https://doi.org/10.1016/j.optlaseng.2020.106094

Optical ghost cryptography and steganography

Hong-Chao Liu[a,†], **Wen Chen**[b,*]

[a]Joint Key Laboratory of the Ministry of Education,
Institute of Applied Physics and Materials Engineering,
University of Macau, Avenida da Universidade,
Taipa, Macao SAR, China
[b]Department of Electronic and Information Engineering,
The Hong Kong Polytechnic University, Hong Kong, China
Emails: †hcliu@um.edu.mo (Hong-Chao Liu) and *owen.chen@polyu.edu.hk (Wen Chen)

Abstract: As an indirect imaging technique, computational ghost imaging (GI) obtains the object information by calculating the intensity correlation between a series of computer-generated matrices and the corresponding bucket signals, which thereby offers a potential application in optical encryption. Here, we propose a new steganography scheme, called ghost steganography, based on the principle of computational GI. In our ghost steganography scheme, the bucket intensity signals of a secret image are concealed into the ones of a non-secret image by applying a non-conspicuous number integration process. To further increase the security, we introduce RSA cryptography to encode the integrated bucket signals after the steganography process. Simulation and experiment results fully demonstrate the feasibility of our optical ghost cryptography and steganography scheme. Our work paves a way to the application of GI in steganography and also enriches the knowledge of symmetric and asymmetric optical cryptography. @ Elsevier, 2020.

Keywords: Computational ghost imaging; Optical data processing; Reconstruction techniques; Ghost cryptography; Ghost steganography.

1. Introduction

Ghost imaging (GI), also known as correlated imaging, is an indirect imaging modality which obtains the object information from the intensity fluctuation correlation of two beams. One beam, called object beam, going through the object, is measured by a bucket detector. The other beam, called reference beam, interacting without the object, is detected by a spatially resolved camera. GI was firstly achieved with entangled photon pairs experimentally in 1995 [1], and later extended into the classical region with various thermal light sources [2-11]. Different from the two-detector GI, Shapiro proposed the computational GI in 2008 [12], which generated the active illumination patterns by using the spatial light modulator instead of passive measurements of reference beam. Similar to the single-pixel camera technique [13], computational GI can recover the object image with only a single-pixel detector [14,15], which largely simplifies the experimental setup. Meanwhile, the correlation between the computer-generated random matrix and the object beam intensity of computational GI offered a potential application in optical encryption [16-30]. To increase the efficiency and security of optical encryption based on GI [16], different methods are proposed and developed, including gray-scale and color encryption [17], multiple-image encryptions [18,26,29], specific phase masks schemes [22,25,27,30], XOR operation scheme [24]. Furthermore, GI encryption was extended into regimes of watermark [19], metasurface [20], identification [21], authentication [28], and secure key distribution [23], etc.

Although many encryption schemes have been developed, steganography has not been effectively introduced into GI. Steganography has been found to be an important and widely-used practice of hiding a message, image or data file into another non-secret one. In ancient times, people used invisible ink to write something secret on an ordinary paper that is steganography. Nowadays, the format of digit file changes the process of steganography. For example, considerable works were focused on image steganography on the basis of its digital pixel and color model [31-35]. Comparing with cryptography which is always relied on a complicated mathematics problem, steganography hides encrypted information in a non-conspicuous approach without attracting any attention, which is a big difference from cryptography. Combining steganography with cryptography usually offers a strong security, which thereby has great potential in GI-based optical encryption.

In this paper, we propose a steganography scheme based on computational GI, by concealing the object beam intensities of a hidden image into the ones of a non-secret image. With the correlation calculations between the non-conspicuous encoded object beam intensities and random matrices, only the non-secret image can be reconstructed instead of the hidden image. To prevent the steganography breaking and increase the security of the encoding process, we further introduce the widely-used RSA cryptography into our optical ghost steganography. Our simulation and proof-of-principle experiment pave a way to the application of GI into the fields of cryptography and steganography.

