Optical computing of zero-knowledge proof with single-pixel imaging

Wei Huang[a], Shuming Jiao[a,*], Huichang Guan[b], Huisi Miao[c], Chao Wang[a]

[a]School of Computing and Information Technology, Great Bay University, No. 16, University Road, Songshan Lake High-Tech Industrial Development Zone, Dongguan, 523000, Guangdong, China
[b]BYD Auto Industry, Co., Ltd., Shenzhen, 518100, Guangdong, China
[c]School of Automation and Electronic Information, Xiangtan University, Yanggutang Street, Yuhu District, Xiangtan, 411105, Hunan, China

Abstract

Optical computing has garnered significant attention in recent years due to its high-speed parallel processing and low power consumption capabilities. It has the potential to replace traditional electronic components and systems for various computation tasks. Among these applications, leveraging optical techniques to address information security issues has emerged as a critical research topic. However, current attempts are predominantly focused on areas such as image encryption and information hiding, with limited exploration of other modern information security concepts, including zero-knowledge proof (ZKP). In this paper, we propose an optical ZKP method based on single-pixel imaging (SPI). By utilizing the flexibility of SPI, our proposed approach can directly acquire randomly permuted results of the source problem's solution in the form of encoded images, thereby encrypting and verifying the original solution. ZKP for the source problem can be realized with optical computing based on a proving protocol without disclosing additional information. Simulated and experimental results show that our proposed method can be effectively applied to two typical ZKP problems: Sudoku and Hamiltonian cycle problem.

[*]Corresponding author

Email addresses: wei_huang@hnu.edu.cn (Wei Huang), jiaoshuming@gbu.edu.cn (Shuming Jiao), guanhuichang163@163.com (Huichang Guan), simonmiao@xtu.edu.cn (Huisi Miao), chaow@gbu.edu.cn (Chao Wang)

Keywords: optical computing, single-pixel imaging, zero-knowledge proof, Sudoku puzzle, Hamiltonian cycle problem

1. Introduction

Single-pixel imaging (SPI)[1] is a computational imaging scheme that utilizes a detector without spatial resolution to record one-dimensional light intensities of a target object under the projection of multiple illumination patterns. It can then reconstruct a two-dimensional image of the target object computationally based on the correlation relationship between acquired light signals and illumination patterns. Different from single-shot imaging based on conventional array sensors, SPI reconstructs the spatial information of the target object computationally by sacrificing imaging efficiency (multiple captures) but reducing reliance on the spatial resolution of the sensor pixels. It enables SPI to exhibit significantly lower sensor cost in the invisible wavebands, and provides superior operational flexibility under weak-light conditions[2]. With those advantages, SPI has been extensively applied in various fields such as terahertz imaging[3, 4], remote sensing[5], three-dimensional imaging[6, 7], microscopy[8, 9], scattering imaging[10, 11, 12], and X-ray imaging[13].

In recent years, with the advancement of optical materials and devices, both industry and academia have reignited their interest in optical computing[14]. By virtue of light's inherent advantages, including broader bandwidth, high-speed parallel processing, and low energy consumption, optical computing devices and systems are promising to circumvent the bottlenecks posed by Moore's law and Dennard's scaling law[15]. Optical computing approach provides novel solutions for a wide range of applications, including deep neural network[16, 17, 18, 19, 20], vector-matrix multiplication[21, 22], logic gate operation[23, 24], and image processing[25]. In addition to these applications, addressing information security challenges using optical methods is also a critical and promising research direction[26].

Optical image encryption and information hiding has been extensively investigated in previous works with various types of optical systems such as cascaded diffractive optical elements[27, 28], holography [29], integral imaging[30], ptychography[31], and scattering media[32]. Due to its indirect imaging property[33], SPI allows for a flexible control of the illumination regions and the projected pattern sequence during the imaging process. This feature is favorable for performing optical computing tasks related to information security, such as image encryption and image information hiding[34, 35, 36, 37, 38, 39, 40]. For instance, using the illumination patterns in the imaging process as a key and the acquired one-dimensional light signals as ciphertext enable the encryption and decryption of the target object image[34, 37]. Moreover, by optimizing the illumination patterns[38] or incorporating a decoding network model[39], the efficiency and security of SPI in image encryption and decryption can be further enhanced. In addition, integrating SPI with visual cryptography (VC) offers a novel approach to implement image hiding and encryption tasks. In [40], SPI is employed to capture multiple visual key images with only one single-pixel detector. The superposition results of visual key images can be reconstructed from the fused light intensity signals and the hidden information will be recovered.

However, the scope of modern information security research in the past decades has become much broader, beyond only image encryption and information hiding. Emerging information security concepts in recent years such as zero-knowledge proof (ZKP)[41] and homomorphic encryption[42, 43] have rarely been considered in previous optical information security works. ZKP, first proposed by Goldwasser et al. in 1985[44], is a cryptographic protocol that enables one party (prover) to prove the truth of a statement to another party (verifier) without revealing any additional information beyond the validity of the statement itself. Sudoku and Hamiltonian cycle problems are two classic problems in ZKP. For Sudoku, representative solving methods include interactive protocols based on commitment schemes[45, 46] and physical ZKP systems[47]. In those approaches, the prover demonstrates the validity of their solution through a series of randomized permutations and challenge steps, without revealing the specific solution itself. Similarly, the Hamiltonian cycle problems can be verified using a ZKP protocol based on graph isomorphism[48]. In this process, the prover confirms the existence of a path by generating an isomorphic graph in response to a random challenge posed by the verifier. In summary, the key step in achieving ZKP is the encryption of the original solution to the problem through random permutation and isomorphism. It should be noted that there also exist other ZKP problems, such as Sukoro [49]. However, Sukoro involves some nonlinear mathematical operations. For example, there are two basic game rules in Sukoro, i.e. neighborhood condition (a number in a cell indicates the number of filled cells vertically or horizontally adjacent to the cell) and connectivity condition (all filled cells are connected vertically or horizontally)Sukoro[49]. Since SPI has a linear mathematical model, it is not well-suited to handle such nonlinear problems. Therefore, we exclude Sukoro from this study. In future works, we plan to investigate alternative optical systems with greater computational capacity to address nonlinear ZKP problems. This paper mainly focuses on realizing ZKPs for problems similar to Sudoku and Hamiltonian cycle using SPI.

This paper explores the optical computing of ZKP using SPI. Initially, the solution to the problem is mapped to a two-dimensional encoded image, which serves as the target object in SPI. During the imaging preparation stage, random permutations are applied to the pixels of the illumination patterns. These permuted illumination patterns are then used to illuminate the object image entirely or partially in selected regions, allowing for the acquisition of a single-pixel light intensity sequence. The recorded data, together with the original illumination patterns, are utilized to reconstruct a result corresponding to a randomly permuted version of the original object image. The reconstruction result is capable of addressing the verifier's random challenge, thereby implementing the ZKP.

2. Principle

2.1. Principle of SPI

As shown in Fig. 1, a typical SPI system consists of a light source (projector or spatial light modulator), a single-pixel detector, and a target object image to be reconstructed. During the imaging process, it is assumed that a series of illumination patterns are emitted by the light source denoted as $\mathbf{P}_i\left(x,y\right)$, where $i = 1, 2, 3, \cdots, M$ represents the i-th measurement, M is the total number of measurements, and (x, y) denotes the image coordinates. The illumination pattern $\mathbf{P}_i\left(x,y\right)$ is projected onto the target object image $\mathbf{I}\left(x,y\right)$ and then captured by the single-pixel detector, yielding a single-pixel light signal S_i. The entire imaging process can be regarded as a liner system, represented by the following equation:

$$S_i = \iint \mathbf{P}_i\left(x,y\right) \cdot \mathbf{I}\left(x,y\right) dxdy \tag{1}$$

To reconstruct the target object image, random speckle patterns can be selected as the illumination patterns. The estimation of the target object image $\mathbf{I}^*(x, y)$ can then be obtained by leveraging the second-order correlation between illumination patterns and the corresponding light signals S_i[50], i.e.

$$\mathbf{I}^*(x,y) \approx \langle S_i \mathbf{P}_i(x,y)\rangle - \langle S_i\rangle \langle \mathbf{P}_i(x,y)\rangle \tag{2}$$

where $\langle\cdot\rangle = \frac{1}{N}\sum_i$ denotes an ensemble average for M measurements.

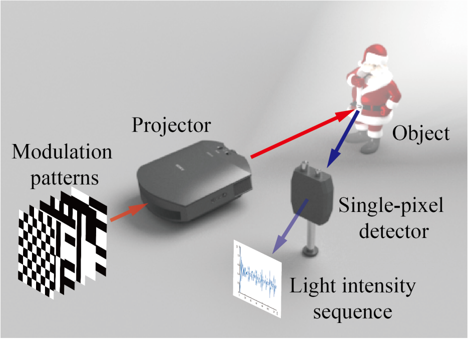


Fig. 1 Single-pixel imaging system.

