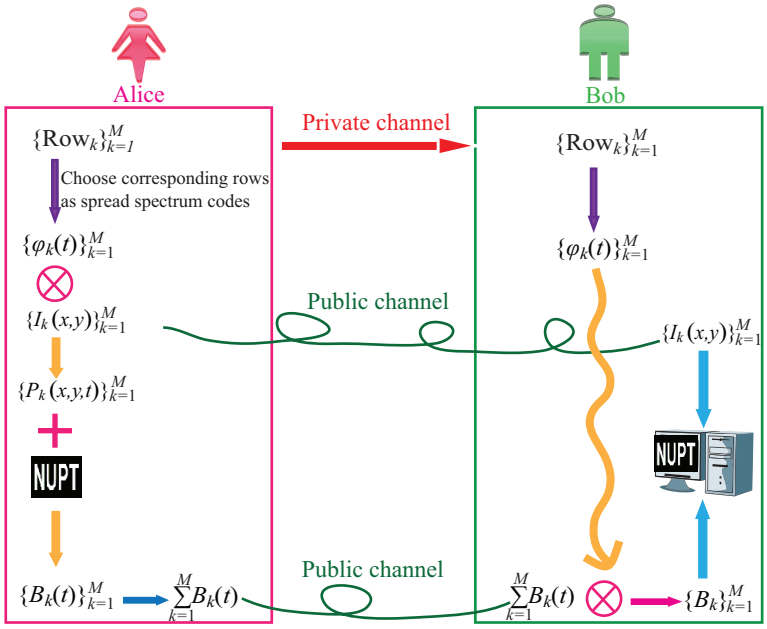



**Fig. 1.** Schematic diagram of the SSGI-OE scheme.

Afterwards, Alice sends the speckle patterns $\{I_k(x,y)\}_{k=1}^M$ to Bob in a public channel. With the correct secure key $\{\mathrm{Row}_k\}_{k=1}^M$, the direct sequence codes $\{\varphi_k(t)\}_{k=1}^M$ can be extracted exactly. Using these correct direct sequence codes, the ciphertext can be decrypted,

$$\begin{aligned}\int_T \varphi_k(t)\sum_{k'=1}^{M} B_{k'}(t)\,\mathrm{d}t &= \sum_{k'=1}^{M} B_{k'}\int_T \varphi_k(t)\varphi_{k'}(t)\,\mathrm{d}t\\ &\overset{k'=k}{=} B_k. \end{aligned} \tag{5}$$

It is shown that the $k$th bucket detection signal corresponding to the $k$th modulated speckle pattern from the ciphertext can be separated efficiently.

Hence, Bob can retrieve the image of the object with the second-order correlation algorithm,[40]

$$\hat{T}(x,y) = \frac{1}{M}\sum_{k=1}^{M}\left(B_k - \langle B\rangle\right) I_k(x,y), \tag{6}$$

where $M$ refers to the number of the speckle patterns, and $\langle B\rangle = \frac{1}{M}\sum_{k=1}^{M} B_k$.

### 2.2. Security analysis

On the other hand, we conduct a comprehensive security analysis of the proposed scheme. The unauthorized user cannot recover the image of the object. The great advantage of the direct sequence codes is that we can obtain a high security in optical encryption. Assume that the unauthorized user decrypts the ciphertext $\sum_{k=1}^{M} B_k(t)$ with the direct sequence codes $\{\varphi_e(t)\}_{e=1}^M$, which are extracted from the wrong secure key $\{\mathrm{Row}_e\}_{e=1}^M$, he will get

$$\begin{aligned}\int_T \varphi_e(t)\sum_{k'=1}^{M} B_{k'}(t)\,\mathrm{d}t &= \sum_{k'=1}^{M} B_{k'}\int_T \varphi_e(t)\varphi_{k'}(t)\,\mathrm{d}t\\ &\overset{k'=e}{=} B_e\int_T \varphi_e(t)\varphi_{k'}(t)\,\mathrm{d}t\\ &= B_e. \end{aligned} \tag{7}$$