2. Model and principle

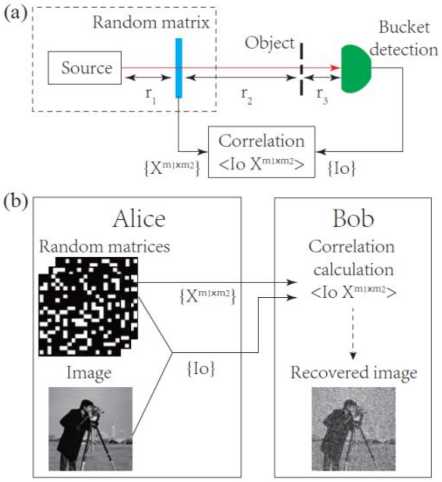

FIG. 1. (a) Schematic setup of computational GI, and (b) encryption flow based on GI.

Figure 1(a) shows the experimental setup for computational GI. A stable light source and different computer-generated random matrices $\{X^{m_1\times m_2}\}$, as shown in the dashed rectangle, are employed to generate the active light intensity fluctuations. After interacting with the object, the bucket intensities $\{Io\}$ are recorded by a single-pixel detector. Then, the object image can be recovered by calculating the second-order correlation function, which is defined by

$$G^{(2)}=\left\langle IoX^{m_1\times m_2}\right\rangle=\frac{1}{N}\sum_{i=1}^{N}Io_i X_i^{m_1\times m_2}, \qquad (1)$$

where $\langle ...\rangle$ is ensemble average of N measurements. Usually, N is much larger than the recovered image pixels $m_1\times m_2$ by using the basic reconstruction algorithm as shown in Eq. (1). In order to improve the imaging efficiency, compressive sensing algorithm [34], i.e., compressive GI [14], is employed here when considering the sparsity property of the imaging object. In compressive GI, each random binary matrix $X^{m_1\times m_2}$ is reshaped into a row vector ($1\times K, K=m_1\times m_2$), and $\{X^{m_1\times m_2}\}$ of N measurements is rewritten into a two-dimensional matrix A ($N\times K$). Meanwhile, the bucket signals $\{Io\}$ are expressed as a column vector Io^{CGI} ($N\times 1$). Assuming the object image is sparse in matrix A, it can be reconstructed by solving the convex optimization program [9,14,20,37].

$$T^{CGI}=|T|,\ \min\|T\|_1 \text{ subject to } Io^{CGI}=AT, \qquad (2)$$

where T^{CGI} denotes the recovered image, T denotes the object information, and $\|T\|_1$ denotes the L_1-norm of T. By applying compressive GI, a much smaller measurement number N ($N < K$) can achieve a clear object image.

According to the definition of computational GI, a symmetric cryptography is offered, as shown in Fig. 1(b). Suppose Alice want to send a secret image to Bob. By using different random matrices $\{X^{m_1\times m_2}\}$ as keys, Alice can encrypt the image into a series of intensity values $\{Io\}$ as the ciphertext, and then send $\{X^{m_1\times m_2}\}$ and $\{Io\}$ separately to Bob. After receiving the keys and ciphertext, Bob can use the GI algorithms, i.e., Eq. (1) or Eq. (2), to decrypt the image. Since both the encryption and decryption processes apply the same keys, communication process of the keys and ciphertext should be extremely careful, which is a fatal weakness of symmetric cryptography.