However, since the random speckle patterns belong to an overcomplete non-orthogonal set[51], achieving a high-quality estimation of the target object image typically requires a large number of acquisitions, resulting in relatively low imaging efficiency. Using deterministic orthogonal basis patterns can significantly reduce the number of acquisitions and enhance imaging efficiency. Currently, commonly employed orthogonal basis patterns include Fourier basis [52], wavelet transform basis [53], cosine basis[54], and Hadamard basis[55]. Those approaches significantly reduce the number of illumination patterns needed for high-quality image reconstruction.

Among these, Hadamard basis patterns are binary orthogonal matrices composed of $+1$ and -1 values. They are characterized by rapid generation and more readily implementable on hardware devices such as spatial light modulators. SPI based on Hadamard basis patterns is commonly referred to as Hadamard SPI (HSPI). This method reconstructs the target object image by applying an inverse Hadamard transform to the Hadamard spectrum of the target object. The Hadamard spectrum is composed of Hadamard coefficients corresponding to the light signals obtained by the single-pixel detector when Hadamard basis patterns are projected onto the target object. The sequence of Hadamard basis patterns can be arranged in various orders[56].

The two-dimensional Hadamard transform in the original form is given by

$$\mathbf{I}_H\left(u,v\right) = H\left\{\mathbf{I}\left(x,y\right)\right\} = \sum_{x=0}^{N-1}\sum_{y=0}^{N-1}\mathbf{I}\left(x,y\right)\left(-1\right)^{p(x,y,u,v)} \tag{3}$$

where $H\left\{\cdot\right\}$ denotes Hadamard transform and N represents the horizontal and vertical resolution of the pattern, satisfying $N = 2^n$, where n is a positive integer. (u, v) denotes the coordinates in the Hadamard domain.

$$p\left(x,y,u,v\right) = \sum_{i=0}^{n-1}\left(u_i x_i + v_i y_i\right) \tag{4}$$

where u_i, v_i, x_i and y_i represent the i-th bits of the binary forms of u, v, x and y, respectively. For example,

$$(u)_{decimal} = (u_{n-1}u_{n-2}\cdots u_1 u_0)_{binary} \tag{5}$$

where $u_i \in \{0, 1\}$. Hadamard basis patterns can be obtained by applying an inverse Hadamard transform to the impulse function $\delta_H\left(u,v\right)$

$$\mathbf{P}_H\left(x,y\right) = \frac{1}{2}\left[1 + H^{-1}\left\{\delta_H\left(u,v\right)\right\}\right] \tag{6}$$

where $H^{-1}\left\{\cdot\right\}$ denotes inverse Hadamard transform.

$$\delta_H\left(u,v\right) = \begin{cases} 1, & u = u_0, v = v_0 \\ 0, & \text{otherwise} \end{cases} \tag{7}$$

In practical applications, to enhance the signal-to-noise ratio of the reconstructed image, differential HSPI can be used to suppress noise. This method needs to project two Hadamard basis patterns, $\mathbf{P}_H$ and its complementary pattern $[1 - \mathbf{P}_H]$, to derive the $H(u, v)$ from the difference between the intensity measurements obtained from these two projections, that is,

$$H\left(u,v\right) = D_{+1} - D_{-1} \tag{8}$$

where D_{+1} and D_{-1} represent the light signals acquired from projecting the patterns $\mathbf{P}_H$ and $[1 - \mathbf{P}_H]$, respectively. After all Hadamard coefficients have been obtained, the target object image can be reconstructed by applying an inverse Hadamard transform to those coefficients. Additionally, the number of Hadamard coefficients matches the number of pixels in the reconstructed target image if the sampling ratio is 100%. Therefore, reconstructing an image with $N \times N$ pixels requires $2N^2$ acquisitions at a full sampling rate.

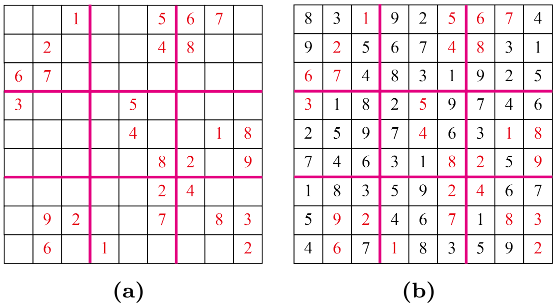
Furthermore, as indicated by Eq. 1, in the reconstruction process of differential HSPI, there is a one-to-one correspondence between the pixels of the target object image and the pixels of the illumination patterns. If the pixel order of the illumination patterns is randomly shuffled to generate new illumination patterns, and they are projected onto the target object image, the acquired sequence of light signals will correspondingly reflect this change. When reconstructing the target object image using this changed sequence of light signals with the original illumination patterns, the pixel order of the resulting target object image will also be shuffled. This feature paves a way for implementing image encryption based on SPI[37] and it is also favorable for enabling ZKP.

2.2. ZKP method based on SPI

In the two canonical ZKP problems, i.e. Sudoku and Hamiltonian cycle problem, random permutations can be used to generate its permuted solution or isomorphic version of the original graph. This allows one to demonstrate knowledge of a solution for such a problem without revealing the original answer, thereby achieving the objective of ZKP. The random permutation of the original problem's solution in ZKP shares a high degree of similarity with the random permutation of pixel orders in illumination patterns of SPI. Specifically, by treating the original problem's solution equivalently as the target object image in a SPI system, randomly shuffling the pixels of the projected illumination patterns yields a correspondingly shuffled reconstruction of the target object image. This process effectively achieves a random permutation of the original solution. Below, we will provide a detailed description of working principles when this method is applied to Sudoku and Hamiltonian cycle problem.

2.2.1. ZKP of Sudoku puzzle based on differential HSPI

Sudoku is one of the most renowned puzzles. As illustrated in Fig. 2(a), a standard Sudoku puzzle consists of a 9×9 grid and it is further divided into 3×3 subgrids. Some cells are prefilled with numbers ranging from 1 to 9. The objective of the puzzle is to fill in the remaining cells with numbers



		1			5	6	7	
	2				4	8		
6	7							
3				5				
				4			1	8
					8	2		9
					2	4		
	9	2			7		8	3
	6		1					2

(a)

8	3	1	9	2	5	6	7	4
9	2	5	6	7	4	8	3	1
6	7	4	8	3	1	9	2	5
3	1	8	2	5	9	7	4	6
2	5	9	7	4	6	3	1	8
7	4	6	3	1	8	2	5	9
1	8	3	5	9	2	4	6	7
5	9	2	4	6	7	1	8	3
4	6	7	1	8	3	5	9	2

(b)

Fig. 2 Example of a standard Sudoku puzzle and its solution: (a) Sudoku puzzle. (b) solution of (a).

from 1 to 9, ensuring that each number appears exactly only once in each row, column, and subgrid (as shown in Fig. 2(b)).

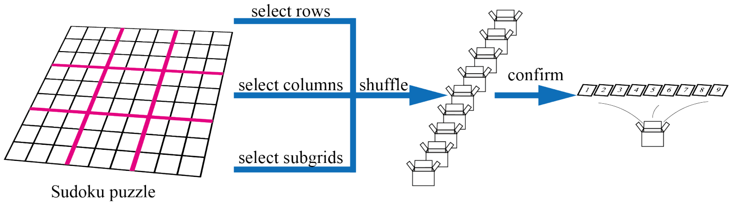


Fig. 3 One ZKP method of Sudoku puzzle.

ZKP of Sudoku puzzles has been extensively studied[47, 46, 45]. Among them, the GNPR Protocol 3 proposed by Gradwohl et al.[47] has garnered significant attention. As shown in Fig. 3, for a publicly known Sudoku puzzle (known to both the prover and the verifier), the prover aims to prove he/she knows the solution but keeps the solution concealed. The prover can employ the proposed protocol to convince the verifier by randomly selecting rows, columns, or subgrids for verification. For instance, if rows are selected, the prover needs to shuffle the data in each row of the Sudoku solution and submit it to the verifier. If the shuffled data in each row contains all numbers from 1 to 9, the verifier can confirm that the prover possesses a valid solution to the Sudoku puzzle.

