

Efficient single-pixel imaging encrypted transmission based on 3D Arnold transformation

Zhen-Yu Liang(梁振宇), Chao-Jin Wang(王朝瑾), Yang-Yang Wang(王阳阳), Hao-Qi Gao(高皓琪), Dong-Tao Zhu(朱东涛), Hao-Li Xu(许颢砾), and Xing Yang(杨星)

Citation: Chin. Phys. B, 2024, 33 (**3**): 034204. DOI: 10.1088/1674-1056/acf204
Journal homepage: http://cpb.iphy.ac.cn; http://iopscience.iop.org/cpb

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

Optical image encryption algorithm based on a new four-dimensional memristive hyperchaotic system and compressed sensing

Yang Du(都洋), Guoqiang Long(隆国强), Donghua Jiang(蒋东华), Xiuli Chai(柴秀丽), and Junhe Han(韩俊鹤)
Chin. Phys. B, 2023, 32 (**11**): 114203. DOI: 10.1088/1674-1056/acef08

Complex-amplitude Fourier single-pixel imaging via coherent structured illumination

Hong-Yun Hou(侯红云), Ya-Nan Zhao(赵亚楠), Jia-Cheng Han(韩佳成), De-Zhong Cao(曹 德忠),Su-Heng Zhang(张素恒), Hong-Chao Liu(刘宏超), and Bao-Lai Liang(梁宝来)
Chin. Phys. B, 2023, 32 (**6**): 064201. DOI: 10.1088/1674-1056/ac8e9a

Color-image encryption scheme based on channel fusion and spherical diffraction

Jun Wang(王君), Yuan-Xi Zhang(张沅熙), Fan Wang(王凡), Ren-Jie Ni(倪仁杰), and Yu-Heng Hu(胡玉衡)
Chin. Phys. B, 2022, 31 (**3**): 034205. DOI: 10.1088/1674-1056/ac1b87

Ghost imaging-based optical cryptosystem for multiple images using integral property of the Fourier transform

Yi Kang(康祎), Leihong Zhang(张雷洪), Hualong Ye(叶华龙), Dawei Zhang(张大伟), and Songlin Zhuang(庄松林)
Chin. Phys. B, 2021, 30 (**12**): 124207. DOI: 10.1088/1674-1056/ac0815

Fast Fourier single-pixel imaging based on Sierra-Lite dithering algorithm

Zhen-Yu Liang(梁振宇), Zheng-Dong Cheng(程正东), Yan-Yan Liu(刘严严), Kuai-Kuai Yu(于快快), Yang-Di Hu(胡洋頔)
Chin. Phys. B, 2019, 28 (**6**): 064202. DOI: 10.1088/1674-1056/28/6/064202

Efficient single-pixel imaging encrypted transmission based on 3D Arnold transformation

Zhen-Yu Liang(梁振宇)[1,2], Chao-Jin Wang(王朝瑾)[1], Yang-Yang Wang(王阳阳)[1], Hao-Qi Gao(高皓琪)[1], Dong-Tao Zhu(朱东涛)[1], Hao-Li Xu(许颢砾)[1], and Xing Yang(杨星)[1,2,†]

[1] *State Key Laboratory of Pulsed Power Laser Technology, National University of Defense Technology, Hefei* 230001, *China*
[2] *Advanced Laser Technology Laboratory of Anhui Province, Hefei* 230001, *China*

(Received 4 June 2023; revised manuscript received 16 August 2023; accepted manuscript online 21 August 2023)

Single-pixel imaging (SPI) can transform 2D or 3D image data into 1D light signals, which offers promising prospects for image compression and transmission. However, during data communication these light signals in public channels will easily draw the attention of eavesdroppers. Here, we introduce an efficient encryption method for SPI data transmission that uses the 3D Arnold transformation to directly disrupt 1D single-pixel light signals and utilizes the elliptic curve encryption algorithm for key transmission. This encryption scheme immediately employs Hadamard patterns to illuminate the scene and then utilizes the 3D Arnold transformation to permutate the 1D light signal of single-pixel detection. Then the transformation parameters serve as the secret key, while the security of key exchange is guaranteed by an elliptic curve-based key exchange mechanism. Compared with existing encryption schemes, both computer simulations and optical experiments have been conducted to demonstrate that the proposed technique not only enhances the security of encryption but also eliminates the need for complicated pattern scrambling rules. Additionally, this approach solves the problem of secure key transmission, thus ensuring the security of information and the quality of the decrypted images.

Keywords: single-pixel imaging, 3D Arnold transformation, elliptic curve encryption, image encryption

PACS: 42.30.–d, 42.68.Sq, 07.05.Pj **DOI:** 10.1088/1674-1056/acf204

1. Introduction

Single-pixel imaging (SPI)[1] has gained much attention in recent years due to its potential in recovering 2D or 3D scene information from 1D light signals using single-pixel detectors. This is particularly relevant to the fast-growing modern spatial light modulation techniques. SPI systems have the potential for a wide range of applications in remote sensing,[2–4] laser radar[5–10] and low-dose x-ray medical imaging [11,12] due to the flexible optical field control, high sensitivity and resistance to atmospheric turbulence.

Compared with traditional imaging techniques, SPI lowers the requirements on detectors. As compensation, this technique requires more measurements and is thus time-consuming. Numerous methods have been put forth to increase the image formation speed and image quality of SPI. By employing image priors such as sparsity, compressive sensing algorithms[13,14] can drastically reduce the measurements required to produce a high-quality image under random illuminations. Instead of random patterns, deterministic model-based SPI approaches use orthogonal basis patterns, for example the Fourier[15] and Hadamard[16] approaches, for SPI modulation to eliminate redundancy between different illuminations. Additionally, deep learning has been used for SPI[18–21] reconstruction algorithms. The trained deep neural network can be used to improve imaging quality while retaining high computational efficiency.

Apart from SPI modulation and reconstruction methods research, the principle of SPI, which transforms 2D or 3D image data into a 1D light signal, also offers promising prospects in image compression and transmission. However, during data communication, these unusual light signals in public channels can easily attract the attention of eavesdroppers. Traditional techniques for encrypting optical images, such as random phase mask (RPM),[22,23] optical inference principle-based encryption,[24,25] phase retrieval algorithms[25] and computer holography,[26,27] are usually capable of providing high-speed parallel processing and secure transmission of 2D images by hiding information of varied dimensions. In recent years, Lai *et al.*[28–31] have proposed a series of well-designed chaotic systems to realize high-security image encryption. By controlling the dimensions of chaotic signals, encryption operations can be performed in high-dimensional spaces.