To enhance the communication security between Alice and Bob, we introduce the optical ghost cryptography and steganography scheme below. Usually, the object beam intensities $\{Io\}$ are a series of numbers consisting of both integer part and decimal part, especially in experimental case. Note that $\{Io\}$ and $\{c_0 Io\}$, where c_0 is a constant, are equivalent in the GI correlation reconstruction. Hence, without affecting the accuracy of GI recovery calculation, one can easily choose a suitable c_0 to make sure that all decimal parts of $\{c_0 Io\}$ are ignorable in the correlation calculations, i.e., $\{c_0 Io\}=\{c_0 Io\}_{\text{int}}+\{c_0 Io\}_{\text{dec}}\approx\{c_0 Io\}_{\text{int}}$. Based on this operation, Figure2 shows the ghost steganography scheme. After encoding the non-secret image and hidden image into $\{Io^{NON}\}$ and $\{Io^{HID}\}$, one can develop them into two integer series $\{c_2 Io^{NON}\}_{\text{int}}$ and $\{c_1 Io^{HID}\}_{\text{int}}$, respectively. Then these two series are integrated into a new series of numbers $\{Io^{STE}\}$, where $\{c_2 Io^{NON}\}_{\text{int}}$ and $\{c_1 Io^{HID}\}_{\text{int}}$ play the roles of integer part and decimal part, respectively. Table 1 shows a typical example of data processing in the designed ghost steganography. In Fig. 2, the simulation results show that a non-secret Cameraman image is obtained by using encrypted $\{Io^{STE}\}$ object beam signal, where the hidden Baboon image is well protected. Here, we estimate the imaging quality by introducing peak signal-to-noise ratio (PSNR), which is defined by

$$PSNR=10\log_{10}\left(\frac{MAX^2}{MSE}\right), \qquad (3)$$

where MAX=255 denotes the maximum possible pixel value of the image, and MSE denotes the mean square error given by $\frac{1}{m_1\times m_2}\sum_{i,j}[T_{re}(x_i,y_j)-T(x_i,y_j)]^2$, where $m_1\times m_2$ denotes the pixel number, $T_{re}(x_i,y_j)$ and $T(x_i,y_j)$ denote the pixel values of the recovered image and the object, respectively. As can be seen, the PSNR values of Cameraman ghost images have little difference before and after the steganography, indicating the feasibility of our optical ghost steganography.

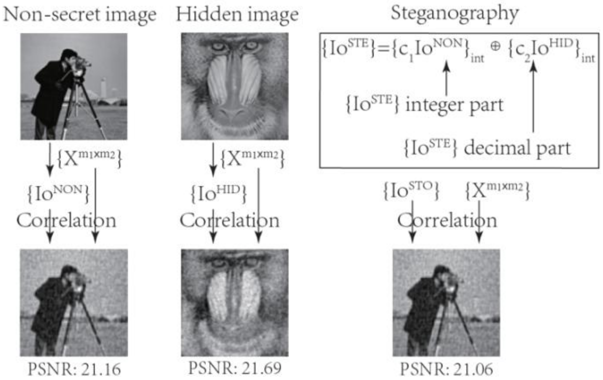

FIG. 2. Ghost steganography scheme. The lower row of images are recovered from simulation, where the sampling measurement times N=8000, and the gray random matrices are 101×101 pixels with random pixel value ranging from 0 to 1.

TABLE 1. The integration process of ghost steganography.

	$N=1$	$N=2$	…	$N=N$
$\{Io^{NON}\}$	31.9452	7.8209	…	24.9077
$\{Io^{HID}\}$	8.8235	67.2189	…	0.7943
$\{c_2 Io^{NON}\}_{\text{in}}$	3194	782	…	2490
$\{c_1 Io^{HID}\}_{\text{int}}$	882	6721	…	79
$\{Io^{STE}\}$	3149.0882	782.6721	…	2490.007 9

TABLE 2. The developed integration process of ghost steganography.