This paper integrates SPI with GNPR Protocol 3, attempting to address the ZKP problem of Sudoku through optical computing. As illustrated in Fig. 4(a), for a Sudoku solution, the numbers 1 to 9 are first encoded using a 4-bit binary representation. Each number is represented by four subcells, filled in with the corresponding four binary bits sequentially in the order

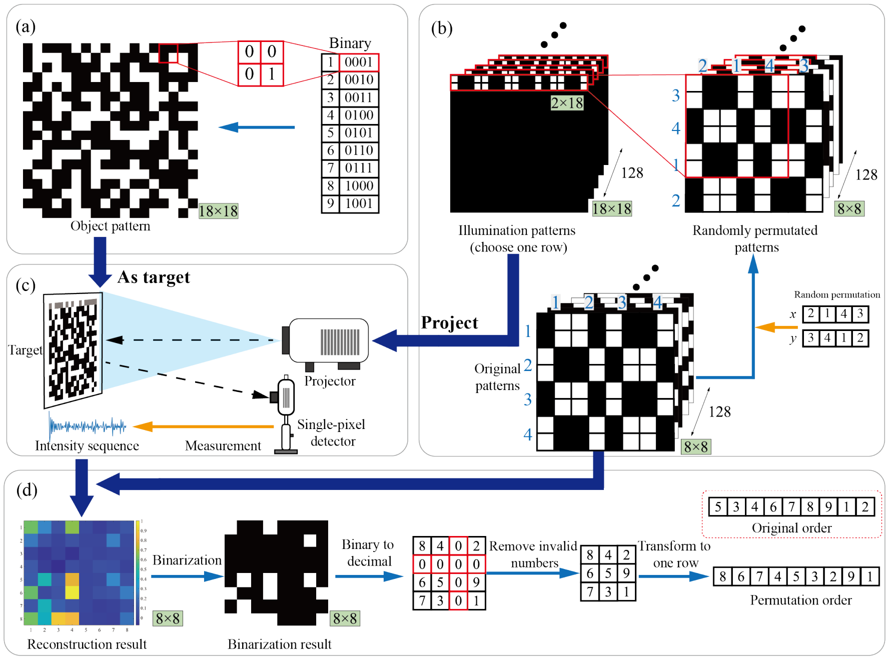


Fig. 4 Proposed ZKP of Sudoku based on differential HSPI: (a) Encoding of Sudoku solution. (b) Permutation of original Illumination patterns. (c) Data acquisition in differential HSPI. (d) Image reconstruction in Differential HSPI and number mapping.

of top-left, top-right, bottom-left and bottom-right, resulting in a matrix composed of binary numbers. To meet the requirements of optical computing in SPI, the binary matrix is converted into a binary image with pixel values of 0 (black) and 255 (white), which serves as the target object in the SPI.

During the verification process, according to GNPR Protocol 3, rows, columns, or subgrids of Sudoku solution need to be selected for verification. Taking a 9×9 Sudoku puzzle as an example, all three selection methods require extracting the cells corresponding to 9 numbers during a single verification. Since the resolution of the illumination pattern matches that of the target object image in differential HSPI, and considering that each number is represented by a 4-bit binary code, the resolution of the illumination pattern should vary depending on the selection method: 2×18 pixels (selecting row), 18×2 pixels (selecting column), and 6×6 pixels (selecting subgrid).

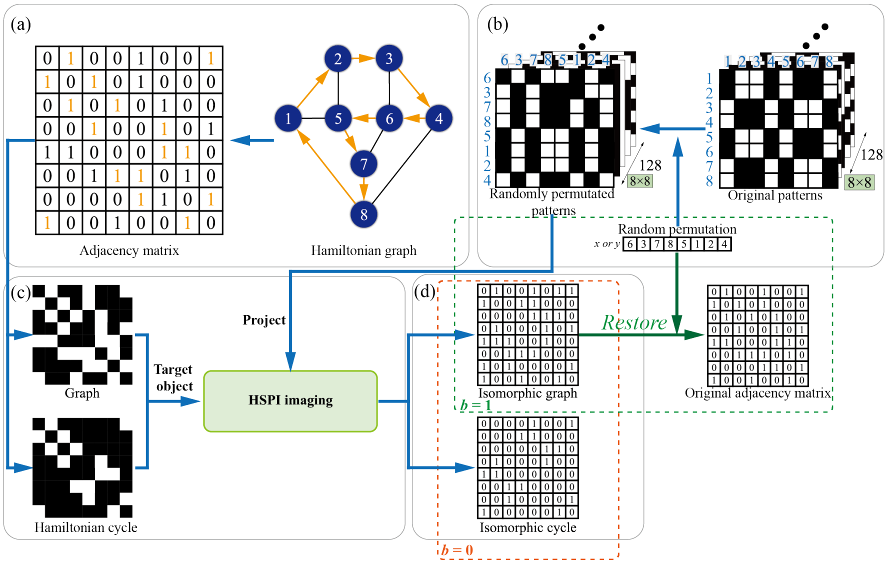
Additionally, the prover needs to permute the pixel order of the illumination patterns in HSPI before projection, such that the reconstructed result directly yields the permuted solution of the Sudoku puzzle. As shown in

Fig. 4(b), firstly, an 8 × 8 matrix is generated. Nextly, treating four cells as one unit, and both rows and columns are randomly permuted using the MATLAB function `randperm()`. The generated results can pass various statistical tests of randomness, satisfying the independent and identically distributed condition. Finally, a 6 × 6 region is selected and converted into images with resolutions of 2 × 18 pixels (selecting row), 18 × 2 pixels (selecting column), or 6 × 6 pixels (selecting subgrid) based on the chosen method. As shown in Fig. 4(c), during the imaging process, the generated permuted illumination patterns are sequentially projected onto the target object image to acquire the corresponding one-dimensional light signals. As shown in Fig. 4(d), during reconstruction, the target object image is reconstructed using the original illumination patterns and the one-dimensional light signals are acquired. The reconstructed encoded image is then binarized, converted back to decimal numbers, and mapped into rows, columns, or subgrids according to the selected method. The order of the reconstructed results obtained using the above method will vary according to the permutation order of the illumination patterns. If each number in the reconstructed sequence appears only once for every reconstruction, it can be verified that the target object image corresponds to a correct Sudoku solution, thereby completing the ZKP. Notably, the entire HSPI process, including the permuted illumination patterns, is kept secret from the verifier. But the imaging results can be accessed by the verifier.

2.2.2. Zero knowledge proof of Hamiltonian cycle based on HSPI

The concept of Hamiltonian graphs is derived from the "icosian game" introduced by William Rowan Hamilton in 1856[57]. A graph G is defined as a Hamiltonian graph if there exists a cycle that visits each vertex of G exactly once. This cycle is referred to as a Hamiltonian cycle. The problem of finding a Hamiltonian cycle in a given graph is known as the Hamiltonian cycle problem.

A ZKP for the Hamiltonian cycle problem can be implemented using graph isomorphism[58]. Suppose there exists a graph G with n nodes containing a Hamiltonian cycle H, where $H \subseteq G$. Both the prover and the verifier know graph G, but only the prover knows Hamiltonian cycle H. If the prover wants to prove knowledge of H to the verifier without revealing H directly, the prover can generate an isomorphic graph G' of the G by applying a random permutation π, and obtain Hamiltonian cycle H' of G'. Subsequently, the prover encrypts G' and sends it to the verifier. The verifier issues a random challenge b, where $b \in \{0, 1\}$. If $b = 0$, the prover reveals the graph G' and its Hamiltonian cycle H', and the verifier checks whether H' is a valid Hamiltonian cycle of G'. If $b = 1$, the prover decrypts the isomorphic graph G' and reveals the random permutation π, allowing the verifier to confirm whether G' is the result of applying π to the original graph G. It is important to note that the prover can forge a response to one of the challenges without knowing H, but cannot simultaneously satisfy both challenges. Thus, the prover has a 50% probability of deceiving the verifier. To enhance the reliability of the ZKP, the above protocol must be repeated over multiple rounds to reduce the likelihood of successful deception.



Adjacency matrix

0	1	0	0	1	0	0	1
1	0	1	0	1	0	0	0
0	1	0	1	0	1	0	0
0	0	1	0	0	1	0	1
1	1	0	0	0	1	1	0
0	0	1	1	1	0	1	0
0	0	0	0	1	1	0	1
1	0	0	1	0	0	1	0

Random permutation

6	3	7	8	5	1	2	4

Isomorphic graph

0	1	0	0	1	0	1	1
1	0	0	1	1	0	0	0
0	0	0	0	1	1	1	0
0	1	0	0	0	1	0	1
1	1	1	0	0	1	0	0
0	0	1	1	1	0	0	0
1	0	1	0	0	0	0	1
1	0	0	1	0	0	1	0

Original adjacency matrix

0	1	0	0	1	0	0	1
1	0	1	0	1	0	0	0
0	1	0	1	0	1	0	0
0	0	1	0	0	1	0	1
1	1	0	0	0	1	1	0
0	0	1	1	1	0	1	0
0	0	0	0	1	1	0	1
1	0	0	1	0	0	1	0

Isomorphic cycle

0	0	0	0	1	0	0	1
0	0	0	1	1	0	0	0
0	0	0	0	0	1	1	0
0	1	0	0	0	1	0	0
1	1	0	0	0	0	0	0
0	0	1	1	0	0	0	0
0	0	1	0	0	0	0	1
1	0	0	0	0	0	1	0

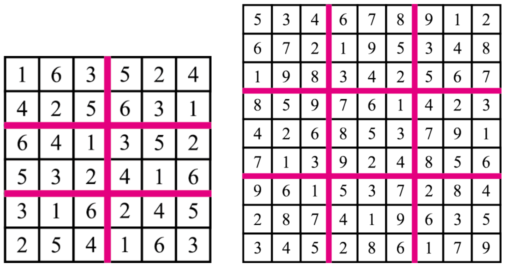
Fig. 5 ZKP of Hamiltonian cycle based on differential HSPI: (a) Adjacency matrix of Hamiltonian graph. (b) Permutation of illumination patterns. (c) Image reconstruction in differential HSPI. (d) Reconstruction of Isomorphic graph and Hamiltonian cycle.