It is shown that $B_e$, instead of $B_k$, is separated from the ciphertext, which means that the correlations between the resultant detection results $\{B_e\}_{e=1}^M$ and the speckle patterns $\{I_k(x,y)\}_{k=1}^M$ are destroyed, so the unauthorized user cannot recover the imaging $\hat{T}^e(x,y)$ with the second-order correlation,

$$\hat{T}^e(x,y) = \frac{1}{M}\sum_{e=1,k=1}^{M}\left(B_e - \langle B^e\rangle\right) I_k(x,y), \tag{8}$$

where $\langle B^e\rangle = \frac{1}{M}\sum_{e=1}^{M} B_e$, and $\hat{T}^e(x,y)$ is random data. No useful information can be obtained from the random data $\hat{T}^e(x,y)$.

In addition, we further analyze the possibility of obtaining the entire secure key in the proposed SSGI-OE scheme. Suppose that the length of the secure key is $M$ and the length of each direct sequence code is $N$, then the probability of obtaining the entire secure key for successfully reconstructing the original image, denoted as $r$, can be written as

$$r = \frac{1}{N}\times\frac{1}{N-1}\times\frac{1}{N-2}\times\cdots\times\frac{1}{N-M+1} \ll 1. \tag{9}$$

From Eq. (9) we can see that, when $N$ is larger, the probability of success $r$ is close to zero. In other words, the unauthorized user has only a slim chance to eavesdrop the entire secure key. It is theoretically deduced that our proposed scheme has a high security.

## 3. Results and discussion

In this section, we testify the proposed SSGI-OE scheme by both numerical simulations and experiments. In addition, we discuss the vulnerability of the proposed scheme.

The experimental setup for the proposed SSGI-OE scheme is shown in Fig. 2. A light emitting diode (LED) is driven by a direct-current (DC) source (Gwinstek GPD-3303S) of 2.9 V to produce the speckle patterns, which are modulated by a digital mirror device (DMD, ViALUX V-7001) with a spatial distribution, where the $k$th speckle pattern $I_k(x,y)$ is firstly modulated by the $k$th direct sequence code $\varphi_k(t)$. Then these speckle patterns are projected onto the object successively. Note that the Hadamard speckle patterns are utilized in practical experiment due to the limitations of experimental equipments. Then a photodetector (Thorlabs PDA100A-EC with gain 30 dB) is employed to collect the total transmission light intensities through the object to generate the bucket detection signals $B_k(t)$, which are recorded via an analogue-to-digital converter (NI USB-6351). Then Alice sends the speckle patterns $\{I_k(x,y)\}_{k=1}^{M}$ and the ciphertext $\sum_{k=1}^{M} B_k(t)$ to the authorized user, Bob, in a public channel. Meanwhile, the secure key is sent to Bob in a private channel.

In order to compare the quality of the reconstructed image quantitatively, mean square error (MSE) and peak signal-to-noise ratio (PSNR) are used as the evaluations, which are defined as[26]

$$\mathrm{MSE} = \frac{1}{L}\sum_{x,y}(\hat{T}(x,y) - T(x,y))^2, \tag{10}$$

$$\mathrm{PSNR} = 10\log_{10}\left(\frac{\max Val^2}{\mathrm{MSE}}\right), \tag{11}$$

where $\hat{T}(x,y)$ and $T(x,y)$ refer to the reconstructed and the original image respectively, $(x,y)$ is Cartesian coordinate, $L$ is the pixels of the image, and $\max Val$ is the maximum possible pixel value of the image.