Unlike the traditional encryption methods, the issues of SPI-based optical encryption are now receiving ever-increasing attention as they provide an alternative for solving problems in optical information processing. Previous works[32–36] have focused on modulating the target scenes through a series of computer-generated pseudo-random patterns. These patterns are treated as secret keys shared only between the sender of the message and its authorized recipient. The light intensity signals of the single-pixel detector are then encrypted and transmitted as ciphertext to ensure secure communication. Scrambling orthogonal basis patterns is a

†Corresponding author. E-mail: yangxing17@nudt.edu.cn

© 2024 Chinese Physical Society and IOP Publishing Ltd

type of encryption transmission scheme that differs from direct encryption transmission using pseudo-random patterns.[37–41] The message sender utilizes a set of rules to modulate the target light field, typically using only the sampling strategy and scrambling rules of orthogonal basis patterns as the secret key. These methods not only improve the quality of decrypted images but also reduce the key space. In addition to orthogonal basis pattern encryption, there are other types of single-pixel encryption schemes, such as visual cryptography,[42] watermarking and steganography techniques[43–46] and encryption with a metasurface key.[47]

Despite the advantages of single-pixel encryption schemes, existing methods still face several major issues such as severe noise in the decrypted results, difficulty in ensuring key transmission security and complex rules for designing orthogonal basis patterns. To address these issues, we propose an SPI encrypted transmission scheme based on 3D Arnold transformation and elliptic curve cryptography. The proposed method does not require complex pixel permutation rules for orthogonal basis patterns. Instead, it employs Hadamard patterns to illuminate the scene, and then uses the 3D Arnold transformation to permutate the 1D light signals of the single-pixel detector (plaintext information). The transformation parameters serve as the secret key, while the security of key transmission is guaranteed by an elliptic curve-based key exchange mechanism. Compared with existing encryption schemes, our proposed technique not only enhances the security of encryption but also eliminates the need for complicated pattern scrambling rules and solves the problem of secure key transmission. As a result, both the security and quality of information decryption are ensured. In summary, our main contributions can be summarized into three points:

(1) We propose a random scramble method that directly transforms the 1D single-pixel light signals and eliminates the need for the design of a complex illumination pattern. Our proposed method not only greatly enhances the security of transmission of single-pixel detection data but also maximizes the accuracy of decryption results.

(2) We present a 3D Arnold transformation-based 1D signal scrambling method that has achieved satisfactory encryption results on various images while demonstrating state-of-the-art performance across different sampling rates.

(3) We develop an elliptic curve-based key exchange mechanism with the proposed 1D signal scrambling method. This mechanism further enhances the security of key transmission by overcoming the challenges associated with conventional symmetric single-pixel encryption schemes.

2. Methodology

In this section, we first utilize non-scrambling Hadamard patterns to illuminate the scene. Then, we propose a novel 3D Arnold scramble method for a 1D single-pixel detection signal on the basis of a differential detection system. Finally, we introduce an elliptic curve-based key exchange mechanism to encrypt the Arnold transformation parameters. At the end of this section, we briefly explain how to encrypt and decrypt using the 3D Arnold method and the key exchange mechanism using a practical example. The schematic of whole technique is shown in Fig. 1.

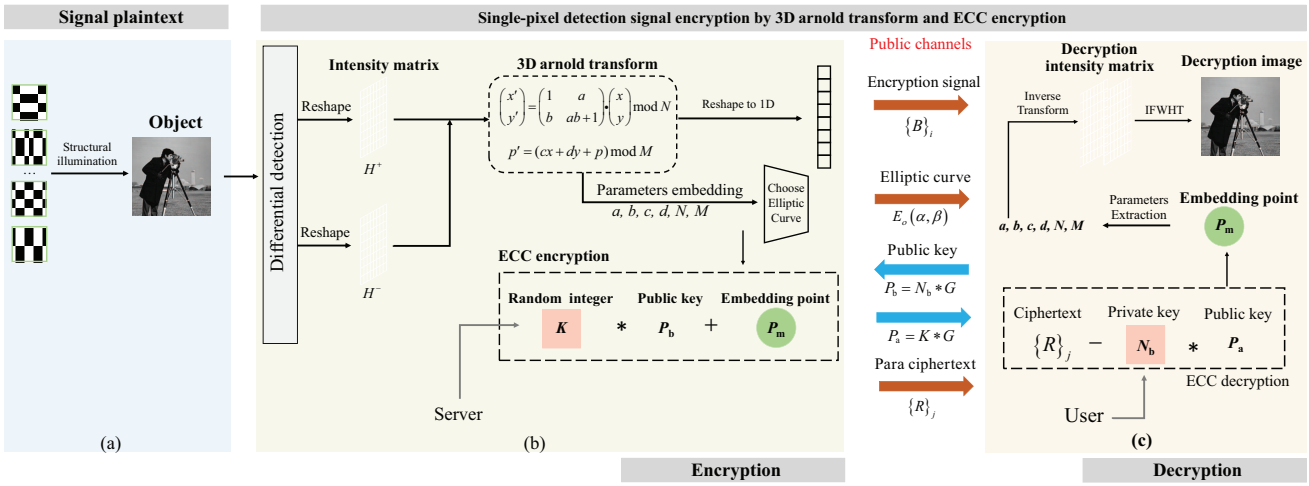


Fig. 1. Schematic of our proposed technique: (a) signal plaintext generation process, (b) encryption process, (c) decryption process (ECC, elliptic curve cryptography).