SPI can achieve random permutations of the graph G through an optical process, thereby obtaining an isomorphic Hamiltonian graph and its corresponding Hamiltonian cycle to assist in completing the ZKP of the Hamiltonian cycle problem. As shown in Fig. 5(a), the graph is converted into an $n \times n$ adjacency matrix. In this matrix, the entry corresponding to two nodes is set to be 1 if there is an edge between them, and 0 otherwise. The orange numbers indicate that the corresponding edge belongs to a Hamiltonian cycle. The process of generating an isomorphic graph G' through a random permutation of the graph G can be equivalently considered, in differential HSPI, as the random permutation of rows and columns in the illumination patterns. As shown in Fig. 5(b), unlike the case in Sudoku where rows and columns are randomly permuted independently, the permutations of rows and columns must be identical to preserve graph isomorphism, and the permutation function used is `randperm()`, the same as that used in Sudoku. The adjacency matrix is used as the target object image for HSPI, which is known to both the prover and the verifier. And using permuted illumination patterns to obtain the one-dimensional light signals as shown in Fig. 5(c). Then the isomorphic subgraph G' of the graph G and its corresponding Hamiltonian cycle H' can be reconstructed with the original illumination patterns (as shown in Fig. 5(d). It should be noted that, in the above process, both the permuted illumination patterns and the original illumination patterns remain unknown to the verifier. Finally, according to the verifier's random challenge, the prover selectively revealed the permutation order or the permuted Hamiltonian cycle, but not both.

3. Results and Discussions

In this section, numerical simulations and optical experiments are conducted to verify the optical computing of ZKP with differential HSPI for Sudoku and Hamiltonian cycle problem, respectively.

3.1. Numerical simulation



1	6	3	5	2	4
4	2	5	6	3	1
6	4	1	3	5	2
5	3	2	4	1	6
3	1	6	2	4	5
2	5	4	1	6	3

(a)

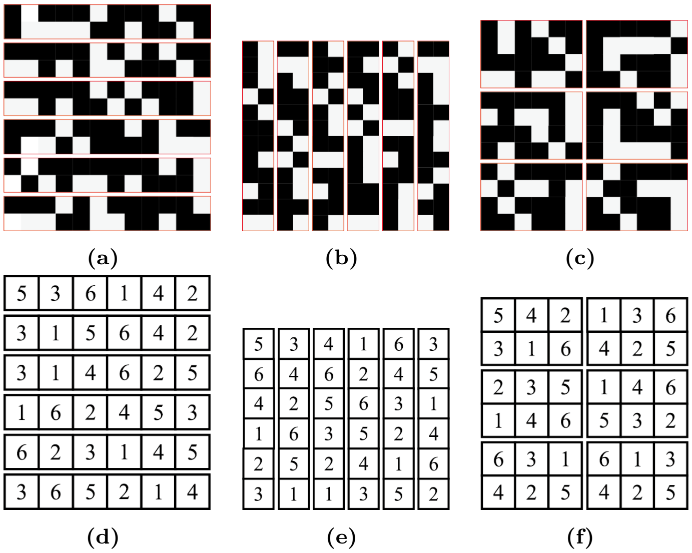
5	3	4	6	7	8	9	1	2
6	7	2	1	9	5	3	4	8
1	9	8	3	4	2	5	6	7
8	5	9	7	6	1	4	2	3
4	2	6	8	5	3	7	9	1
7	1	3	9	2	4	8	5	6
9	6	1	5	3	7	2	8	4
2	8	7	4	1	9	6	3	5
3	4	5	2	8	6	1	7	9

(b)

Fig. 6 Sudoku puzzle instances: (a) 6 × 6 Sudoku. (b) 9 × 9 Sudoku.

In the numerical simulation, Sudoku and Hamiltonian cycle problem are converted into two-dimensional numerical matrices, which serve as virtual target object images. Subsequently, standard Hadamard pattern sequences are generated based on a zig-zag path[51] and then randomly permuted. The process of acquiring one-dimensional light signals in a differential HSPI system is simulated by calculating the inner product between the virtual target object image and the permuted Hadamard patterns.

In sudoku puzzle numerical simulation, as illustrated in Fig. 6, we selected two Sudoku puzzles with sizes 6×6 and 9×9 respectively. Unlike the standard 9 × 9 Sudoku puzzle, the 6 × 6 Sudoku puzzle requires that numbers within each 2 × 3 subgrid contain exactly one, two, , and six. During the ZKP process for Sudoku based on GNPR Protocol 3, rows, columns, or subgrids need to be selected for verification. To evaluate the robustness of the ZKP based on differential HSPI, we conducted imaging verification for all the three selection modes.



5	3	6	1	4	2
3	1	5	6	4	2
3	1	4	6	2	5
1	6	2	4	5	3
6	2	3	1	4	5
3	6	5	2	1	4

(d)

5	3	4	1	6	3
6	4	6	2	4	5
4	2	5	6	3	1
1	6	3	5	2	4
2	5	2	4	1	6
3	1	1	3	5	2

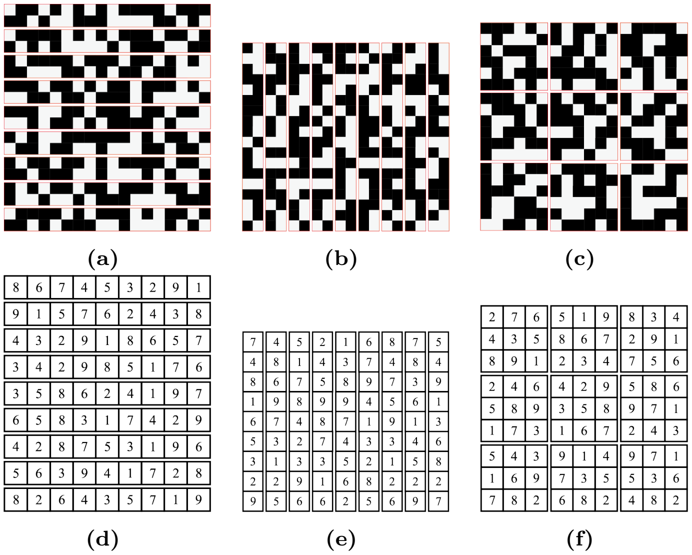
(e)

5	4	2	1	3	6
3	1	6	4	2	5
2	3	5	1	4	6
1	4	6	5	3	2
6	3	1	6	1	3
4	2	5	4	2	5

(f)

Fig. 7 Numerical simulation results of ZKP for the 6 × 6 Sudoku puzzle based on differential HSPI: (a)-(c) Differential HSPI reconstruction results for selecting row, column,and subgrid, respectively. (d)-(f) Corresponding results converted into decimal numbers for row, column, and subgrid.

As previously discussed, to enhance imaging stability, each number is represented using a 4-bit binary encoding. Consequently, the actual resolutions of the two Sudoku instances increase to 12 × 12 pixels (for the original 6 × 6 Sudoku) and 18 × 18 pixels (for the original 9 × 9 Sudoku). Additionally, since the dimensions of Hadamard patterns must be powers of 2, the total pixel count for Hadamard patterns used in imaging single rows, columns, or subgrids of these Sudoku is set to 64 pixels (corresponding to an 8 × 8 Hadamard matrix). Therefore, based on the principle of differential HSPI, the number of illumination patterns required to verify single row, column, or subgrid for these two Sudoku instances is 128.



8	6	7	4	5	3	2	9	1
9	1	5	7	6	2	4	3	8
4	3	2	9	1	8	6	5	7
3	4	2	9	8	5	1	7	6
3	5	8	6	2	4	1	9	7
6	5	8	3	1	7	4	2	9
4	2	8	7	5	3	1	9	6
5	6	3	9	4	1	7	2	8
8	2	6	4	3	5	7	1	9

(d)

7	4	5	2	1	6	8	7	5
4	8	1	4	3	7	4	8	4
8	6	7	5	8	9	7	3	9
1	9	8	9	9	4	5	6	1
6	7	4	8	7	1	9	1	3
5	3	2	7	4	3	3	4	6
3	1	3	3	5	2	1	5	8
2	2	9	1	6	8	2	2	2
9	5	6	6	2	5	6	9	7

(e)

2	7	6	5	1	9	8	3	4
4	3	5	8	6	7	2	9	1
8	9	1	2	3	4	7	5	6
2	4	6	4	2	9	5	8	6
5	8	9	3	5	8	9	7	1
1	7	3	1	6	7	2	4	3
5	4	3	9	1	4	9	7	1
1	6	9	7	3	5	5	3	6
7	8	2	6	8	2	4	8	2

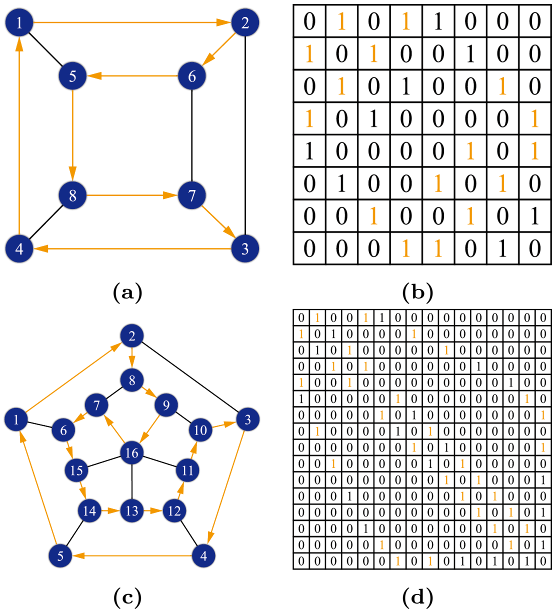
(f)

Fig. 8 Number simulation results of ZKP for the 9 × 9 Sudoku puzzle based on differential HSPI: (a)-(c) Differential HSPI reconstruction results for select rows, columns, and subgrids, respectively. (d)-(f) Corresponding results converted into decimal numbers for rows, columns, and subgrids.