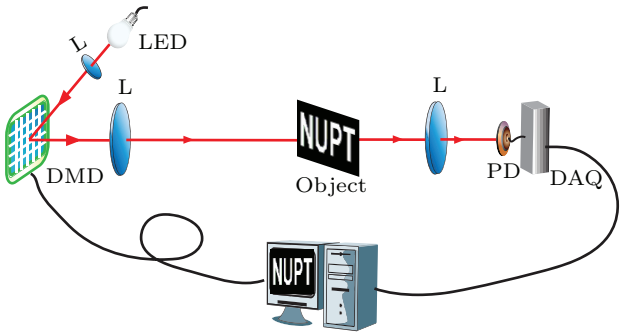



**Fig. 2.** The experimental setup for the proposed SSGI-OE scheme system. LED: light emitting diode. DMD: digital mirror device. L: lens. PD: photodetector. DAQ: data acquisition card.

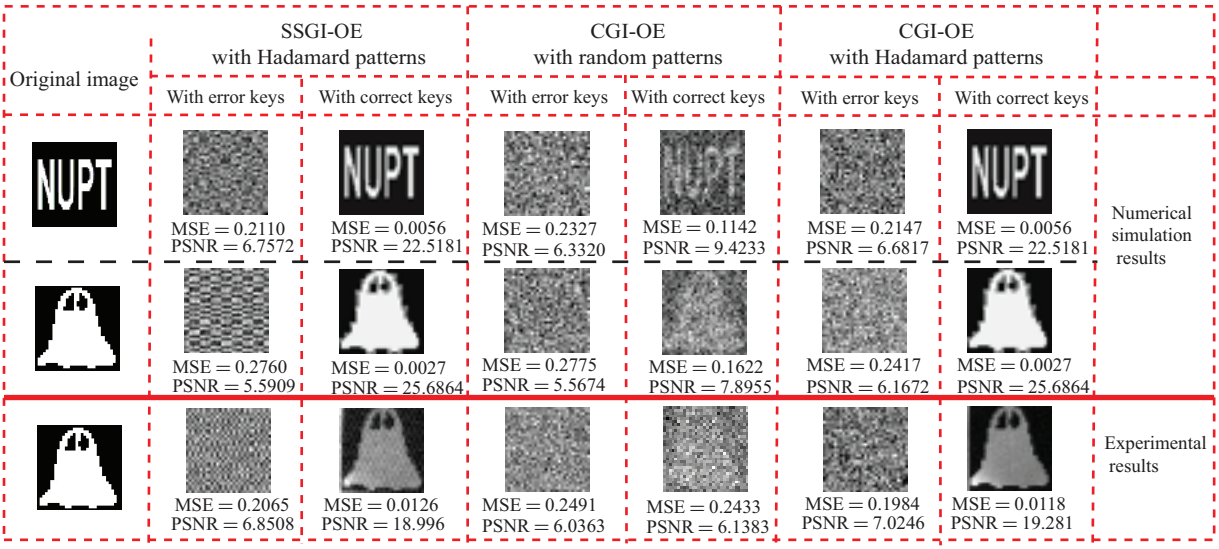



**Fig. 3.** Comparison of the numerical simulations and experimental results by SSGI-OE and CGI-OE with Hadamard speckle patterns and random speckle patterns.

We first demonstrate the feasibility of the proposed SSGI-OE scheme shown in Fig. 3, where the picture of 'NUPT' and the 'Ghost' image with the size of $32 \times 32$ pixels are selected as the objects in the simulation, and only the 'Ghost' is used for the experiment. Here, 1024 Hadamard speckle patterns are considered for SSGI-OE scheme and 1024 random speckle patterns are used for the CGI-OE scheme. To provide a fair comparison, we also present the CGI-OE scheme with Hadamard speckle patterns together. For the SSGI-OE scheme, a Hadamard matrix of order $N = 2048$ is generated first, and 1024 rows are selected randomly as the direct sequence codes, whose rows' numbers are regarded as the secure key. Note that we use the same secure key in both simulations and experiments. For the CGI-OE scheme, the random speckle patterns (or the Hadamard speckle patterns) are taken as the secure key. The results show that the reconstructed images with the correct key have the complete information of the original ones, especially when the Hadamard speckle patterns are used the recovered images are reconstructed perfectly by both optical encryption schemes, whereas the recovery images with the error key have no useful information of the original object images. In addition, from the column of SSGI-OE