2.1. Structural illumination with Hadamard patterns

In a typical SPI framework, a 1D light intensity signal $b^{(i)}$ is obtained by actively illuminating the scene $T(x,y)$ with pre-designed two-dimensional patterns $I_r^{(i)}(x,y)$. The single-pixel detector records the reflected or transmitted signals by the scene

$$b^{(i)} = \int I_r^{(i)}(x,y)\, T(x,y)\, \mathrm{d}x\mathrm{d}y. \tag{1}$$

The illumination patterns can be designed in various forms, such as random intensity patterns or orthogonal basis

patterns. In our method, we utilize Hadamard basis patterns to illuminate the scene, and the single-pixel detection 1D light signal is mathematically equivalent to the inner product between the Hadamard basis patterns and the scene

$$b_H^{(i)}(u,v) = \sum_{x=0}^{M-1}\sum_{y=0}^{N-1} I_H^{(i)}(x,y;u,v)\,T(x,y), \tag{2}$$

where $I_H^{(i)}(x,y;u,v)$ denotes the Hadamard basis pattern in the Hadamard domain corresponding to the coordinates (u,v). Each measurement can be interpreted as the calculation of each Hadamard coefficient in the spectral transformation of the scene. Since the Hadamard basis patterns consist of two elements, $+1$ and -1, it is not practical to use negative illumination during experimental procedures. Therefore, the Hadamard coefficients of the scene can be obtained by projecting $I_H^{(i)}(x,y;u,v)$ and its complementary pattern $\left[1-I_H^{(i)}(x,y;u,v)\right]$

$$H(u,v) = b_{H^+}^{(i)}(u,v) - b_{H^-}^{(i)}(u,v). \tag{3}$$

Based on differential detection, 1D light signals can be separated into two components, b_{H^+} and b_{H^-}, which are utilized in the subsequent encryption process.

2.2. The 3D Arnold transformation for single-pixel 1D detection signal

The Arnold transformation, also known as the Arnold cat map,[48] is a method of discrete chaotic mapping that repeatedly folds and stretches input images within a limited region. Due to its well-established chaotic characteristics and easily controllable parameters, it is widely used in digital image encryption. The commonly used Arnold transformation is the 2D form

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} 1 & a \\ b & ab+1 \end{pmatrix} \cdot \begin{pmatrix} x \\ y \end{pmatrix} \bmod N, \tag{4}$$

where x and y denote the original position of any pixel in the image, x' and y' indicate the transformed pixel location, a and b serve as controlling factors and N is the dimension of the square image.

To achieve more secure and efficient pixel transformations, the 2D Arnold transformation can be extended to higher dimensions. By introducing new parameters c and d, the higher-dimensional 3D Arnold transformation[49] has been developed

$$\begin{pmatrix} x' \\ y' \\ z' \end{pmatrix} = \begin{pmatrix} 1 & a & 0 \\ b & ab+1 & 0 \\ c & d & 1 \end{pmatrix} \cdot \begin{pmatrix} x \\ y \\ z \end{pmatrix} \bmod N, \tag{5}$$

where z represents the grayscale value at any pixel location (x, y), and z' denotes the transformed grayscale value. To facilitate computation, we have employed the modified form of the 3D Arnold transformation proposed by Liu *et al.*[50]

$$\begin{cases} \begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} 1 & a \\ b & ab+1 \end{pmatrix} \cdot \begin{pmatrix} x \\ y \end{pmatrix} \bmod N, \\ p' = (cx+dy+p) \bmod M, \end{cases} \tag{6}$$

where p and p' denote the grayscale values at the same pixel location before and after transformation, respectively. M represents the maximum grayscale value of the image, which is usually 255 (for an 8-bit grayscale image from 0 to 255). It implies that not only the pixel positions of the image are disordered, but also the grayscale values of the image are scrambled. This will further enhance the security of image encryption. The plaintext image can be recovered by applying the inverse 3D Arnold transformation to the ciphertext resulting from the following equation:

$$\begin{cases} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} ab+1 & -a \\ -b & 1 \end{pmatrix} \cdot \begin{pmatrix} x' \\ y' \end{pmatrix} \bmod N, \\ p = (2M+p'-cx-dy) \bmod M. \end{cases} \tag{7}$$

Therefore, utilizing the 3D Arnold transformation for image encryption would result in a more robust security effect compared with the 2D transformation method. It is difficult for an attacker to obtain accurate results if the encryption key or algorithm remains confidential.

In this paper, we propose the idea of applying the 3D Arnold transformation to 1D light intensity signals. As shown in Fig. 1, we transform the single-pixel detection values acquired into 2D matrices H^+ and H^- of light intensity. It should be noted that while pixel values in image encryption applications can be quantified using a grayscale value of 255, the single-pixel measurement values typically differ from image grayscale values. Therefore, in practical implementation, we utilize the maximum value in the light intensity as one of the transmitted parameters for the 3D Arnold transformation of the light intensity matrix.

2.3. Elliptic curve Diffie–Hellman key exchange

Elliptic curve cryptography (ECC) is a public key encryption method proposed by Koblitz and Miller in 1985.[51] It is based on the theory of elliptic curves. By utilizing the discrete logarithm difficulty of the Abel group composed of points on an elliptic curve over a finite field, it can achieve encryption, decryption and a digital signature. By associating addition operations in elliptic curves with modulo multiplication operation in a discrete logarithm, it is possible to establish a corresponding cryptographic system based on elliptic curves. Compared with the traditional public key encryption system RSA, ECC requires a significantly smaller of key size to achieve the same level of security performance. Here, an elliptic curve that satisfies the Weierstrass equation over a finite field $\mathbb{F}_p$ is defined as

$$y^2 \bmod p = x^3 + \alpha x + \beta \bmod p, \tag{8}$$

where x, y, α, $\beta \in \mathbb{F}_p$, and satisfies $4\alpha^3 + 27\beta^2 \neq 0$. The security of the elliptic curve encryption mechanism is based on the difficulty of solving the discrete logarithm problem on elliptic curves. Assuming two points G and Q on an elliptic curve, where $Q = KG$ for some integer K. Although it is relatively easy to calculate Q using the four arithmetic operations of finite field, computing K from G and Q is a highly challenging task. Here, G is referred to as the base point, K is the private key and Q is the public key.

The elliptic curve Diffie–Hellman (ECDH) key exchange mechanism combines elliptic curves with the Diffie–Hellman protocol[52] to provide a shared key exchange method over an insecure channel. The process involves the following steps:

(1) The server publicly selects an elliptic curve and randomly chooses a point on the curve, which is referred to as the base point G. Simultaneously, a random positive integer K is selected as the private key, while the corresponding public key P_s is generated and made available to the public.