Fig. 7 and 8 present the simulation results for selecting row, column, and subgrid on 6 × 6 and 9 × 9 Sudoku puzzles, respectively. Among them, Fig. 7(a) and 8(a) show the direct imaging results when verifying rows, while Fig. 7(d) and 8(d) display the results converted into decimal numbers. As shown in the figures, the random permutation of illumination patterns leads to corresponding permutations in the reconstructed number sequences, yet each number still appears only once in each row, satisfying the Sudoku constraints. Additionally, because the permutation order of illumination pattern images differs during the imaging of each row, the solutions to any column or any subgrid will be encrypted and not revealed. The same mechanism applies to the analysis of column and subgrid modes, which is skipped for brevity here.

As illustrated in Fig. 9, in the numerical simulation of ZKP for Hamiltonian cycle problems, we constructed two Hamiltonian graphs containing

8 nodes (Fig. 9(a)) and 16 nodes (Fig. 9(c)), with their corresponding adjacency matrices displayed in Fig. 9(b) and 9(d), respectively. Based on the graph isomorphism method, it is required to generate isomorphic graphs of the original Hamiltonian graphs along with their corresponding Hamiltonian cycles to achieve ZKP. According to the principle of differential HSPI, Hadamard pattern sequences with 8 × 8 pixels and 16 × 16 pixels were utilized for imaging the two Hamiltonian graphs, respectively. As described above, this process required 128 and 256 acquisition operations, respectively. Similar to Sudoku, random permutations of the Hadamard patterns can be used to obtain isomorphic subgraphs of the Hamiltonian graphs.



0	1	0	1	1	0	0	0
1	0	1	0	0	1	0	0
0	1	0	1	0	0	1	0
1	0	1	0	0	0	0	1
1	0	0	0	0	1	0	1
0	1	0	0	1	0	1	0
0	0	1	0	0	1	0	1
0	0	0	1	1	0	1	0

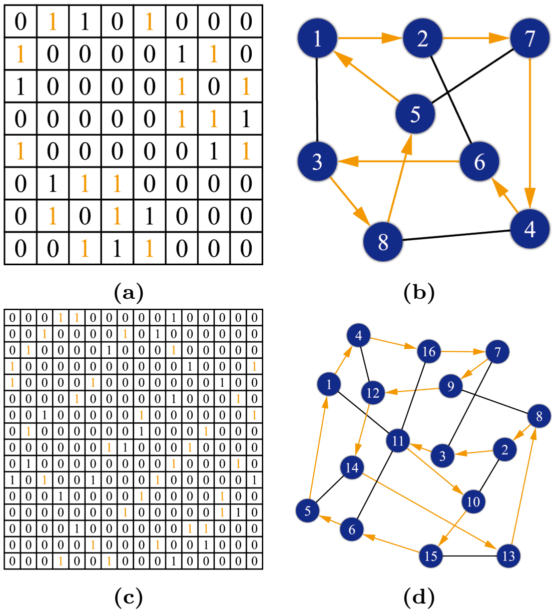
(a) **(b)**

0	1	0	0	1	1	0	0	0	0	0	0	0	0	0	0
1	0	1	0	0	0	0	1	0	0	0	0	0	0	0	0
0	1	0	1	0	0	0	0	0	1	0	0	0	0	0	0
0	0	1	0	1	0	0	0	0	0	0	1	0	0	0	0
1	0	0	1	0	0	0	0	0	0	0	0	0	1	0	0
1	0	0	0	0	0	1	0	0	0	0	0	0	0	1	0
0	0	0	0	0	1	0	1	0	0	0	0	0	0	0	1
0	1	0	0	0	0	1	0	1	0	0	0	0	0	0	0
0	0	0	0	0	0	0	1	0	1	0	0	0	0	0	1
0	0	1	0	0	0	0	0	1	0	1	0	0	0	0	0
0	0	0	0	0	0	0	0	0	1	0	1	0	0	0	1
0	0	0	1	0	0	0	0	0	0	1	0	1	0	0	0
0	0	0	0	0	0	0	0	0	0	0	1	0	1	0	1
0	0	0	0	1	0	0	0	0	0	0	0	1	0	1	0
0	0	0	0	0	1	0	0	0	0	0	0	0	1	0	1
0	0	0	0	0	0	1	0	1	0	1	0	1	0	1	0

(c) **(d)**

Fig. 9 Hamiltonian graph examples: (a) Hamilton graph with 8 nodes. (b) Corresponding adjacency matrix of (a). (c) Hamilton graph with 16 nodes. (d) Corresponding adjacency matrix of (c).

As shown in Fig. 10(a) and 10(c), these are the isomorphic adjacency matrices corresponding to Fig. 9(b) and 9(d), obtained using differential HSPI. Fig. 10(b) and 10(d) represent the Hamiltonian graphs generated from Fig. 10(a) and 10(c). A comparison between Fig. 9(b) and Fig. 10(a), as well as Fig. 9(d) and Fig. 10(c), reveals that the Hamiltonian graphs acquired through differential HSPI are isomorphic to the original Hamiltonian graphs. In accordance with the ZKP process for Hamiltonian cycle problems, the verifier randomly selects one of two verification methods and the prover will show the corresponding outcome: 1) reconstructing both the permuted Hamiltonian graph and the permuted Hamiltonian cycle from the one-dimensional light signals acquired during the imaging process with the original illumination patterns and show they are matched, while disclosing the permutation order of the Hamiltonian graph to the verifier; or 2) reconstructing only the permuted graph from the one-dimensional light signals acquired during the imaging process with the original illumination patterns, convert the permuted one to the original one based on the permutation order and show it is the correct original graph. Through this approach, the prover can fake neither the Hamiltonian graph nor the Hamiltonian cycle. Therefore, ZKP for Hamiltonian cycle problems can be achieved.



0	1	1	0	1	0	0	0
1	0	0	0	0	1	1	0
1	0	0	0	0	1	0	1
0	0	0	0	0	1	1	1
1	0	0	0	0	0	1	1
0	1	1	1	0	0	0	0
0	1	0	1	1	0	0	0
0	0	1	1	1	0	0	0

(a)

(b)

0	0	0	1	1	0	0	0	0	0	1	0	0	0	0	0
0	0	1	0	0	0	0	1	0	1	0	0	0	0	0	0
0	1	0	0	0	0	1	0	0	0	1	0	0	0	0	0
1	0	0	0	0	0	0	0	0	0	0	1	0	0	0	1
1	0	0	0	0	1	0	0	0	0	0	0	0	1	0	0
0	0	0	0	1	0	0	0	0	0	1	0	0	0	1	0
0	0	1	0	0	0	0	0	1	0	0	0	0	0	0	1
0	1	0	0	0	0	0	0	1	0	0	0	1	0	0	0
0	0	0	0	0	0	1	1	0	0	0	1	0	0	0	0
0	1	0	0	0	0	0	0	0	0	1	0	0	0	1	0
1	0	1	0	0	1	0	0	0	1	0	0	0	0	0	1
0	0	0	1	0	0	0	0	1	0	0	0	0	1	0	0
0	0	0	0	0	0	0	1	0	0	0	0	0	1	1	0
0	0	0	0	1	0	0	0	0	0	0	1	1	0	0	0
0	0	0	0	0	1	0	0	0	1	0	0	1	0	0	0
0	0	0	1	0	0	1	0	0	0	1	0	0	0	0	0

(c)

(d)

Fig. 10 Numerical simulation results of ZKP for Hamiltonian graphs with 8 nodes and 16 nodes based on differential HSPI: (a) Imaging result of adjacency matrix for isomorphic Hamilton graph with 8 nodes. (b) Corresponding graph of (a). (c) Imaging result of adjacency matrix for isomorphic Hamilton graph with 16 nodes. (d) Corresponding graph of (c).

3.2. Optical experiment

The experimental differential HSPI setup is shown in Fig. 11. The system employs a projector with a resolution of 1280 × 720 pixels (Philips NeoPix

Prime 2) and uses a Thorlabs 100A2 PDA (photo-diode array) as the single-pixel sensor. The data acquired by the sensor are collected using an NI-USB-6216 data acquisition card (DAQ). The original problem in the ZKP is converted into an image composed of black and white squares (where black represents 0 and white represents 1), which is then printed using a A4 paper to serve as the target object image. All the experiments are conducted in a darkroom environment to avoid interference from ambient light.

