Received August 3, 2019, accepted August 8, 2019, date of publication August 19, 2019, date of current version September 6, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2936119

Known-Plaintext Attack and Ciphertext-Only Attack for Encrypted Single-Pixel Imaging

SHUMING JIAO, TING LEI, YANG GAO, ZHENWEI XIE, AND XIAOCONG YUAN
Nanophotonics Research Center, Shenzhen University, Shenzhen 518060, China

Corresponding author: Xiaocong Yuan (xcyuan@szu.edu.cn)

This work was supported in part by the National Natural Science Foundation of China under Grant 61805145 and Grant11774240, in part by the Leading Talents Program of Guangdong Province under Grant 00201505, in part by the Natural Science Foundation of Guangdong Province under Grant 2016A030312010, and in part by the Shenzhen Science and Technology Innovation Commission under Grant KQJSCX20170727100838364.

ABSTRACT In many previous works, a single-pixel imaging (SPI) system has been constructed as an optical image encryption system. Unauthorized users are not able to reconstruct the plaintext image from the ciphertext intensity sequence without knowing the illumination pattern key. However, the cryptanalysis of encrypted SPI has been seldom investigated in the past. In this work, we propose a known-plaintext attack scheme and a ciphertext-only attack scheme for an encrypted SPI system for the first time. The known-plaintext attack is implemented by interchanging the roles of illumination patterns and object images in the SPI model. The ciphertext-only attack is implemented based on the statistical features of single-pixel intensity values under certain circumstances. The two schemes can crack encrypted SPI systems and successfully recover the key containing correct illumination patterns.

INDEX TERMS Single-pixel imaging, ghost imaging, encryption, attack, plaintext, ciphertext.

I. INTRODUCTION

Optical encryption, authentication and watermarking systems [1]–[3] constructed for information security applications have several advantages such as multi-dimensional parallel processing capabilities, fast processing speed and direct processing of physical objects without digitalization. In previous works, an image encryption system can be physically implemented by adopting various types of optical imaging systems, including but not limited to systems based on double random phase encoding (DRPE) [4], holography [5], [6], integral imaging [7]–[9], ptychography [10], [11], and single-pixel imaging (SPI) [12]–[21]. In these systems, a plaintext image is first converted to a light field, and it is then optically transformed into a ciphertext light field with certain physical encryption keys (e.g. random phase masks or random illumination patterns).

SPI [22], [23] is an optical imaging technique that captures an object image with a single-pixel detector instead of a pixelated sensor array. After the target object is sequentially illuminated with many varying patterns and a single-pixel intensity sequence is recorded, the object image can be computationally reconstructed. SPI has some potential advantages over conventional sensor-array cameras [22]–[24]. For example, the cost of a single-pixel detector is much lower than a sensor array in some invisible wavebands. SPI can support indirect-line-of-sight imaging and weak-light imaging. Compared with other optical encryption architectures [4]–[11], the sensor is a simple bucket light detector and a real intensity value instead of a complex light field is recorded each time in an encrypted SPI system, which is easier to implement experimentally. A typical optical setup for a SPI system is shown in Fig. 1.

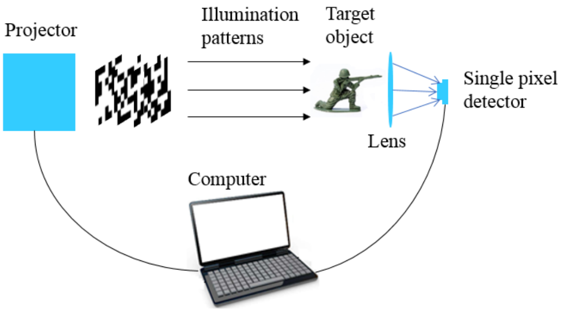

FIGURE 1. Optical setup for a SPI system.

The strength of security is a crucial concern for any type of encryption system. Attacking methods can be developed to

The associate editor coordinating the review of this manuscript and approving it for publication was Chien-Ming Chen.

uncover the security flaws of an existing encryption system. Meanwhile, the security strength of an encryption system can be further enhanced against these attacking methods. Analogous to a shield-and-spear relationship, encryption methods and attacking methods (or cryptanalysis) are upgraded regarding to each other's previous upgrades in an iterative manner to finally produce a more secure system.