(2) The user selects an arbitrary positive integer N_u as their private key based on the elliptic curve and base point selected by the server. Subsequently, a corresponding public key $P_u = N_u G$ is generated and made publicly available to the user.

(3) The server and user compute a shared ECDH key based on their respective private keys.

For the server

$$P_{AB} = KP_u = KN_u G. \tag{9}$$

For the user

$$P_{AB} = N_u P_s = N_u KG. \tag{10}$$

In this paper, we adopt the idea of applying the ECDH key exchange mechanism to the chosen parameters from 3D Arnold transformation. As shown in Fig. 1, we first embed the secret key in the 3D Arnold transformation, such as a, b, M and the iteration times, into an elliptic curve. Subsequently, a private key is randomly selected to generate an exchangeable public key. The key is then further encrypted using the four arithmetic operations of finite field. Finally, the secure transmission of the key in the public channel is realized.

2.4. Encryption and decryption process

The proposed encryption process mainly consists of six steps:

Step 1 Record the light intensity values of an SPI system based on Hadamard differential detection; these are subsequently transformed from the one-dimensional vector format to the two-dimensional differential light intensity matrix H^+ and H^-.

Step 2 Apply 3D Arnold transformation to H^+ and H^-. The transformation parameters such as a, b, c, d, N, M and the iteration times serve as secret keys.

Step 3 Randomly choose an elliptic curve $E_p(\alpha, \beta)$; a random point on the curve serves as the base point G. Then the server selects a random positive integer K to generate the public key $P_s = KG$. All of above information is shared with the user through a public channel.

Step 4 The server embeds the parameters into the selected curve. Consider parameter M as an illustrative example. P_m denotes a point on the embedded elliptic curve.

Step 5 After receiving the elliptic curve from the server, the user selects a random positive integer N_u as a private key, and generates a public key $P_u = N_u G$ which can be shared in public channel.

Step 6 The server receives the public key P_u from the user, and generates ciphertext by $C = P_m + KP_u$. The ciphertext and encrypted single-pixel detection values can be shared with the user in a public channel, thus completing the encryption process.

The proposed decryption process mainly consists of three steps:

Step 1 After receiving the ciphertext and encrypted single-pixel detection values from the server, the user decrypts P_m by using the private key N_u

$$P_m = C - N_u P_s = P_m + K(N_u G) - N_u(KG). \tag{11}$$

Step 2 Extract the 3D Arnold transform parameters from P_m by embedding rules, and apply an inverse 3D Arnold transform to recover the single-pixel detection plaintext.

Step 3 Apply an inverse Hadamard transform algorithm or other compressed sensing algorithms; the original image information can be reconstructed, thus completing the decryption process.

3. Results

In this section the proposed method is verified by both computer simulation and optical experiments.

3.1. Simulation results

To validate our method, we perform computer simulations on Intel CPU i7-12700KF@3.60 GHz hardware with 32 GB RAM. The gray-scale image 'Cameraman' is used as the ground truth.

3.1.1. Encryption and decryption process

Firstly, we generate 64×64 Hadamard patterns with a 'zigzag' order.[53] The 1D single-pixel detection signal is shown in Fig. 2(b). It is obvious that the unencrypted single-pixel intensity values are concentrated and exhibit a conspicuous regularity. If an eavesdropper has a certain knowledge of Hadamard transformation, they can easily identify that this signal has been encrypted using an SPI system. The eavesdropper can directly use the inverse Hadamard transformation

to obtain the correct image information, which would expose a significant risk of data leakage.

Secondly, we set the controllable parameters in a 3D Arnold transformation, $a = b = 3$, $c = d = 7$, $M = 1994$, and the iteration times are set as 10. The plaintext of single-pixel light intensity values is directly encrypted into ciphertext via selected parameters. The generated ciphertext signal is depicted in Fig. 2(c). It can be observed that the single-pixel light intensity values applying the proposed scrambling method resemble noise, lacking any discernible rules or orders. If an eavesdropper does not have access to the decryption key, using the inverse Hadamard transformation algorithm alone will not be sufficient to obtain accurate target image information, as illustrated in Fig. 2(d).

Finally, we achieve encryption using the parameters set in the 3D Arnold transformation through the ECDH key exchange mechanism, as detailed below:

(1) We select an elliptic curve with $p = 123457$, $\alpha = 5376$, $\beta = 2438$ and randomly choose a point $G = (2225, 75856)$ on the curve.

(2) Considering parameter M as an illustrative example, we utilize the value of M as the horizontal axis on the curve, of which the embedding point P_{m} is (1994, 104163). We set the server's private key $K = 35$, and the public key P_{s} is (112799, 97369).

(3) The user receives elliptic curve parameters and P_{s} in a public channel, and shares the public key $P_{\mathrm{u}} = (94953, 15581)$ by setting the private key $N_{\mathrm{u}} = 95$.

(4) We generate ciphertext $C = (106784, 55261)$, and the encryption process is completed.

(5) The user decrypts the ciphertext according to Eq. (11), which will recover the controllable parameters of the 3D Arnold transformation. Then, the user applies the inverse 3D Arnold transformation to reconstruct the original single-pixel light signals, and the decryption process is completed.