with Hadamard patterns and the column of CGI-OE with random patterns, we can see that the images reconstructed by the proposed SSGI-OE scheme are much better than those by the CGI-OE scheme. Therefore, we carry out the simulations and experiments with Hadamard speckle patterns later. Moreover, from the column of SSGI-OE with Hadamard patterns and the column of CGI-OE with Hadamard patterns, we can see that both encryption schemes have similar results, which indicates that the proposed SSGI-OE scheme has a similar decryption performance to the CGI-OE scheme in this situation.

Moreover, the proposed SSGI-OE scheme has a much smaller key. For the $32 \times 32$ pixels image, the number of bits of the secure key sent from Alice to Bob by the proposed SSGI-OE scheme ($M = 1024$, $N = 2048$) can be calculated by

$$\mathrm{Num}_{\mathrm{SSGI}} = M \times \log_2 N, \tag{12}$$

where $M$ is the length of the secure key, $N$ is the order of the generated Hadamard matrix, and $\log_2 N$ refers to the transmitted bits of each row number in the secure key. Similarly, for the $32 \times 32$ pixels image, the secure key in the CGI-OE scheme can be computed by

$$\mathrm{Num}_{\mathrm{CGI}} = M \times L, \tag{13}$$

where $M$ is the number of speckle patterns, and $L$ is the number of pixels of each speckle pattern.

The number of bits of the secure key sent from Alice to Bob is listed in Table 1. From Table 1 we can see that when $M = 1024$, $N = 2048$, the number of bits sent from Alice to Bob by using SSGI-OE scheme is about $1.1264 \times 10^4$ bits, while the secure key by using the CGI-OE ($M = 1024$) scheme is about $1.048 \times 10^6$ bits, which is almost 93.04 times over the SSGI-OE scheme on key distribution. In other words, the number of bits sent from Alice to Bob by using the SSGI-OE ($M = 1024$, $N = 2048$) scheme is only 0.0107 times over the CGI-OE ($M = 1024$) scheme. It is indicated that the proposed SSGI-OE considerably reduces the number of bits sent by Alice to Bob.

**Table 1.** The number of bits of the secure key sent from Alice to Bob by using the SSGI-OE and CGI-OE schemes.

| Methods | Number ($M = 1024$) | Number ($M = 256$) |
|---|---|---|
| SSGI-OE ($N = 2048$) | $1.1264 \times 10^4$ (bits) | $2.816 \times 10^3$ (bits) |
| SSGI-OE ($N = 1024$) | $1.024 \times 10^4$ (bits) | $2.56 \times 10^3$ (bits) |
| CGI-OE | $1.048 \times 10^6$ (bits) | $6.5536 \times 10^4$ (bits) |