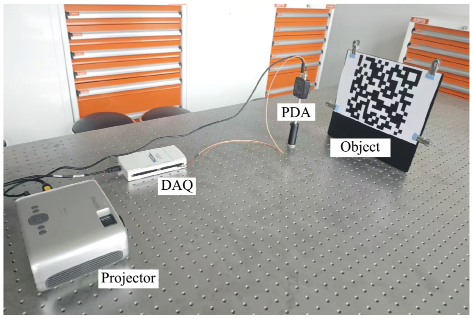


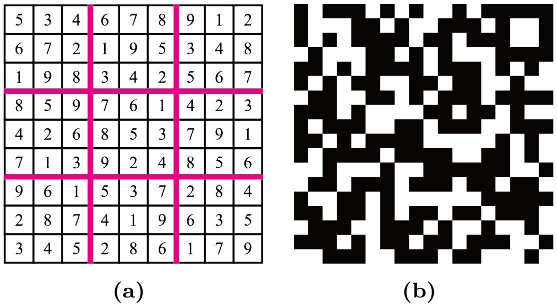
Fig. 11 Experimental differential HSPI setup in this work.

In the ZKP of a 9×9 Sudoku puzzle shown in Fig. 12(a), its corresponding two-dimensional encoded image is shown in Fig. 12(b). After image reconstruction by differential HSPI, the results are presented in Fig. 13(a), 13(d) and 13(g) show the direct imaging results for each row, column, and subgrid, respectively. Due to environmental noise during the imaging process and variations in the reflectance of the target object, the acquired images are not ideal binary images and require further processing. In this work, binarization is performed by treating the four binary bits corresponding to each number as a unit (denoted as B). The formula for calculating the binarization values is as follows:

$$V\left(i,j\right)=\begin{cases}1, & B\left(i,j\right)\geq \max\left(B\right)/2\\ 0, & B\left(i,j\right)<\max\left(B\right)/2\end{cases} \tag{9}$$

where (i,j) represents the relative coordinates of the four binary bits within a unit $(i,j=0,1,2,3)$, and $\max\left(\cdot\right)$ denotes the function for calculating the maximum value.

Using the aforementioned formula, the acquired imaging results can be further converted into binary matrices, as shown in Fig. 13(b), 13(e) and 13(h). These results can then be transformed to decimal numbers, as illustrated in Fig. 13(c), 13(f) and 13(i). The experimental results for the



5	3	4	6	7	8	9	1	2
6	7	2	1	9	5	3	4	8
1	9	8	3	4	2	5	6	7
8	5	9	7	6	1	4	2	3
4	2	6	8	5	3	7	9	1
7	1	3	9	2	4	8	5	6
9	6	1	5	3	7	2	8	4
2	8	7	4	1	9	6	3	5
3	4	5	2	8	6	1	7	9

Fig. 12 Sudoku puzzle example used in the optical experiment: (a) Sudoku puzzle example. (b) Corresponding encoded image representation.

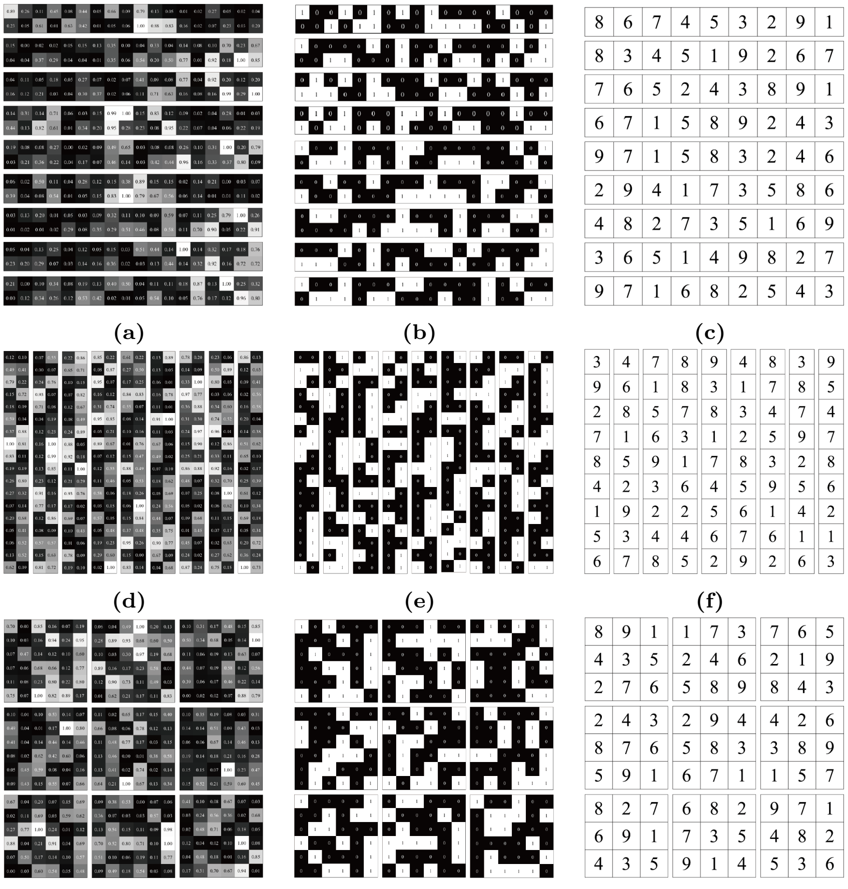
ZKP of the Sudoku puzzle align with the simulation outcomes. The uniqueness of numbers in rows, columns, or subgrids can all be verified while the original solution remains unrevealed.

In the ZKP experiment for Hamiltonian cycle problems, we selected an 8-node Hamiltonian graph, as shown in Fig. 14(a) (with the orange line representing the Hamiltonian cycle), and converted it into two target object images composed of black-and-white square dots. Specifically, Fig. 14(b) represents the image generated from the original Hamiltonian graph, while Fig. 14(c) represents the image generated from the Hamiltonian cycle.

The results of differential HSPI reconstruction are shown in Fig. 15(a) and 15(d) represent the direct imaging results of the Hamiltonian graph and its Hamiltonian cycle, respectively. Fig. 15(b) and 15(e) show the corresponding binarization results, and Fig. 15(c) and 15(f) display the reconstructed permuted Hamiltonian graph and corresponding Hamiltonian cycle, respectively. As it can be seen from the figures, using our method, both the isomorphic Hamiltonian graph(Fig. 15(c) compared to Fig. 14(a)) and the corresponding Hamiltonian cycle can be obtained, enabling the ZKP for this Hamiltonian graph problem.

4. Conclusion

In this study, we propose a novel method for achieving optical computing of ZKP based on SPI. The major steps can be summarized as follows. First, one solution of the problem to be verified is mapped to a two-dimensional encoded image and it is input to a SPI system as a target object image. Then, the object image is captured using illumination patterns with random pixel


(a)
(b)
(c)

8	6	7	4	5	3	2	9	1
8	3	4	5	1	9	2	6	7
7	6	5	2	4	3	8	9	1
6	7	1	5	8	9	2	4	3
9	7	1	5	8	3	2	4	6
2	9	4	1	7	3	5	8	6
4	8	2	7	3	5	1	6	9
3	6	5	1	4	9	8	2	7
9	7	1	6	8	2	5	4	3

(d)
(e)
(f)

3	4	7	8	9	4	8	3	9
9	6	1	8	3	1	7	8	5
2	8	5	7	8	3	4	7	4
7	1	6	3	1	2	5	9	7
8	5	9	1	7	8	3	2	8
4	2	3	6	4	5	9	5	6
1	9	2	2	5	6	1	4	2
5	3	4	4	6	7	6	1	1
6	7	8	5	2	9	2	6	3

(g)
(h)
(i)

8	9	1	1	7	3	7	6	5
4	3	5	2	4	6	2	1	9
2	7	6	5	8	9	8	4	3
2	4	3	2	9	4	4	2	6
8	7	6	5	8	3	3	8	9
5	9	1	6	7	1	1	5	7
8	2	7	6	8	2	9	7	1
6	9	1	7	3	5	4	8	2
4	3	5	9	1	4	5	3	6

Fig. 13 Optical experimental results of ZKP for a 9Œ9 Sudoku puzzle based on differential HSPI in row mode: (a) Direct imaging results. (b) Corresponding binarization results of (a). (c) Reconstructed decimal results in column mode. (d) Direct imaging results. (e) Corresponding binarization results of (d). (f) Reconstructed decimal results in subgrid mode. (g) Direct imaging results. (h) Corresponding binarization results of (g). (i) Reconstructed decimal results in subgrid mode.

permutation, equivalently obtaining a randomly permuted reconstruction result of the solution to be verified. Based on this permuted result, the ZKP for the problem can be further implemented following proper protocols. To validate the effectiveness of our proposed method, we tested it with two typical ZKP problems: Sudoku and Hamiltonian cycle problem. Through numerical simulations and practical experiments, we demonstrated that the proposed method can efficiently implement ZKP with optical computing based on SPI.