	$N=1$	$N=2$	…	$N=N$
$\{Io^{NON}\}$	31.9452	7.8209	…	24.9077
$\{Io^{HID}\}$	8.8235	67.2189	…	0.7943
$\{c_2 Io^{NON}\}_{\text{in}}$	3194	782	…	2490
$\{c_1 Io^{HID}\}_{\text{int}}$	882	6721	…	79
$\{Io^{STE}\}$	314908.82	78267.21	…	249000.79

The basic principle of ghost steganography is the existence of a large value discrepancy between $\{c_2 Io^{NON}\}_{\text{int}}$ and $\{c_1 Io^{HID}\}_{\text{int}}$ in the new $\{Io^{STE}\}$. Within this principle, the integration process of ghost steganography can be further improved based on Fig. 2 and Table 1. Table 2 gives an improved example. Different from the integration process of $\{Io^{STE}\}$ shown in Table 1, Table 2 presents a developed integration process, where $\{c_1 Io^{HID}\}_{\text{int}}$ plays as the decimal part as well as a small portion of the integer part of $\{Io^{STE}\}$. Without changing the effectiveness, this developed integration process makes our optical ghost steganography more flexible and more effective.

It should be note that the key characteristic of a steganography is "non-conspicuous". In our ghost steganography, all $\{Io^{STE}\}$ signals look like those obtained by conventional GI (e.g., $\{Io^{NON}\}$ and $\{Io^{HID}\}$), which makes the scheme difficult to realize. However, any steganography will fail if it has been noted. To further increase security of the ghost steganography scheme, we further introduce a famous RSA cryptography into the steganography process. RSA is a message encryption algorithm, which was invented by Ron Rivest, Adi Shamir, and Leonard Adleman in 1970's [38]. The basic idea of RSA encryption algorithm is the complex of prime factorization, that means, it is difficult to find the two prime factors of a large number [39,40]. Different from the symmetric cryptography, RSA uses a public key to encode the message into the ciphertext and another private key for the decoding process. Both the public key and ciphertext can be known to everyone, but only the one holding the private key can decode the message. As shown in Fig. 3, encryption flow of RSA is briefly described as follows:

Bob chooses two large different primes p and q, and calculates the value of modulus n with $n = pq$.

Bob calculates the totient $\phi(n) = (p-1)(q-1)$, and chooses an integer e which is coprime to $\phi(n)$ and satisfies $1 < e < \phi(n)$.

After obtaining the public key (e, n), Bob then calculates the value of d which satisfies the congruence relation $de \equiv 1 \bmod (\phi(n))$, and gets the corresponding private key (d, n).

Bob sends the public key (e, n) to Alice.

Alice encodes the message M into the ciphertext $c \equiv M^e (\mathrm{mod}\ n)$ by using the public key (e, n).

Alice sends the ciphertext c to Bob.

Bob operates the decoding process with the function $M \equiv c^d (\mathrm{mod}\ n)$, and obtains the recovered message.

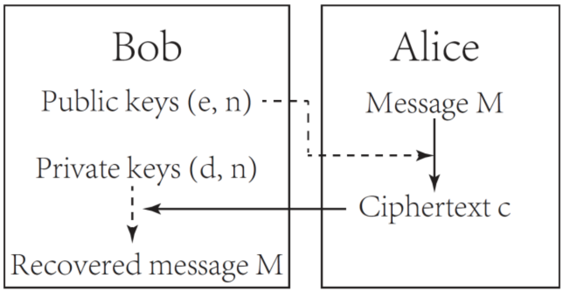

FIG. 3. Encryption flow in the RSA cryptography.

Compared to symmetric cryptography, there is no concern about the eavesdropping during the communications process of public key and ciphertext of RSA. For simplicity, we choose p = 521, q =523, e = 1669 in our experiments below.

3. Results and discussion

To verify our ghost cryptography and steganography scheme, an optical experimental setup of computational GI is shown in Fig. 4. A hot plate (178 mm × 178 mm) set at 50 °C is applied as a stable radiation source. Printed on regular paper sheets, random binary masks have a transmissive to nontransmissive ratio as 1:99. All random binary masks are 51×51 pixels, with the pixel size of 2.85 mm × 2.85 mm. The hidden object "0" and no-secret object "1" are transmissive ones, with size of 140 mm × 140 mm. In each measurement (or for each random binary mask), the total radiation intensity of long-wave infrared signal transmitted from the object is bucket detected [37]. A FLUKE TiX560 infrared camera is employed as the bucket detector, and the sampling measurement numbers are 650 in our experiment. As shown in Fig. 4, r_1 = 150 mm, r_2 = 30 mm, r_3 = 500 mm. To enhance the image reconstruction efficiency and reduce the measurement number, we use compressive GI algorithm with orthogonal matching pursuit to recover the object image. As shown in Fig. 4, a high-quality reconstructed digit "0" can be obtained after 650 measurements using compressive GI algorithm.