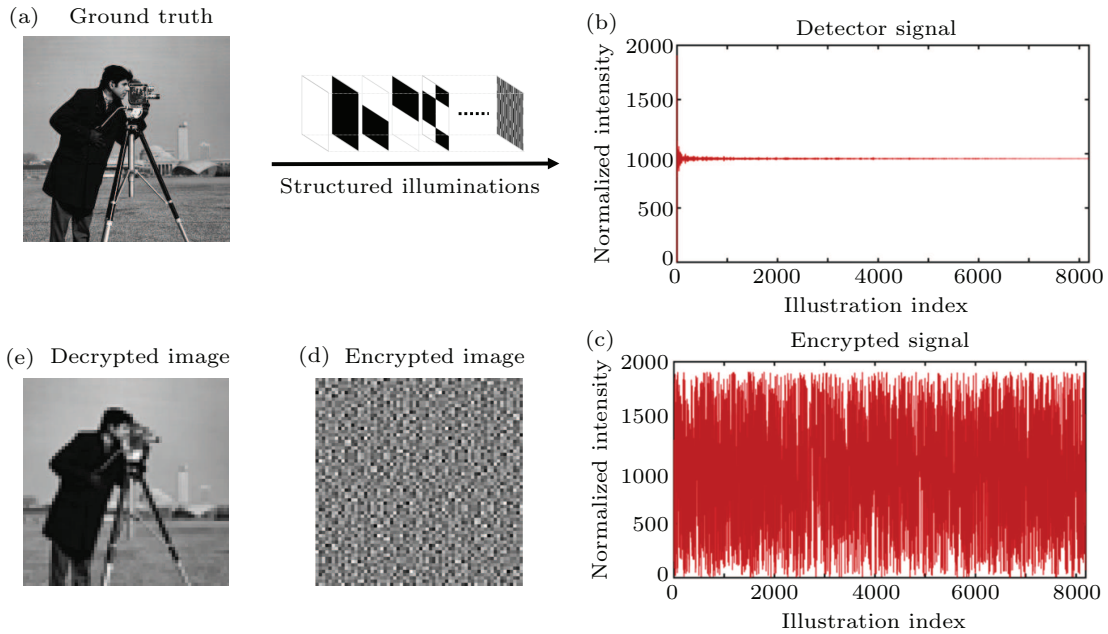


Fig. 2. Simulation results: (a) the ground truth 'Cameraman'; (b) single-pixel detection light signal without encryption; (c) signal encrypted by 3D Arnold transformation; (d) recovered image without the correct key; (e) recovered image with the correct key.

3.1.2. Security analysis

To further illustrate the security of our proposed method, in this section we discuss the security analysis of the proposed method, for example correlation analysis, sensitivity analysis with respect to the key and plaintext.

(1) Correlation analysis We have calculated the correlation coefficient (CC) between plaintext and ciphertext for quantitative evaluation. CC is defined as follows:

$$CC = \frac{\sum_m \sum_n (A_{mn} - \bar{A})(B_{mn} - \bar{B})}{\sqrt{\left(\sum_m \sum_n (A_{\max} - \bar{A})^2\right)\left(\sum_m \sum_n (\bar{B}_{\max} - \bar{B})^2\right)}}, \quad (12)$$

where A and B denote two different two-dimensional distributions and m and n are the indices of the rows and columns, respectively. In this paper, A represents the encrypted image after 3D Arnold transformation and B represents the original image. The security of encryption is determined by calculating the CC value between A and B. The higher CC is, the stronger the correlation between the two images, indicating a lower level of security. Furthermore, if the CC value is negative, it indicates that the two images are negatively correlated. We conduct a comparative analysis between the proposed methodology and two baseline SPI encryption techniques: Hadamard patterns permutation (HPP) and random patterns (RP). The grayscale images 'Cameraman' and 'Baboon' are also adopted as two typical ground truths. In addition, the CC values under

different sampling ratios are also calculated. Table 1 shows the *CC* values for the simulation, where M_{b} denotes the permutation block size in HPP.

According to the results presented in Table 1, it can be observed that the *CC* values for the reconstructed images without the correct key are significantly lower than for the other two baseline methods. The results indicate that when applied to the same object, our proposed method yields the smallest *CC* value at sampling ratios of 0.1, 0.25 and 1. When the sampling ratio is 0.5, although the *CC* value obtained by our method is not the minimum it is similar to the comparable values. Meanwhile, for the same object, when the sampling ratio changes, the *CC* values obtained by our proposed method do not change significantly. In other words, our proposed method has the lowest sensitivity to the sampling ratio itself.

(2) Sensitivity analysis An ideal encryption procedure should be sensitive with respect to the secret key, i.e., the change of a single bit in the secret key should produce a completely different encrypted image. We measured the number of pixel changing rate (NPCR) and unified averaged changed intensity (UACI) values to see the influence of changing a single pixel in the original image on the encrypted image using the the proposed method. We take two encrypted images C and C', whose corresponding original images have a difference of only one pixel. NPCR and UACI are defined as

$$\mathrm{NPCR} = \frac{\sum_{i=1}^{m}\sum_{j=1}^{n} D(i,j)}{m \times n} \times 100\%, \tag{13}$$

$$\mathrm{UACI} = \frac{\sum_{i=1}^{m}\sum_{j=1}^{n} |C(i,j) - C'(i,j)|}{m \times n \times I_{\max}} \times 100\%, \tag{14}$$

where m and n are the width and height of the encrypted image, $I_{\max}$ is the maximum value of pixel intensity and $D(i,j)$ is defined as

$$D(i,j) = \begin{cases} 0 \text{ if } C(i,j) = C'(i,j), \\ 1 \text{ if } C(i,j) \neq C'(i,j). \end{cases} \tag{15}$$

The results of NPCR and UACI are shown in Table 2. According to the results, NPCR and UACI values for the reconstructed images using our method are significantly better than for the other two methods. These results indicate that this method can provide higher security than existing methods.

Table 1. Results for *CC* values.

Ground truth	Method	Sampling ratio			
		10%	25%	50%	100%
Peppers	RP	–0.0921	0.0356	**–0.0103**	–0.0192
	HPP (M_{b} =1)	0.0528	0.0237	–0.0308	–0.0145
	HPP (M_{b} =4)	0.0668	–0.0199	0.0601	–0.0042
	HPP (M_{b} =8)	–0.1451	–0.0583	0.0857	-0.0347
	Ours	**–0.0061**	**–0.0065**	0.0108	**0.0013**
Cameraman	RP	0.1027	–0.0354	0.0157	–0.0400
	HPP (M_{b} =1)	0.0985	–0.0169	0.0095	–0.0343
	HPP (M_{b} =4)	-0.1045	0.0325	0.0815	0.0327
	HPP (M_{b} = 8)	–0.0256	–0.0236	–0.0107	–0.0123
	Ours	**–0.0007**	**–0.0076**	**–0.0035**	**0.0007**
Baboon	RP	0.0266	-0.0096	-0.0170	0.0031
	HPP (M_{b} =1)	-0.0149	0.0400	-0.0199	-0.0117
	HPP (M_{b} = 4)	–0.0230	–0.1070	–0.0552	–0.0103
	HPP (M_{b} =8)	–0.0217	–0.0031	**0.0097**	0.0036
	Ours	**–0.0057**	**0.0080**	0.0132	**0.0024**

Table 2. Results for NPCR and UACI values.