Common attacks to an image encryption system include chosen-plaintext attack (CPA), known-plaintext attack (KPA) and ciphertext-only attack (COA). In a CPA, it is assumed that the attacker can access the encryption system and control the input plaintext content. The security keys are recovered using selected pairs of plaintexts and ciphertexts. The CPA is relatively easy to implement but the assumption that the attacker can freely choose the plaintext may be invalid in many practical situations. In a KPA, a number of plaintext-ciphertext pairs are available and they are given randomly instead of being selected by the attackers. A KPA can threaten an encryption system under conditions that are more general than those for a CPA. In a COA, the attacker can only access a certain number of ciphertexts and does not know any plaintext information. A COA requires the least amount of information to crack an encryption system and reveals the most severe security flaw of an encryption system. At the same time, COA is usually most difficult to implement for an attacker.

For digital encryption, the cryptanalysis of different encryption systems can be found in many past literatures [25]–[29]. For other types of optical encryption systems such as DRPE [4], various implementations of encryption systems [30]–[34] and various types of cryptanalysis [35]–[41] including the CPA, KPA and COA have been extensively investigated. However, for encrypted SPI, many works have been conducted on the design of encryption systems [12]–[21] since the earliest attempt [12] but there has been little work on cryptanalysis previously. As far as the authors know, there has been only one such work [42], in which CPA methods were proposed. No KPA or COA schemes have even been proposed for encrypted SPI systems. In this work, a KPA scheme and a COA scheme for encrypted SPI are investigated for the first time.

II. WORKING PRINCIPLES OF AN ENCRYPTED SPI SYSTEM

There are usually three major components in SPI, namely the object image $O(n)$ (n = 1, 2, ..., N), the illumination patterns $K(m, n)$ (m = 1, 2, ..., M; n = 1, 2, ..., N) and the recorded single-pixel intensity sequence $C(m)$ (m = 1, 2, ..., M). In an encrypted SPI system, the object image $O(n)$ can be employed as the plaintext image, the illumination patterns $K(m, n)$ are employed as the encryption (and decryption) key and the recorded single-pixel intensity sequence $\mathcal{C}(m)$ is employed as the ciphertext [12]. The general framework of an encrypted SPI system is shown in Fig. 2.

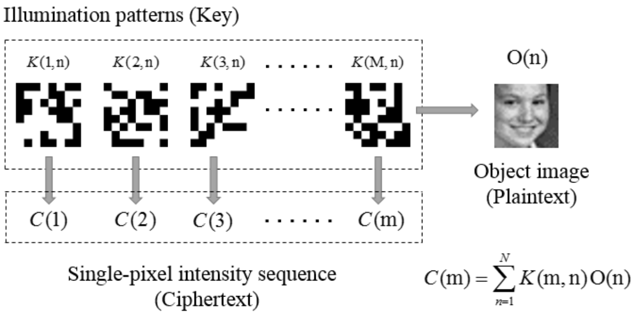
Illumination patterns (Key)
K(1,n)
K(2,n)
K(3,n)
K(M,n)
O(n)
Object image
(Plaintext)
C(1)
C(2)
C(3)
C(m)
Single-pixel intensity sequence
(Ciphertext)
$C(\mathrm{m}) = \sum_{n=1}^{N} K(\mathrm{m,n})O(\mathrm{n})$

FIGURE 2. General framework of an encrypted SPI system.

The total number of pixels in the object image is denoted as N and the plaintext image is represented by a column vector $O(n)$ with length N. The total number of pixels in each illumination pattern is identical to the resolution of the object image. It is assumed that the object image $O(n)$ is sequentially illuminated by a total of M different illumination patterns and all these patterns jointly constitute an illumination pattern matrix $K(m, n)$ with M rows and N columns. The m_{th} single-pixel intensity value recorded by the detector is the inner product of the m_{th} row in K and the object image $O(n)$ mathematically. The single-pixel intensity sequence can be represented as a column vector $\mathcal{C}(m)$ (m = 1, 2, ..., M) with length M. The mathematical model of the entire SPI imaging process is expressed by (1). The number of illuminations M can be smaller than, equal to and larger than the number of pixels N in the object image. The ratio M/N is referred to as the sampling ratio in SPI.