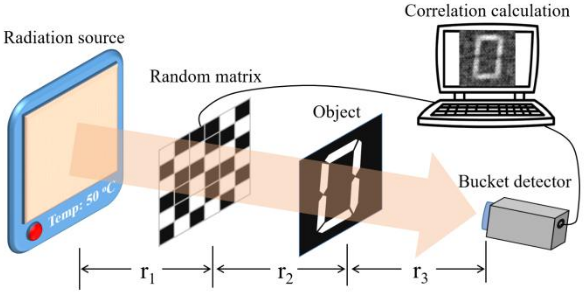

FIG. 4. Experimental setup of computational GI for ghost cryptography and steganography scheme.

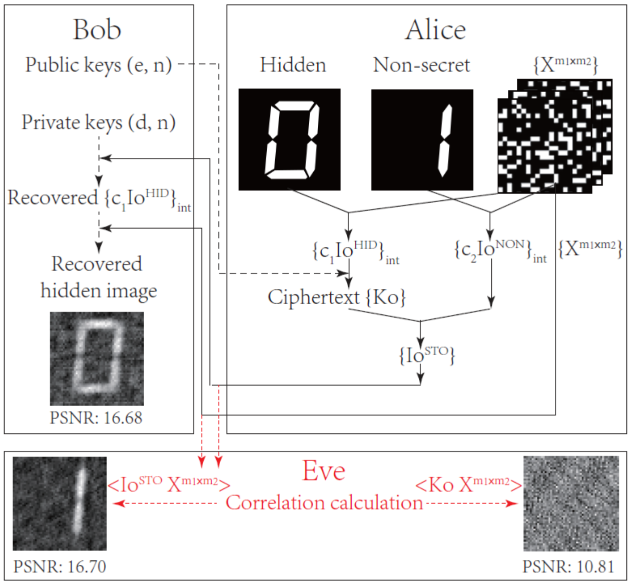

FIG. 5. Ghost steganography process based on the RSA cryptography.

Based on the experimental setup in Fig. 4, we further apply the ghost steganography together with RSA cryptography to enhance the security. In Fig. 5, a step-by-step process is given as follows:

Bob generates the public key (*e*, *n*) and private key (*d*, *n*) as described in Fig. 3, and sends the public key (*e*, *n*) to Alice.

Based on the computational GI experiment, Alice encodes the hidden image and non-secret image into $\{Io^{HID}\}$ and $\{Io^{NON}\}$, respectively, by using random matrices $\{X^{m_1\times m_2}\}$ as security keys. Then Alice obtains two corresponding integer series $\{c_1Io^{HID}\}_{\text{int}}$ and $\{c_2Io^{NON}\}_{\text{int}}$.

After receiving the public key (*e*, *n*), Alice then encodes message integer series $\{c_1Io^{HID}\}_{\text{int}}$ into the ciphertext $\{Ko\}$.

Alice integrates the ciphertext $\{Ko\}$ and integer series $\{c_2Io^{NON}\}_{\text{int}}$ into $\{Io^{STE}\}$ as described in the aforementioned ghost steganography in Fig. 2.

Alice sends both the encoded intensity signals $\{Io^{STE}\}$ and random matrices $\{X^{m_1\times m_2}\}$ to Bob.

Bob firstly ignores the integer part of $\{Io^{STE}\}$, and decodes decimal part $\{Ko\}$ with his private key (*d*, *n*) to obtain message $\{c_1Io^{HID}\}_{\text{int}}$.