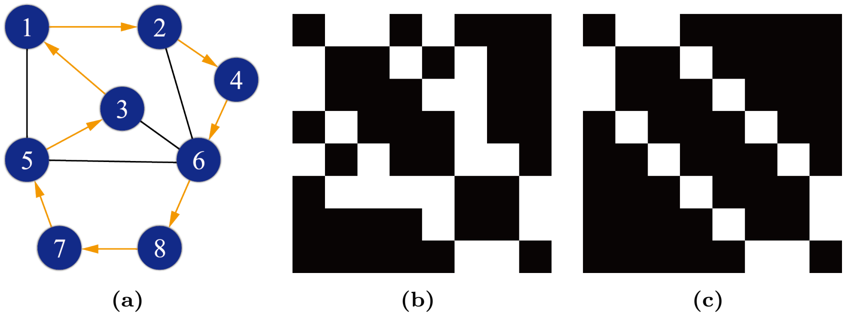
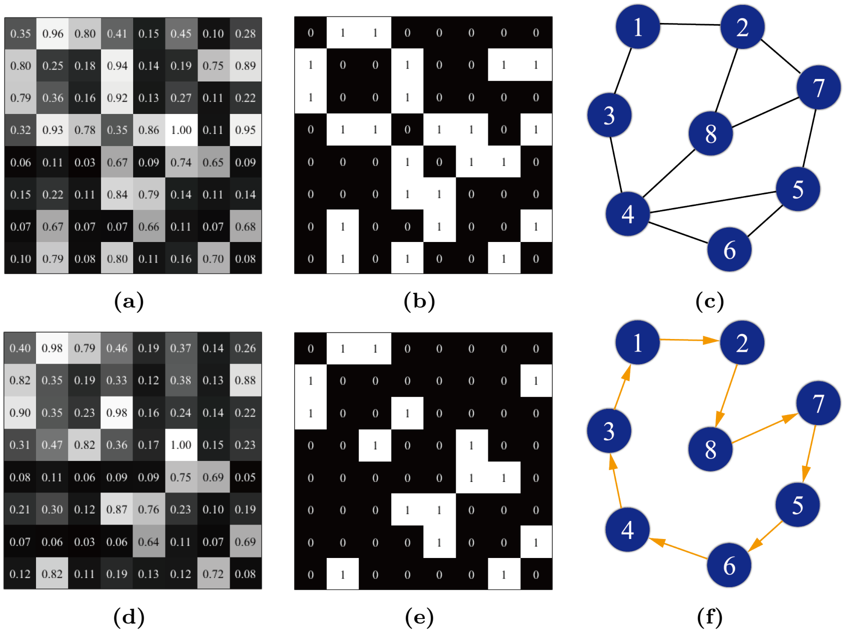


Fig. 14 Hamiltonian graph example with 8 nodes used in optical experiment: (a) Original Hamiltonian graph and Hamiltonian cycle. (b) Encoded image corresponding to Hamiltonian graph. (c) Encoded image corresponding to Hamiltonian cycle.



0.35	0.96	0.80	0.41	0.15	0.45	0.10	0.28
0.80	0.25	0.18	0.94	0.14	0.19	0.75	0.89
0.79	0.36	0.16	0.92	0.13	0.27	0.11	0.22
0.32	0.93	0.78	0.35	0.86	1.00	0.11	0.95
0.06	0.11	0.03	0.67	0.09	0.74	0.65	0.09
0.15	0.22	0.11	0.84	0.79	0.14	0.11	0.14
0.07	0.67	0.07	0.07	0.66	0.11	0.07	0.68
0.10	0.79	0.08	0.80	0.11	0.16	0.70	0.08

(a)

0	1	1	0	0	0	0	0
1	0	0	1	0	0	1	1
1	0	0	1	0	0	0	0
0	1	1	0	1	1	0	1
0	0	0	1	0	1	1	0
0	0	0	1	1	0	0	0
0	1	0	0	1	0	0	1
0	1	0	1	0	0	1	0

(b)

0.40	0.98	0.79	0.46	0.19	0.37	0.14	0.26
0.82	0.35	0.19	0.33	0.12	0.38	0.13	0.88
0.90	0.35	0.23	0.98	0.16	0.24	0.14	0.22
0.31	0.47	0.82	0.36	0.17	1.00	0.15	0.23
0.08	0.11	0.06	0.09	0.09	0.75	0.69	0.05
0.21	0.30	0.12	0.87	0.76	0.23	0.10	0.19
0.07	0.06	0.03	0.06	0.64	0.11	0.07	0.69
0.12	0.82	0.11	0.19	0.13	0.12	0.72	0.08

(d)

0	1	1	0	0	0	0	0
1	0	0	0	0	0	0	1
1	0	0	1	0	0	0	0
0	0	1	0	0	1	0	0
0	0	0	0	0	1	1	0
0	0	0	1	1	0	0	0
0	0	0	0	1	0	0	1
0	1	0	0	0	0	1	0

(e)

Fig. 15 Optical experimental results of ZKP for 8-node Hamiltonian graph based on differential HSPI: (a) Directly reconstructed gray-scale encoded image for the permuted Hamiltonian graph. (b) Corresponding binarized image of (a) after conversion. (c) Corresponding reconstructed permuted graph of (b). (d) Directly reconstructed gray-scale encoded image for the permuted Hamiltonian cycle. (e) Corresponding binarized image of (d) after conversion. (f) Corresponding reconstructed permuted cycle of (e).

It can be potentially useful in a wide range of application scenarios.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgments

This work is supported by Guangdong Research Team for Communication and Sensing Integrated with Intelligent Computing (2024KCXTD047).

References

[1] G. M. Gibson, S. D. Johnson, M. J. Padgett, Single-pixel imaging 12 years on: a review, Opt. Express 28 (19) (2020) 28190–28208.

[2] J. Liu, Z. Yang, Z. Zhao, Y. Tian, Z. Dong, M. Li, Y. Yu, Block scanning single-pixel imaging at the single photon level in a near-infrared band, Opt. Express 33 (5) (2025) 9745–9755.

[3] J. Liang, J. Zhang, Z. Wang, R. Wang, Z. Yao, R. Singh, Z. Tian, W. Zhang, Photoactive polymer-silicon heterostructures for terahertz spatial light modulation and video-rate single-pixel compressive imaging, Adv. Funct. Mater (2025) 2422478.

[4] S. Orlov, R. Ivaškevičiūtė-Povilauskienė, K. Mundrys, P. Kizevičius, E. Nacius, D. Jokubauskis, K. Ikamas, A. Lisauskas, L. Minkevičius, G. Valušis, Light engineering and silicon diffractive optics assisted nonparaxial terahertz imaging, Laser & Photonics Rev. 18 (5) (2024) 2301197.

[5] J. Ma, Single-pixel remote sensing, IEEE Geosci. Remote Sens. Lett. 6 (2) (2009) 199–203.

[6] K. Song, Y. Bian, F. Zeng, Z. Liu, S. Han, J. Li, J. Tian, K. Li, X. Shi, L. Xiao, Photon-level single-pixel 3d tomography with masked attention network, Opt. Express 32 (3) (2024) 4387–4399.

[7] J. Li, T. Liu, B. Wu, Y. Chen, Q. Zhang, Single-pixel fresnel incoherent correlation holography for 3d imaging, Opt. Laser Technol. 174 (2024) 110641.

[8] L. Uguen, R. Piedevache, G. Russias, S. Helmer, D. Tregoat, S. Perrin, Single-pixel-based hyperspectral microscopy, Appl. Phys. Lett. 125 (7) (2024).

[9] L. Ordóñez, A. J. Lenz, E. Ipus, J. Lancis, E. Tajahuerce, Single-pixel microscopy with optical sectioning, Opt. Express 32 (15) (2024) 26038–26051.

[10] Q. Song, Q. H. Liu, W. Chen, High-resolution ghost imaging through dynamic and complex scattering media with adaptive moving average correction, Appl. Phys. Lett. 124 (21) (2024).

[11] D. Ji, B. Zhang, Z. Wang, M. Sun, Speckle pattern calculation and scattering imaging for general surface scattering problem, ACS Photonics 11 (2) (2024) 452–463.

[12] L. Lin, J. Cao, D. Zhou, H. Cui, Q. Hao, Ghost imaging through scattering medium by utilizing scattered light, Opt. Express 30 (7) (2022) 11243–11253.

[13] L. Yi, H. Q. Tan, B. Hou, X. Liu, X-ray-to-nir multi-wavelength imaging through stochastic photoluminescence and compressed encoding, Matter 7 (7) (2024) 2431–2447.

[14] P. L. McMahon, The physics of optical computing, Nat. Rev. Phys. 5 (12) (2023) 717–734.

[15] N. L. Kazanskiy, M. A. Butt, S. N. Khonina, Optical computing: Status and perspectives, Nanomaterials 12 (13) (2022) 2171.

[16] D. Mengu, Y. Luo, Y. Rivenson, A. Ozcan, Analysis of diffractive optical neural networks and their integration with electronic neural networks, IEEE J. Select. Topics Quantum Electron. 26 (1) (2019) 1–14.