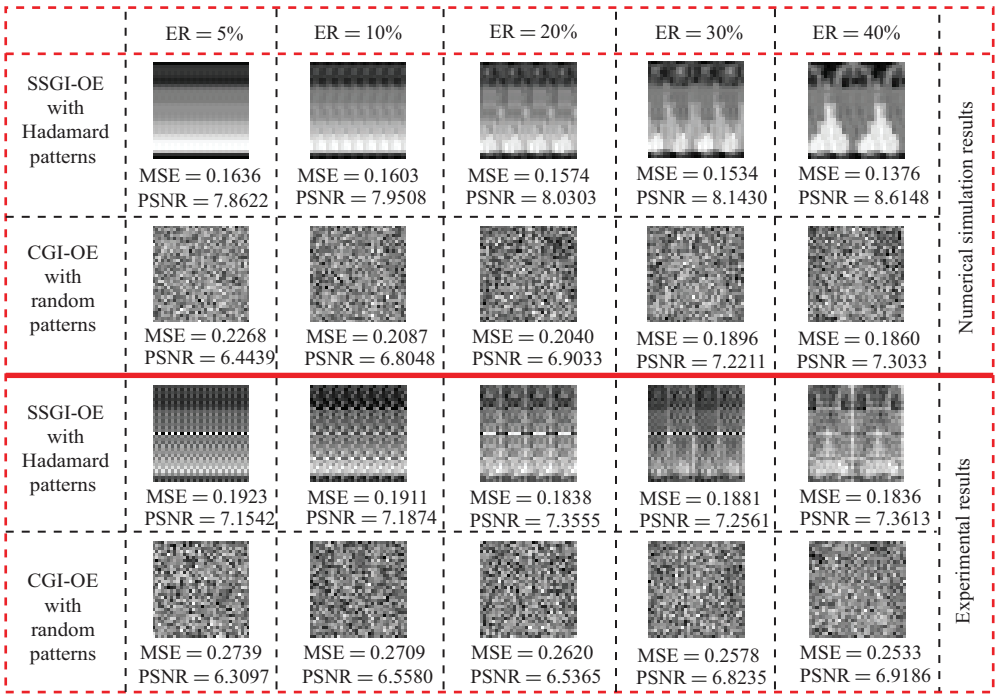



**Fig. 4.** Comparison of simulated and experimental results under different eavesdropping ratios.

Next, we test the security of the proposed SSGI-OE scheme with the object 'Ghost' and compare with the results of the CGI-OE scheme. Assume that a potential eavesdropper, Eve, has an eavesdropping ratio (ER) of the secure key. The eavesdropping ratio (ER) is defined as

$$\mathrm{ER} = \frac{M'}{M}, \tag{14}$$

where $M'$ refers to the length of the eavesdropping secure key, and $M$ is the length of the whole secure key. The value of ER is set from 5% to 40%. The reconstructed results are displayed in Fig. 4. Here, the size of the binary 'Ghost' mage is $32 \times 32$ pixels, and the length of the direct sequence code is $N = 2048$. The proposed SSGI-OE scheme adopts 1024 Hadamard speckle patterns, and the CGI-OE scheme uses 1024 random speckle patterns. The first two rows are simulated results, from which we can see that the encrypted infor-

mation by both schemes cannot be retrieved correctly when ER is less than 40%, even though the outline of the images reconstructed by the SSGI-OE scheme are more or less distinguished. The last two experimental results also show that Eve could not recover the original image when ER is less than 40%, which indicates that the proposed SSGI-OE scheme has a high security.

Figure 5 further shows the MSE and PSNR curves against the eavesdropping ratio by using the proposed SSGI-OE scheme and the CGI-OE scheme. Figure 5(a) shows the simulated results. Figure 5(b) shows the experimental results. Here the object is a binary Ghost image with the size of $32 \times 32$ pixels, and the length of the direct sequence code is $N = 2048$. The proposed SSGI-OE scheme uses 1024 Hadamard speckle patterns, and the CGI-OE scheme employs 1024 random speckle patterns. Both simulations and experimental results show that even though the MSEs (PSNRs) value by using the proposed SSGI-OE scheme is smaller (larger) than those by using CGI-OE scheme, Eve could not obtain any information of the original image by using SSGI-OE scheme. The proposed scheme has a high security with a much smaller key. In addition, compared with the other normal encryption scheme based on ghost imaging, such as the scheme demonstrated in Ref. [24], our proposed scheme has a smaller key distribution with a similar security. Because the randomly selected row numbers are the key in our proposed scheme, while the speckle patterns are often used as the key in the normal GI-OE. The size of the row numbers is absolutely smaller than that of the speckle patterns.