By calculating the correlation between $\{c_1Io^{HID}\}_{\text{int}}$ and $\{X^{m_1\times m_2}\}$, Bob can finally recover the hidden ghost image of object "0".

Assuming there is an eavesdropper, called Eve, has stolen both the signals $\{Io^{STE}\}$ and random matrices $\{X^{m_1\times m_2}\}$. By using the correlation calculation of GI, only the non-secret ghost image "1" can be recovered. Even Eve knows the ghost steganography scheme and uses the decimal parts $\{Ko\}$ to recover the image, no image will be achieved as shown in Fig. 5 with the protection of RSA cryptography. It clearly indicates that the security of GI encryption is largely enhanced by steganography and RSA asymmetric cryptography.

To evaluate the security of our scheme, we can see that it is protected by both steganography and RSA cryptography. For the security of a steganography, the most critical factor is the perception of its existence. In our ghost steganography, all signals look like those obtained by conventional GI, making it difficult to note. What's more, all signals are encoded with RSA cryptography, ensuring them as secure as RSA cryptography. No matter how many percentages of signals are eavesdropped, the eavesdropper cannot reconstruct any information unless he/she is aware of our steganography scheme and knows the private key of RSA cryptography.

Comparing to traditional steganography, our ghost steganography could convey more information amount. As the most popular traditional steganography, least significant bit (LSB) describes the method to insert the hidden message into the least significant bit of non-secret image [31]. One downside of LSB is the limitation of the hidden message amount (i.e., only 1-bit for each pixel), which is always much less than the data amount of non-secret image (e.g., 8-bit for each pixel in general). In our ghost steganography, the data amounts of hidden image and non-secret image are equivalent to those in $\{Io^{STE}\}$. Moreover, based on the principle of ghost steganography shown in Fig. 2 and the two Tables, the number values in $\{Io^{STE}\}$ can even consist of three or more portions. The portion occupies the most significant bits coming from the non-secret image, and the other portions can consist of different hidden images. Hence, the data amounts of hidden images can exceed the non-secret image, making our ghost steganography more efficient.

Although RSA cryptography has a high security level, it might not be a safe method to encode an image independently. This is because a common image format is usually 8-bit, that means there are only 256 different values for millions of pixels. By applying RSA, the numbers from 0~255 can be encoded into only 256 different numbers, which however can be easily guessed out based on the relationship of different pixels. Therefore, to enhance the security, another method is necessary to encode an image together with RSA. In our ghost steganography and cryptography process, RSA is applied to encode the bucket signals of GI after steganography process. As all bucket signals of GI are independent and have no value limitation, the strong security of RSA can be fully exploited.

Based on the ghost cryptography and steganography scheme in Fig. 5, we can further add additional digits to the hidden image signals $\{c_1Io^{HID}\}_{\text{int}}$ as a watermark. For example, with a single-digit watermark {3,4,…,2}, one can rewrite $\{c_1Io^{HID}\}_{\text{int}}=\{882,6721,...,79\}$ as $\{c_1Io^{HID}\}_{\text{int}}=\{8823,67214,...,792\}$. Since the watermark locates in the lowest digit of new $\{c_1Io^{HID}\}_{\text{int}}$, the impact on GI reconstruction quality can be ignored. The additional watermark can prevent data tampering from the eavesdropper during the communications between Alice and Bob, which enhances the security.

For computational GI, different random or specific matrices were applied to enhance the imaging efficiency and reduce the measurement number, e.g., Hadamard matrix [11] and random foveated matrix [41]. Since our scheme is based on computational GI, it is compatible to other random or specific matrices which can thereby reduce the data amount during the communication process.