[17] H. Ren, Y. Feng, S. Zhou, D. Wang, X. Yang, S. Chen, All-optical dct encoding and information compression based on diffraction neural network, ACS Photonics 12 (2) (2025) 1196–2111.

[18] G. Lu, J. Qiu, T. Liu, D. Zhang, S. Xiao, T. Yu, Metasurface-based diffractive optical networks with dual-channel complex amplitude modulation, J. Lightwave. Technol. 42 (20) (2024) 7282–7290.

[19] Y. Huang, W. Liu, R. Sun, T. Fu, Y. Wang, Z. Huang, S. Yang, H. Chen, Diffraction-driven parallel convolution processing with integrated photonics, Laser & Photonics Rev. 19 (4) (2025) 2400972.

[20] Z. Zhou, Z. Li, W. Zhou, N. Chi, J. Zhang, Q. Dai, Resource-saving and high-robustness image sensing based on binary optical computing, Laser & Photonics Rev. 19 (7) (2024) 2400936.

[21] S. Hengeveld, N. R. da Silva, D. Gonçalves, P. S. Ribeiro, A. Mucherino, An optical processor for matrix-by-vector multiplication: an application to the distance geometry problem in 1d, J. Opt. 24 (1) (2021) 015701.

[22] J. Spall, X. Guo, T. D. Barrett, A. Lvovsky, Fully reconfigurable coher-

ent optical vector–matrix multiplication, Optics Letters 45 (20) (2020) 5752–5755.

[23] J. Xu, Y. Luo, S. Xiao, F. Kang, K. L. Tsakmakidis, All-optical digital logic based on unidirectional modes, Adv. Opt. Mater 11 (1) (2023) 2201836.

[24] Y. Wang, J. Cheng, F. Fan, Y. Peng, Y. Liu, S. Chang, S. Zhuang, All-in-one cascadable dynamic terahertz logic gates enabled by polarization encoding and multiplexing, Laser & Photonics Rev. (2025) 2500072.

[25] L. Liu, D. Ni, L. Dai, Spatial anomaly detection in hyperspectral imaging using optical neural networks, IEEE Intell. Syst. 38 (2) (2023) 64–72.

[26] F. Zhang, Y. Guo, M. Pu, L. Chen, M. Xu, M. Liao, L. Li, X. Li, X. Ma, X. Luo, Meta-optics empowered vector visual cryptography for high security and rapid decryption, Nat. Commun 14 (1) (2023) 1946.

[27] X. Yang, M. S. S. Rahman, B. Bai, J. Li, A. Ozcan, Complex-valued universal linear transformations and image encryption using spatially incoherent diffractive networks, Adv. Photonics Nexus 3 (1) (2024) 016010–016010.

[28] Y. Gao, S. Jiao, J. Fang, T. Lei, Z. Xie, X. Yuan, Multiple-image encryption and hiding with an optical diffractive neural network, Opt. Commun. 463 (2020) 125476.

[29] S. Jiao, C. Zhou, Y. Shi, W. Zou, X. Li, Review on optical image hiding and watermarking techniques, Opt. Laser Technol. 109 (2019) 370–380.

[30] X. Li, M. Zhao, Y. Xing, L. Li, S.-T. Kim, X. Zhou, Q.-H. Wang, Optical encryption via monospectral integral imaging, Opt. Express 25 (25) (2017) 31516–31527.

[31] Y. Shi, T. Li, Y. Wang, Q. Gao, S. Zhang, H. Li, Optical image encryption via ptychography, Optics letters 38 (9) (2013) 1425–1427.

[32] L. Bian, X. Chang, S. Jiang, L. Yang, X. Zhan, S. Liu, D. Li, R. Yan, Z. Gao, J. Zhang, Large-scale scattering-augmented optical encryption, Nat. Commun 15 (1) (2024) 9807.

[33] P. Zheng, Z. Ye, J. Xiong, H. Liu, Computational ghost imaging encryption with a pattern compression from 3d to 0d, Opt. Express 30 (12) (2022) 21866–21875.

[34] P. Clemente, V. Durán, V. Torres-Company, E. Tajahuerce, J. Lancis, Optical encryption based on computational ghost imaging, Optics letters 35 (14) (2010) 2391–2393.

[35] X. Wang, Q. Zhou, L. Zhang, J. Xue, B. Xu, X. Yu, S. Wang, Z. Zhang, Computational imaging encryption with a steganographic and holo-

graphic authentication strategy, Laser & Photonics Rev. 18 (6) (2024) 2300820.

[36] H. Zeng, C. Zhang, X. Li, S. Liu, J. Guo, Y. Xing, S.-T. Kim, D. Li, Y. Liu, Chosen plaintext attack on single pixel imaging encryption via neural differential cryptanalysis, Laser & Photonics Rev. 19 (3) (2025) 2401056.

[37] Z. Zhang, S. Jiao, M. Yao, X. Li, J. Zhong, Secured single-pixel broadcast imaging, Opt. Express 26 (11) (2018) 14578–14591.

[38] Z. Ye, B. Su, P. Qiu, W. Gao, Secured regions of interest (srois) in single-pixel imaging, Sci. Rep. 9 (1) (2019) 12782.

[39] X. Zhan, C. Zhu, Z. Gao, S. Wang, Q. Jiao, L. Bian, Ultrahigh-security single-pixel semantic encryption, Optics Letters 47 (23) (2022) 6169–6172.

[40] S. Jiao, J. Feng, Y. Gao, T. Lei, X. Yuan, Visual cryptography in single-pixel imaging, Opt. Express 28 (5) (2020) 7301–7313.

[41] S. Goldwasser, S. Micali, C. Rackoff, The knowledge complexity of interactive proof-systems, ACM, 2019.

[42] A. Acar, H. Aksu, A. S. Uluagac, M. Conti, A survey on homomorphic encryption schemes: Theory and implementation, ACM Comput. Surv 51 (4) (2018) 1–35.

[43] M. Albrecht, M. Chase, H. Chen, J. Ding, S. Goldwasser, S. Gorbunov, S. Halevi, J. Hoffstein, K. Laine, K. Lauter, et al., Homomorphic encryption standard, Springer, 2021.

[44] S. Goldwasser, S. Micali, C. Rackoff, The knowledge complexity of interactive proof-systems, in: STOC, 1985, pp. 291–304.

[45] K. Tanaka, S. Sasaki, K. Shinagawa, T. Mizuki, Only two shuffles perform card-based zero-knowledge proof for sudoku of any size, in: 2025 Symposium on Simplicity in Algorithms (SOSA), 2025, pp. 94–107.

[46] T. Sasaki, D. Miyahara, T. Mizuki, H. Sone, Efficient card-based zero-knowledge proof for sudoku, Theor. Comput. Sci. 839 (2020) 135–142.

[47] R. Gradwohl, M. Naor, B. Pinkas, G. N. Rothblum, Cryptographic and physical zero-knowledge proof systems for solutions of sudoku puzzles, Theory of Computing Syst. 44 (2) (2009) 245–268.

[48] F. Martín-Fernández, P. Caballero-Gil, C. Caballero-Gil, Authentication based on non-interactive zero-knowledge proofs for the internet of things, Sensors 16 (1) (2016) 75.

[49] S. Sasaki, K. Shinagawa, Physical zero-knowledge proof for sukoro, New Gener. Comput. 42 (3) (2024) 381–398.

[50] B. Sun, M. Edgar, R. Bowman, L. Vittert, S. Welsh, A. Bowman, M. Padgett, 3-dimensional computational ghost imaging, in: Frontiers in Optics, 2013, pp. FW5D–2.

[51] Z. Zhang, X. Wang, G. Zheng, J. Zhong, Hadamard single-pixel imaging versus fourier single-pixel imaging, Opt. Express 25 (16) (2017) 19619–19639.

[52] Z. Tang, T. Tang, J. Chen, S. Lv, Y. Liu, Spatial temporal fourier single-pixel imaging, Optics letters 48 (8) (2023) 2066–2069.

[53] M. Alemohammad, J. R. Stroud, B. T. Bosworth, M. A. Foster, High-speed all-optical haar wavelet transform for real-time image compression, Opt. Express 25 (9) (2017) 9802–9811.

[54] B. Liu, Z. Yang, X. Liu, L.-a. Wu, Coloured computational imaging with single-pixel detectors based on a 2d discrete cosine transform, J. Mod. Opt. 64 (3) (2017) 259–264.

[55] X. Yu, R. I. Stantchev, F. Yang, E. Pickwell-MacPherson, Super sub-nyquist single-pixel imaging by total variation ascending ordering of the hadamard basis, Sci. Rep. 10 (1) (2020) 9338.

[56] P. G. Vaz, D. Amaral, L. Requicha Ferreira, M. Morgado, J. Cardoso, Image quality of compressive single-pixel imaging using different hadamard orderings, Opt. Express 28 (8) (2020) 11666–11681.

[57] J. C. Bermond, Hamiltonian graphs, Selected topics in graph theory (1979) 127–167.

[58] M. Blum, How to prove a theorem so no one else can claim it, in: Proceedings of the International Congress of Mathematicians, Vol. 1, 1986, p. 2.