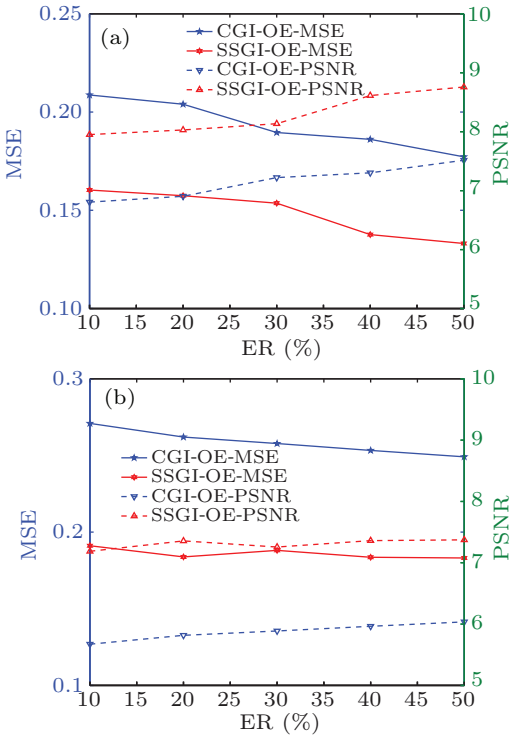



**Fig. 5.** The MSE and PSNR of the recovered images against the eavesdropping ratio: (a) the simulated results, (b) the experimental results.

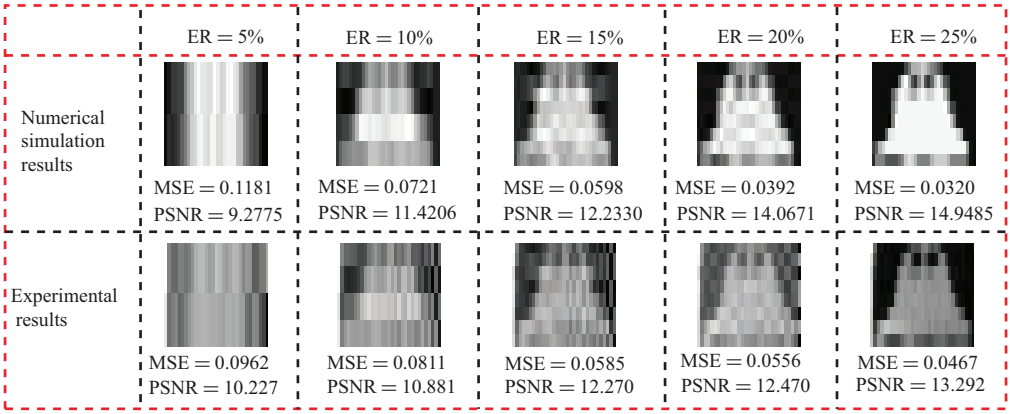



**Fig. 6.** Simulated and experimental results by the proposed SSGI-OE scheme under different eavesdropping ratios at the extreme circumstance.

Finally, we discuss the security of the proposed SSGI-OE scheme at the extreme circumstance. As we all know, different Hadamard speckle patterns have different contributions on the imaging, the speckle patterns with lower frequency usually have a bigger contributions of imaging, while the higher frequency speckle patterns have less contributions. These speckle patterns with different frequencies can be known from the sequency ordering algorithm.[41] Generally, a Hadamard matrix $H$ of order $N$ is in natural order, which can be defined as

$$S_i = \mathrm{wal_h}(i), \quad (i = 0, 1, 2, \ldots, N-1), \tag{15}$$

where $S_i$ refers to the $i$th row vector of the hadamard matrix $H$, and $\mathrm{wal_h}$ denotes the natural ordered Walsh functions. Here, $\mathrm{wal_o}$ is defined as the sequency-ordered Walsh functions, then

$$\mathrm{wal_h}(i) = \mathrm{wal_o}[b(\langle i \rangle)], \tag{16}$$

where $\langle i \rangle$ stands for the bit-reversed representation of $i$ and $b$ $(\langle i \rangle)$ is the gray code to binary conversion of $\langle i \rangle$. The gray code is a reflective binary code wherein two successive values differ in only one bit. By the sequency ordering algorithm, the Walsh–Hadamard speckle patterns are ordered from lower frequency to higher frequency.