4. Conclusions

We have proposed an optical ghost cryptography and steganography scheme on the basis of computational GI. In a non-conspicuous number integration process, the bucket signals of a hidden image and a non-secret image are firstly integrated into a series of new bucket signals, in which the ones of non-secret image dominate the number values and thereby protect the information of hidden image. RSA asymmetric cryptography is then applied to encode the new bucket signals and enhance the security of steganography process. Our ghost cryptography and steganography have been well verified by numerical simulations and a proof-of-principle optical encryption experiment. Comparing to conventional LSB steganography, ghost steganography scheme can conceal more effective data amount and has a high security level with RSA cryptography. Our work not only extends the GI into the steganography region, but also integrates RSA cryptography into GI encryption which enriches the knowledge of symmetric and asymmetric optical cryptography.

Acknowledgements

This work was supported by Start-up Research Grant (SRG2019-00174-IAPME), University of Macau. The support from Hong Kong Research Grants Council (25201416) was also acknowledged. The authors acknowledge the supports from S. Zhang's group at University of Birmingham.

References

1. Pittman TB, Shih YH, Strekalov DV, Sergienko AV. Optical imaging by means of two-photon quantum entanglement. Phys. Rev. A 1995; 52: 3429(R).
2. Bennink RS, Bentley SJ, Boyd RW. "Two-Photon" coincidence imaging with a classical source. Phys. Rev. Lett. 2002; 89: 113601.
3. Wang K, Cao DZ. Subwavelength coincidence interference with classical thermal light. Phys. Rev. A 2004; 70: 041801(R).
4. Ferri F, Magatti D, Gatti A, Bache M, Brambilla E, Lugiato A. High-resolution ghost image and ghost diffraction experiments with thermal light. Phys. Rev. Lett. 2005; 94: 183602.
5. Valencia A, Scarcelli G, D'Angelo M, Shih YH. Two-photon imaging with thermal light, Phys. Rev. Lett. 2005; 94: 063601.
6. Chen XH, Liu Q, Luo KH, Wu LA. Lensless ghost imaging with true thermal light. Opt. Lett. 2009; 34: 695-697.
7. Cheng J. Ghost imaging through turbulent atmosphere. Opt. Express 2009;17: 7916.
8. Meyers RE, Deacon KS, Shih YH. Positive-negative turbulence-free ghost imaging. Appl. Phys. Lett. 2012; 100: 131114.
9. Zhao C, Gong W, Chen M, Li E, Wang H, Xu W, Han S. Ghost imaging lidar via sparsity constraints. Appl. Phys. Lett. 2012; 101: 141123.
10. Liu XF, Yao XR, Lan RM, Wang C, Zhai GJ. Edge detection based on gradient ghost imaging. Opt. Express 2015; 23: 33802-33811.
11. Jiang S, Li X, Zhang Z, Jiang W, Wang Y, He G, Wang Y, Sun B. Scan efficiency of structured illumination in iterative single pixel imaging. Opt. Express 2019;27: 22499-22507.
12. Shapiro JH, Computational ghost imaging. Phys. Rev. A 2008; 78: 061802(R).
13. Duarte MF, Davenport MA, Takhar D, Laske JN, Sun T, Kelly KF, Baraniuk RG. Single-pixel imaging via compressive sampling. IEEE Signal Process. Mag. 2008; 25: 83.
14. Katz O, Bromberg Y, Silberberg Y. Compressive ghost imaging. Appl. Phys. Lett. 2009; 95: 131110.
15. Sun MJ, Edgar MP, Gibson GM, Sun BQ, Radwell N, Lamb R, Padgett MJ. Single-pixel three-dimensional imaging with time-based depth resolution. Nat. Commun. 2016; 7: 12010.
16. Clemente P, Duran V, Tajahuerce E, Lancis J. Optical encryption based on computational ghost imaging. Opt. Lett. 2010; 35: 2391-2393.
17. Tanha M, Kheradmand R, Ahmadi-Kandjani S. Gray-scale and color optical encryption based on computational ghost imaging. Appl. Phys. Lett. 2012; 101: 101108.