Type	Ground truth	Method				
		Ours	RP	HPP (M_{b} = 1)	HPP (M_{b} = 4)	HPP (M_{b} = 8)
NPCR (100%)	Peppers	**99.34**	60.74	0.49	0.49	0.03
	Cameraman	**98.17**	57.76	0.02	0.02	0.02
	Baboon	**99.90**	42.92	0.03	0.02	0.02
UACI (100%)	Peppers	**14.80**	0.27	0.01	0.01	0.01
	Cameraman	**16.11**	0.25	0.01	0.01	0.01
	Baboon	**7.60**	0.17	0.01	0.01	0.01

3.1.3. Analysis of decrypted image quality

We also conduct a comparative evaluation of the quality of image reconstruction with the correct key. The reconstructed results under different sampling ratios are shown in Fig. 3.

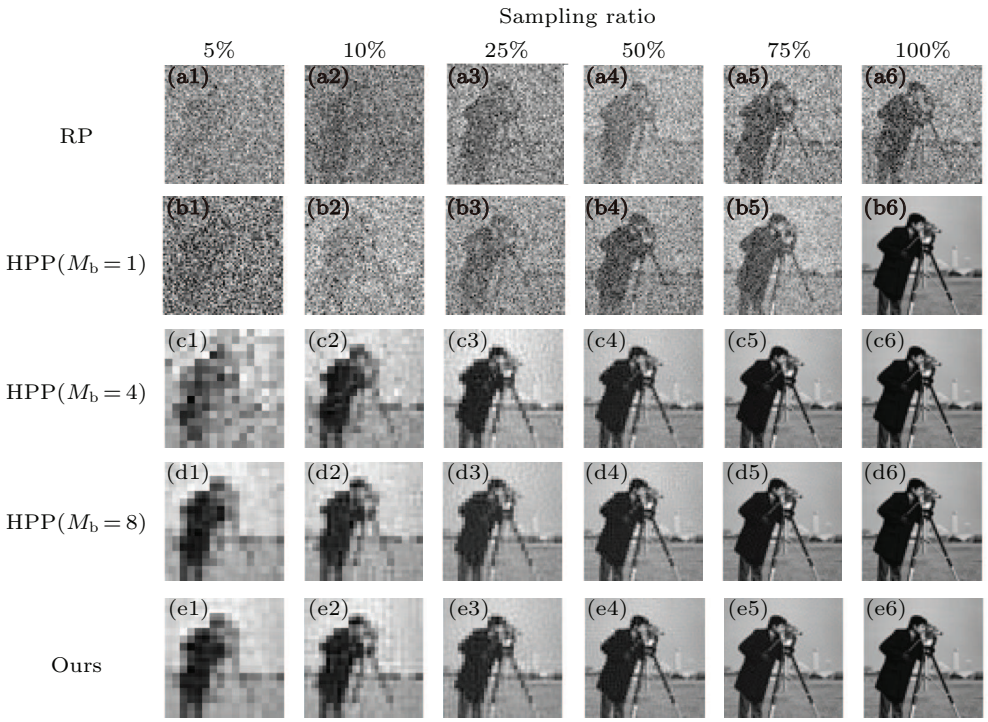


Fig. 3. Simulation results of the decryption process with the correct key at different sampling ratios. (a1)–(a6) Reconstruction images using the RP method. (b)–(d) Reconstruction images using the HPP method with different pixel permutation parameters M_b. (e1)–(e6) Reconstruction images using our proposed method.

Table 3. The SSIM results of image reconstruction.

Ground truth	Method	Sampling ratio			
		10%	25%	50%	100%
Peppers	RP	0.1727	0.2643	0.3393	0.4431
	HPP ($M_b = 1$)	0.1782	0.2899	0.4428	1.0000
	HPP ($M_b = 4$)	0.5683	0.7911	0.8867	1.0000
	HPP ($M_b = 8$)	0.6132	0.8003	0.9010	1.0000
	Ours	**0.6241**	**0.8113**	**0.9159**	**1.0000**
Cameraman	RP	0.1006	0.1681	0.2075	0.2780
	HPP ($M_b = 1$)	0.1012	0.2688	0.4606	1.0000
	HPP ($M_b = 4$)	0.4361	0.6459	0.8026	1.0000
	HPP ($M_b = 8$)	0.5446	0.7021	0.8467	1.0000
	Ours	**0.5544**	**0.7215**	**0.8606**	**1.0000**
Baboon	RP	0.1738	0.2527	0.3275	0.4468
	HPP ($M_b = 1$)	0.1799	0.3089	0.4464	1.0000
	HPP ($M_b = 4$)	0.5402	0.7599	0.8804	1.0000
	HPP ($M_b = 8$)	0.5662	0.7690	0.8971	1.0000
	Ours	**0.6201**	**0.7718**	**0.9104**	**1.0000**

As shown in Fig. 3, the quality of reconstructed image with the correct key improves as the sampling ratio increases in the three schemes. It is evident that the RP and HPP ($M_b = 1, 4$) methods are more susceptible to the influence of the sampling ratio. Our proposed method exhibits a degree of visual similarity that is comparable to that of the HPP ($M_b = 8$) method, which demonstrates that the proposed technique can achieve a better quality reconstructed image than other two baseline methods. To quantitatively evaluate the quality of reconstruction images, the structural similarity index (SSIM)[54] is employed.

The SSIM results are shown in Table 3. For the same sampling ratio, our proposed method achieves the best SSIM value for different ground truths. Therefore, the above results suggest that our proposed method not only achieves more secure encryption, but also produces a competitive reconstructed image.

3.2. Experimental results

We performed an experiment to demonstrate the proposed technique. A printed character '3' was used as an object. A schematic of our experimental setup is shown in Fig. 4. We used a DLP development kit (DLP 4710EVM-LC) for spatial light illumination, and generated Hadamard patterns in a zigzag order. A Si switchable gain detector (Thorlabs PDA100A2) was used to measure the intensity of the reflected light from the object. The electronic signals were transferred to the computer via a data acquisition board (NI USB-6343).