Suppose that the eavesdropper, Eve, she eavesdrops the secure key to decrypt the ciphertext and achieves a number of

bucket values which are properly corresponding to the speckle patterns with lower frequency, she extracts the image of the object at a lower eavesdropping ratio. The results are displayed in Fig. 6. Here, the size of the binary 'Ghost' image is $32 \times 32$ pixels, the number of the speckle patterns is $M = 1024$, and the length of the direct sequence code is $N = 2048$. The value of ER is set from 5% to 25%. Both simulations and experimental results show that the encrypted information begins to be retrieved when ER is less than 15%. However, this situation happens with a poor probability. According to Eq. (9), the length of the 15% secure key is $M' = 1024 \times 0.15 = 154$ and the length of each direct sequence code is $N = 2048$, then the probability $r$ is

$$r = \frac{1}{2048} \times \frac{1}{2047} \times \frac{1}{2046} \times \cdots \times \frac{1}{1896} \times \frac{1}{1895} \ll 1. \quad (17)$$

From Eq. (17), we can see that the probability $r$ is close to 0. It is indicated that the proposed SSGI-OE scheme has a high security.

## 4. Conclusion

In summary, we have proposed a novel optical encryption scheme based on the spread spectrum ghost imaging, named as SSGI-OE. In the scheme, the row numbers randomly selected from a Hadamard matrix with order $N$ are regarded as the secure key, transmitted from Alice to Bob in a private channel, and the corresponding row vectors are used as the direct sequence codes in the SSGI system. Only the authorized user, Bob, could decrypt the ciphertext by the correct key, and recover the encrypted image with the theory of SSGI, whereas the unauthorized user, Eve, could not obtain any useful information of the encrypted image. The numerical simulations and experimental results have shown the feasibility and the security of the proposed SSGI-OE scheme. When the ER is less than 40%, the eavesdropper cannot acquire any information of the encrypted image. Meanwhile, the authorized user could recover completely the encrypted information with the secure key. Moreover, for the extreme circumstance, the eavesdropper begins to retrieve the information of the encrypted image when ER is less than 15%. However, this situation happens with a lower probability. For the $32 \times 32$ pixels image, the number of bits sent from Alice to Bob by using the SSGI-OE ($M = 1024$, $N = 2048$) scheme is only 0.0107 times over the CGI-OE scheme. It is indicated that our proposed SSGI-OE scheme has a higher security with a smaller key distribution. It has provided a practical method to complement optical encryption with the CGI system. Furthermore, the proposed scheme could promise widespread application of ghost imaging encryption in high security data transferring.

## Acknowledgements

Project supported by the National Natural Science Foundation of China (Grant Nos. 61871234 and 62001249), the Postgraduate Research & Practice Innovation Program of Jiangsu Province (Grant No. KYCX20_0729), the Natural Science Research Project of Higher Education of Jiangsu Province (Grant No. 20KJB510030), the Qing Lan Project of Jiangsu Province (Su Teacher's Letter [2022] No. 29), the Research project of NanJing Tech University Pujiang Institute (Grant No. njpj2022-1-25), and the Priority Academic Program Development of Jiangsu Higher Education Institutions.