18. Wu J, Xie Z, Liu Z, Liu W, Zhang Y, Liu S. Multiple-image encryption based on computational ghost imaging. Opt. Commun. 2016; 359: 38-43.
19. Wang L, Zhao S, Cheng W, Gong L, Chen H. Optical image hiding based on computational ghost imaging. Opt. Commun. 2016; 366: 314-320.
20. Liu HC, Yang B, Guo QH, Shi JH, Guan CY, Zheng GX, Muhlenbernd H, Li GX, Zentgraf T, Zhang S. Single-pixel computational ghost imaging with helicity-dependent metasurface hologram. Sci. Adv. 2017; 3: e1701477.
21. Chen W. Ghost identification based on single-pixel imaging in big data environment. Opt. Express 2017; 25: 16509.
22. Chen W, Chen XD. Ghost imaging for three-dimensional optical security. Appl. Phys. Lett. 2013; 103: 221106.
23. Li S, Yao XR, Yu WK, Wu LA, Zhai GJ. High-speed secure key distribution over an optical network based on computational correlation imaging. Opt. Lett. 2013; 38: 2144–2146.
24. Qin Y, Zhang YY. Information encryption in ghost imaging with customized data container and XOR operation. IEEE Photon. J. 2017; 9: 7802208.
25. Sui LS, Cheng Y, Li B, Tian AL, Anand KA. Optical image encryption via high-quality computational ghost imaging using iterative phase retrieval. Laser Phys. Lett. 2018; 15: 075204.
26. Chen W, Chen XD. Marked ghost imaging. Appl. Phys. Lett. 2014; 104: 251109.
27. Chen W. Optical cryptosystem based on single-pixel encoding using the modified Gerchberg-Saxton algorithm with a cascaded structure. Journal of the Optical Society of America A, 2016; 33: 2305 – 2311.
28. Xiao Y, Zhou L, Chen W. Experimental demonstration of ghost-imaging-based authentication in scattering media, Opt. Express 2019; 27: 20558 -20566.
29. Zhou N, Jiang H, Gong L, Xie X. Double-image compression and encryption algorithm based on co-sparse representation and random pixel exchanging. Opt. Lasers Eng. 2018; 110: 72-79.
30. Yu SS, Zhou NR, Gong LH, Nie Z. Optical image encryption algorithm based on the phase-truncated short-time fractional Fourier transform and hyperchatic system. Opt. Lasers Eng. 2020; 124: 105816.
31. Johnson NF, Jajodia S. Exploring steganography: Seeing the unseen. IEEE Computer 1998; 31: 26-34.
32. Katzenbeisser S. Petitcolas F. Information hiding techniques for steganography and digital watermarking. Norwood: Artech House; 2000.
33. Lin CC, Tsai WH, Secret image sharing with steganography and authentication. Journal of Systems and Software 2004; 73: 405-414.
34. Cox I, Miller M, Bloom J, Fridrich J, Kalker T, Digital water-marking and steganography. Morgan Kaufmann, San Francisco, Calif, USA, 2nd edition; 2008.
35. Hamam H. Digital holography-based steganography. Opt. Lett. 2010; 35: 4175-4177.
36. Candes E, Romberg J, Tao T. Robust uncertainty principles: exact signal reconstruction from highly incomplete frequency information. IEEE Trans. Inf. Theory 2006; 52: 489.
37. Liu HC, Zhang S. Computational ghost imaging of hot objects in long-wave infrared range. Appl. Phys. Lett. 2017; 111: 031110.
38. Rivest R, Shamir A, Adleman L, A method for obtaining digital signatures and public-key cryptosystems. Communications of ACM 1978; 21: 120-126.
39. Goldreich O. Foundations of cryptography I: Basic Tools. Cambridge University Press, Cambridge; 2001.
40. Elgamal T. A public key cryptosystem and a signature scheme based on discrete logarithms. IEEE Transactions on Information Theory 1985; 31: 469-472.
41. Phillips DB, Sun MJ, Taylor JM, Edgar MP, Barnett SM, Gibson GM, Padgett MJ. Adaptive foveated single-pixel imaging with dynamic supersampling. Sci. Adv. 2017; 3: e1601782.