$$\begin{bmatrix} C(1) \\ C(2) \\ \vdots \\ C(M) \end{bmatrix} = \begin{bmatrix} K(1,1) & \cdots & K(1,N) \\ \vdots & \ddots & \vdots \\ K(M,1) & \cdots & K(M,N) \end{bmatrix} \begin{bmatrix} O(1) \\ O(2) \\ \vdots \\ O(N) \end{bmatrix} \tag{1}$$

In SPI, after M illuminations and recordings, the object image can be computationally reconstructed from $K(m, n)$ $(1 <= m <= M, 1 <= n <= N)$ and $C(m)(1 <= m <= M)$ with various algorithms [43]. The image reconstruction in SPI is essentially the process of solving a system of linear equations and finding the optimal solutions. As an encryption system, the plaintext image $O(n)$ is recovered when both the ciphertext $C(m)$ and key $K(m, n)$ are available. For unauthorized users not knowing the key, the plaintext image cannot be disclosed from the ciphertext and its information is protected.

In practical SPI experiments, projection devices for pattern illuminations, such as a digital micromirror device (DMD), are usually binary [44], [45]. Each pixel in the illumination patterns can be assumed to have a random binary value of 0 or 1. The total number of possible combinations for M illumination patterns in the key space is 2^{MN}. A brute-force attack is difficult to realize because it takes huge computational resources to attempt all possible combinations in reconstructing the true plaintext image when the key is not known. If any information about the M illumination patterns in the key is not open to the public, the system is referred as a Type-I encrypted SPI system in this paper. The data size of all M illumination patterns (each having N pixels)

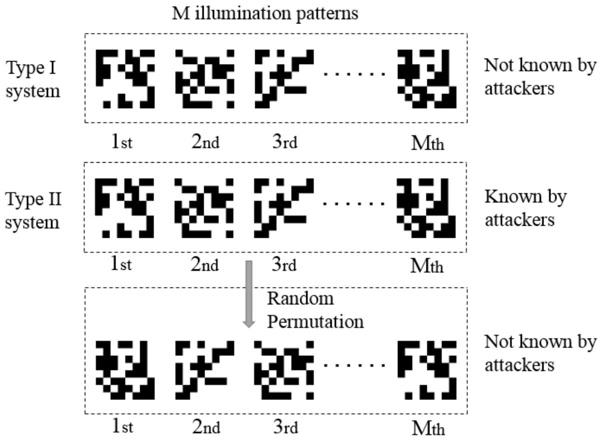

FIGURE 3. Type-I and Type-II encrypted SPI systems.

can be considerably large and the transmission & storage cost of encryption (and decryption) keys can be rather high. As an alternative, the permutation of illumination patterns, instead of the original illumination patterns, can be employed as the key, which is referred to as a Type-II encrypted SPI system in this paper. In a Type-II system, the pixel values of the original M illumination patterns before permutation are open to the public. However, the order is random and remains known to authorized users only. For example, the original fifth illumination pattern may be arranged as the first one in the key while the original seventh pattern may be arranged as second one. The total number of possible combinations in the key is $M!$ (where "!" indicates the factorial) for M illumination patterns. Even though $M!$ is significantly smaller than 2^{MN}, the key space of a Type-II system still grows rapidly as the value of M increases. As an example, even if there are only M = 16 illumination patterns, there are 16! = 20,922,789,888,000 arrangements. The number of possible combinations reaches 2.6×10^{35} when M = 32. A brute-force attack is thus difficult to realize for a Type-II system as well. In Fig. 3, Type-I and Type-II encrypted SPI systems are compared. In this work, some investigations of KPA and COA are conducted for encrypted SPI systems of both Type-I and Type-II.

III. KPA TO AN ENCRYPTED SPI SYSTEM

As stated above, the plaintext image can only be recovered from the ciphertext (i.e. the single-pixel intensity sequence) when the key (containing all the illumination patterns) is known. However, if the same key is repetitively employed to encrypt different object images, the attacker may collect all these plaintext images and corresponding ciphertext intensity sequences. From these plaintext-ciphertext pairs, the attacker can possibly figure out most of the pixel values in the key and crack the encryption system. A KPA scheme for encrypted SPI is proposed for the first time in this paper. Our proposed KPA is similar to the image reconstruction process in conventional SPI but the roles of illumination patterns and object images are interchanged. In conventional SPI, the object image is sequentially illuminated by varying illumination patterns. In our proposed KPA model, one illumination pattern is considered to be "sequentially illuminated" by varying plaintext images.