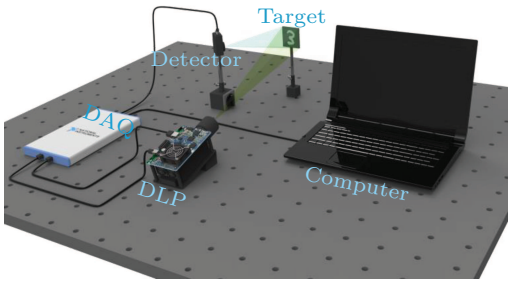


Fig. 4. Diagram of the experimental setup: DLP, digital light processing development kit (DLP 4710EVM-LC); detector, single-pixel detector (Thorlabs PDA100A2); DAQ, data acquisition board (NI USB-6343).

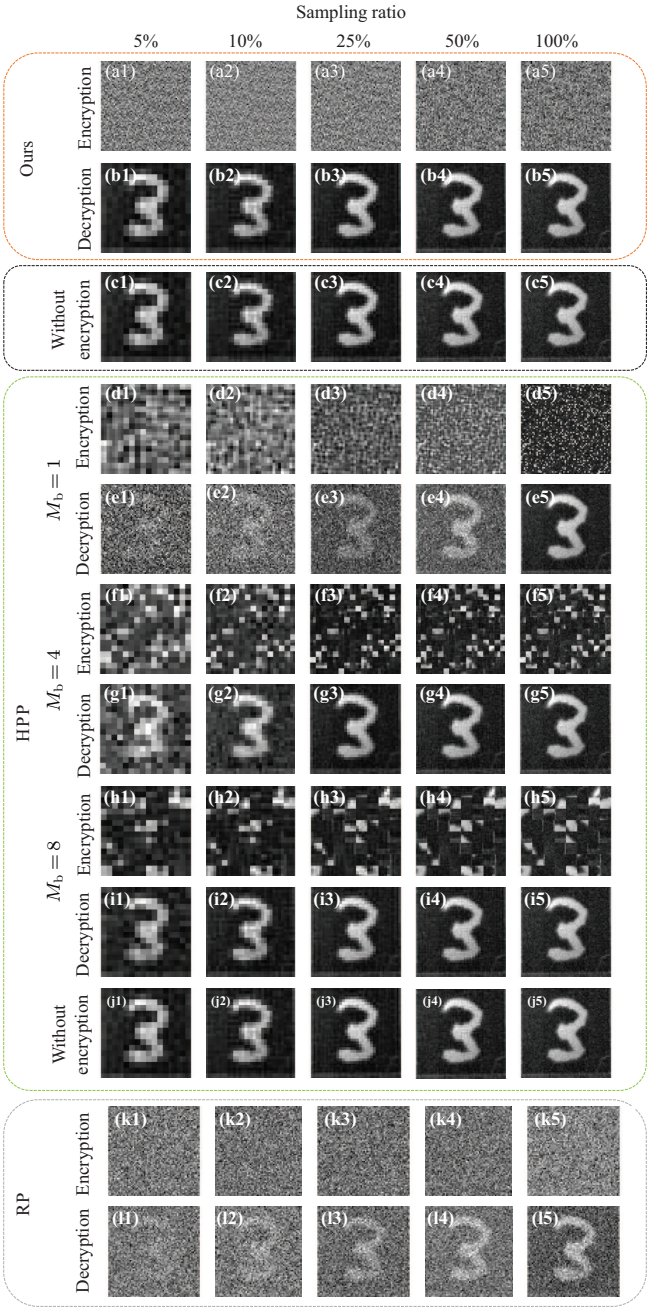


Fig. 5. Experimental results of encryption and decryption at different sampling ratios. (a)–(c) Reconstruction images using our method. (b)–(j) Reconstruction images using the HPP method with different pixel permutation parameters M_b. (k), (l) Reconstruction images using the RP method.

Figure 5 shows the experimental results of the reconstruction for different sampling ratios. The first (top) panel displays the recovered encrypted image and final decrypted image produced by our proposed method with different sampling ratios. The second panel showcases the original image without encryption for various sampling ratios. The third panel illustrates the recovered encrypted image and final decrypted image produced by HPP with different M_b values and sampling ratios. At the bottom of this panel, reconstructions by original Hadamard SPI without encryption are shown for different sampling ratios. Finally, the fourth panel displays the recovered encrypted image and final decrypted image produced by conventional encrypted ghost imaging with random illumination patterns for different sampling ratios.

The quality of the reconstructed image improves as the sampling ratio increases in three schemes. It is evident that the RP and HPP ($M_b = 1, 4$) methods are more susceptible to the influence of sampling ratio. Our proposed method exhibits a degree of visual similarity that is comparable to that of the HPP ($M_b = 8$) method. It can be observed that the object scene is not recognizable from the reconstruction algorithm for different sampling ratios. In the second panel, the quality of the decrypted images is unaffected by encryption operation compared with the reconstructed images in the third panel. The experimental results are consistent with the simulation results.

4. Conclusion

In summary, we propose an efficient framework for encrypted transmission of SPI data. We employ direct scrambling of the 1D light signal from the single-pixel detector instead of generating pseudo-random illumination patterns or designing complex permutation rules for orthogonal basis patterns. The improved 3D Arnold transformation in 1D signal encryption operations introduces stronger security for the encryption system. To solve the problem of key transmission in public channels, we construct a secure key transmission mechanism by applying the ECDH key exchange protocol. Simulation and experimental results demonstrate our proposed scheme, ensuring both security and good quality decryption of information. This work generates new insights for encrypted transmission of SPI data and provides a solution for developing a secure SPI data communication system for remote sensing or laser radar.

Acknowledgements

The authors thank Mr Yi Chen and Mr Xie Bo for their precious time and invaluable comments on this work.

Project supported by the National Natural Science Foundation of China (Grant No. 62075241).