## References

[1] Hamza A and Kumar B 2020 *9th International Conference System Modeling and Advancement in Research Trends (SMART)*, December 04–05, 2020, Moradabad, India, p. 333
[2] Deng F and Long G 2004 *Phys. Rev. A* **69** 052319
[3] Bennett C H and Brassard G 2003 arXiv:2003.06557v1 [quant-ph]
[4] Bennett C H, Brassard G and Mermin N D 1992 *Phys. Rev. Lett.* **68** 557
[5] Ekert A K 1991 *Phys. Rev. Lett.* **67** 661
[6] Refregier P and Javidi B 1995 *Opt. Lett.* **20** 767
[7] Liu S, Guo C and Sheridan J T 2014 *Opt. Laser Technol.* **57** 327
[8] Pittman T B, Shih Y H, Strekalov D V and Sergienko A V 1995 *Phys. Rev. A* **52** R3429(R)
[9] Bennink R S, Bentley S J and Boyd R W 2002 *Phys. Rev. Lett.* **89** 113601
[10] Zhang D, Zhai Y, Wu L and Chen X 2005 *Opt. Lett.* **30** 2354
[11] Deng C, Gong W and Han S 2016 *Opt. Express* **24** 25983
[12] Huang H, Zhou C, Tian T, Liu D and Song L 2018 *Opt. Commun.* **412** 60
[13] Zhang H and Duan D 2021 *Opt. Express* **29** 43929
[14] Wang C, Lan R, Ren C and Cao D 2020 *Phys. Rev. A* **101** 033819
[15] Wang L and Zhao S 2020 *IEEE Photon. J.* **12** 6901113
[16] Wang L and Zhao S 2021 *Opt. Express* **29** 24486
[17] Liu J, Wang L and Zhao S 2022 *Chin. Phys. B* **31** 084202
[18] Guo H, Wang L and Zhao S 2022 *Chin. Phys. B* **31** 084201
[19] Wang L, Guo H and Zhao S 2022 *Chin. Phys. B* **31** 114202
[20] Zhang H, Xia Y and Duan D 2021 *Chin. Phys. B* **30** 124209
[21] He X, Zhao S and Wang L 2021 *Chin. Phys. B* **30** 054201
[22] Shapiro J H 2008 *Phys. Rev. A* **78** 061802(R)
[23] Clemente P, Durán V, Torres-Company V, Tajahuerce E and Lancis J 2010 *Opt. Lett.* **35** 2391
[24] Tanha M, Kheradmand R and Ahmadi-Kandjani S 2012 *Appl. Phys. Lett.* **101** 101108
[25] Zhao S, Wang L, Liang W, Cheng W and Gong L 2015 *Opt. Commun.* **353** 90
[26] Zhang Y and Zhao S 2017 *Chin. Phys. B* **26** 054205
[27] Kang Y, Zhang L and Zhang D 2018 *Opt. Laser Eng.* **111** 58
[28] Sui L, Du C, Xu M, Tian A and Asundi A 2019 *Opt. Express* **27** 16493
[29] Zhao S, Yu X, Wang L, Li W and Zheng B 2020 *Opt. Commun.* **474** 126086
[30] Yuan S, Wang L, Liu X and Zhou X 2020 *Opt. Lett.* **45** 3917
[31] Zafari M, Kheradmand R and Ahmadi-Kandjani S 2014 *J. Opt.* **16** 105405
[32] Zhu J, Yang X, Meng X, Wang Y, Yin Y, Sun X and Dong G 2018 *Opt. Commun.* **420** 34
[33] Chen Z, Shi J and Zeng G 2016 *Appl. Opt.* **55** 8644
[34] Kong L, Li Y, Qian S, Tu C and Wang H 2013 *Phys. Rev. A* **88** 013852
[35] Zheng P, Tan Q and Liu H 2021 *Opt. Express* **29** 21290
[36] Zheng P, Ye Z, Xiong J and Liu H 2022 *Opt. Express* **30** 21866
[37] Liu Y, Zheng P and Liu H 2022 *Opt. Express* **30** 14073
[38] Wang L, Zhao S, Cheng W, Gong L and Chen H 2016 *Opt. Commun.* **366** 314
[39] Liu J, Wang L and Zhao S 2021 *Opt. Express* **29** 41485
[40] Liu J, Wang L and Zhao S 2022 *Appl. Opt.* **61** 7102
[41] Corinthios M 2009 *Signals, Systems, Transforms and Digital Signal Processing with MATLAB* (New York: CRC Press) pp. 914–915