References

[1] Duarte M F, Davenport M A, Takhar D, Laska J N, Sun T, Kelly K F and Baraniuk R G 2008 *IEEE Signal Process Mag.* **25** 83

[2] Ma J W 2009 *IEEE Geosci. Remote. Sens. Lett.* **6** 676
[3] Erkmen B I 2012 *J. Opt. Soc. Am. A* **29** 782
[4] Edgar M P, Gibson G M and Padgett M J 2019 *Nat. Photonics* **13** 13
[5] Sun M J and Zhang J M 2019 *Sensors* **19** 732
[6] Chen Y, Yin K, Shi D, Yang W, Huang J, Guo Zi, Yuan K and Wang Y 2022 *Appl. Opt.* **61** 6905
[7] Wang F, Wang C, Chen M, Gong W, Zhang Y, Han S and Situ G 2022 *Light Sci. Appl.* **11** 27
[8] Zhao C, Gong W, Chen M, Li E, Wang H, Xu W and Han S 2012 *Appl. Phys. Lett.* **101** 141123
[9] Chu C, Liu S, Liu Z, Hu C, Zhao Y and Han S 2021 *Appl. Opt* **60** 4632
[10] Li W, Tong Z, Xiao K, Liu Z, Gao Q, Sun J, Liu S, Han S and Wang Z 2019 *Optica* **6** 1515
[11] Yu H, Lu R, Han S, Xie H, Du G, Xiao T and Zhu D 2016 *Phys. Rev. Lett.* **117** 113901
[12] Zhang A X, He Y H, Wu L A, Chen L M and Wang B B 2018 *Optica* **5** 374
[13] Lin J, Yan Q, Lu S, Zheng Y, Sun S and Wei Z 2022 *Photonics* **9** 343
[14] Zhou N R, Zhang A D, Zheng F and Gong L H 2014 *Optics and Laser Technology* **62** 152
[15] Zhang Z B, Ma X and Zhong J G 2015 *Nat. Commun.* **6** 6225
[16] Huynh N, Zhang E, Betcke M, Arridge S, Beard P and Cox B 2016 *Optica* **3** 26
[17] Lyu M, Wang W, Wang H, Wang H, Li G, Chen N and Situ G 2017 *Sci. Rep.* **7** 17865
[18] Higham C F, Murray-Smith R, Padgett M J and Edgar M P 2018 *Sci. Rep.* **8** 2369
[19] Wang F, Wang H, Wang H, Li G and Situ G 2019 *Opt. Express* **27** 25560
[20] Wang F, Wang C, Deng C, Han S and Situ G 2022 *Photonics Res.* **10** 104
[21] Wang F, Wang C, Chen C, Gong W, Zhang Y, Han S and Situ G 2022 *Light: Sci. Appl.* **11** 1
[22] Situ G and Zhang J 2004 *Opt. Lett.* **29** 1584
[23] Liao M, Zheng S, Pan S, Lu D, He W, Situ G and Peng X 2021 *Opto-Electronic Advances* **4** 200016
[24] Zhang Y and Wang B 2008 *Opt. Lett.* **33** 2443
[25] Shan M, Liu L, Liu B and Zhong Z 2021 *Opt. Lasers Eng.* **145** 106662
[26] Zhang Y L, Lu Y X, Wang H X, Chen P and Liang R H 2021 *Optics & Laser Technology* **139** 106979
[27] Muniraj I, Guo C, Malallah R, Ryle J P, Healy J J, Lee B G and Sheridan J T 2017 *Opt. Lett.* **42** 2774
[28] Lai Q, Wan Z Q, Keng N, Leandre K, Kamdem K, Paul D and Chen C Y 2021 *IEEE Trans. Neural Netw Learn Syst.* **68** 1549
[29] Lai Q, Wan Z Q and Paul D 2023 *IEEE T. Circuits-I* **70** 1324
[30] Lai Q, Hu G W, Erkan U and Toktas A 2023 *Expert Syst. Appl.* **213** 118845
[31] Lai Q, Liang Y and Liu Y 2022 *Chaos Solitons Fractals* **165** 112781
[32] Clemente P, Durán V, Torres-Company V, Tajahuerce E and Lancis J 2010 *Opt. Lett.* **35** 2391
[33] Chen W and Chen X 2013 *Appl. Phys. Lett.* **103** 221106
[34] Qin Y and Zhang Y Y 2017 *IEEE Photon. J.* **9** 7802208
[35] Zhang L H, Pan Z L and Zhou G L 2017 *J. Opt.* **84** 471
[36] Zheng P, Ye Z, Xiong J and Liu H 2022 *Opt. Express* **30** 21866
[37] Zhang Z, Jiao S, Yao M, Li X and Zhong J 2018 *Opt. Express* **26** 14578
[38] Sun S L 2018 *IEEE Photon. J.* **10** 1
[39] Yi K, Leihong Z, Hualong Y, Mantong Z, Kanwal S and Dawei Z 2020 *Opt. Lasers Eng.* **134** 106154
[40] Qu G, Meng X, Yin Y, Wu H, Yang X, Peng X and He W 2020 *Opt. Lasers Eng.* **137** 106392
[41] Liu Y, Zheng P and Liu H C 2022 *Opt. Express* **30** 14073
[42] Jiao S, Feng J, Gao Y, Lei T and Yuan X 2020 *Opt. Express* **28** 7301
[43] Yuan S, Magayane D A, Liu X, Zhou X, Lu G, Wang Z, Zhang H and Li Z 2020 *Opt. Commun.* **482** 126568
[44] Liu H C and Chen W 2020 *Opt. Lasers Eng.* **130** 106094
[45] Ghanbari-Ghalehjoughi H, Eslami M, Ahmadi-Kandjani S, Ghanbari-Ghalehjoughi M and Yu Z 2020 *Opt. Lasers Eng.* **134** 106227
[46] Lin S, Wang X, Zhu A, Xue J and Xu B 2022 *Opt. Express* **30** 36144
[47] Zheng P X, Dai Q, Li Z L, Ye Z Y, Xiong J, Liu H C, Zheng G X and Zhang S 2021 *Sci. Adv.* **7** 1
[48] Arnol'd V I and Avez A 1968 *Ergodic Problems of Classical Mechanics* (New York: Benjamin)
[49] Chen G, Mao Y and Chui C K 2004 *Chaos Solitons Fractals* **21** 749
[50] Liu H, Zhu Z, Jiang H and Wang B 2008 *International Workshop on Chaos-Fractals Theories and Applications & the 9th International Conference for Young Computer Scientists, November*, 2008 Hunan, China
[51] Koblitz N 2010 *Math. Comput.* **48** 203
[52] Diffie W and Hellman M 2004 *IEEE Trans. Inf. Theory* **22** 644
[53] Zhang Z, Wang X, Zheng G and Zhong J 2017 *Opt. Express* **25** 19619
[54] Zhou W, Alan B, Hamid R S and Eero P S 2004 *IEEE Trans. Image Process.* **13** 600