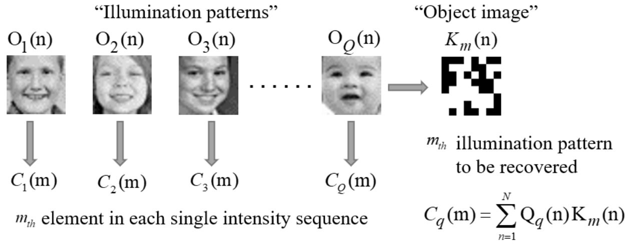
"Illumination patterns"
"Object image"
$O_1(n)$
$O_2(n)$
$O_3(n)$
$O_Q(n)$
$K_m(n)$
$C_1(m)$
$C_2(m)$
$C_3(m)$
$C_Q(m)$
m_{th} illumination pattern to be recovered
m_{th} element in each single intensity sequence
$C_q(m) = \sum_{n=1}^{N} Q_q(n)K_m(n)$

FIGURE 4. Proposed KPA model for encrypted SPI.

As an example, it is assumed that the attacker collects Q pairs of plaintexts $O_q(n)$ (n = 1, 2, . . ., N; q = 1, 2, . . ., Q) and ciphertexts $C_q(m)$ (m = 1, 2, . . ., M; q = 1, 2, . . ., Q). For the m_{th} illumination pattern $K_m(n)$ (m = 1, 2, . . ., M; n = 1, 2, . . ., N), the following relationship holds, given by (2).

$$\begin{bmatrix} O_1(1) & O_1(2) & \cdots & O_1(N) \\ O_2(1) & O_2(2) & \cdots & O_2(N) \\ \vdots & \vdots & \ddots & \vdots \\ O_Q(1) & O_Q(2) & \cdots & O_Q(N) \end{bmatrix} \begin{bmatrix} K_m(1) \\ K_m(2) \\ \vdots \\ K_m(N) \end{bmatrix} = \begin{bmatrix} C_1(m) \\ C_2(m) \\ \vdots \\ C_Q(m) \end{bmatrix} \tag{2}$$

In (2), each plaintext image O_q [each row in the matrix $O_q(n)$ (n = 1, 2, . . ., M; q = 1, 2, . . ., Q)] can be considered as the "q_{th} illumination pattern", the m_{th} illumination pattern K_m can be considered as the "object image" and all m_{th} elements in the Q ciphertexts can be considered as the "intensity sequence" in the KPA model. The m_{th} illumination pattern K_m can be reconstructed from all plaintext images and all m_{th} elements in ciphertext single-pixel intensity sequences $C_q(m)$(q = 1, 2, . . ., Q) with conventional reconstruction algorithms [43] in SPI, as shown in Fig. 4 (in comparison with Fig. 2). Each individual illumination pattern in the key is recovered independently from m = 1 to m = M. The only difference is that in conventional SPI, the object images are usually locally smooth in terms of neighboring pixel intensities and the illumination patterns are orthogonal or random. Total-variation regularization [43], [46] can be employed to achieve a high-quality reconstruction with a minimum number of illuminations. However, in a KPA, each "object image" is a random illumination pattern and the "illumination pattern" becomes locally smooth when the roles of images and illumination patterns are interchanged. It becomes more difficult to achieve good reconstruction results for a low sampling-rate (i.e. a small number of plaintext-ciphertext pairs).

In this work, the conjugate gradient descent algorithm [43], [47] is adopted for the recovery of illumination patterns from plaintext-ciphertext pairs. More details on the working principles of this algorithm can be found in the literature [43]. In brief, the conjugate gradient descent algorithm is an iterative method of searching for an optimal that best fits (2). In each iteration, the algorithm calculates the gradient to locate the direction of steepest descent, and then performs a line search to locate the optimum step size. The solution moves downhill towards the minimum fitting error efficiently in conjugate directions rather than along local gradients. After the optimal is obtained, it is normalized and binarized.

Each of M illumination patterns is recovered individually with the same approach stated above. Finally, the entire encryption key matrix is recovered and a Type-I encryption system is cracked. For a Type-II system, we compare each recovered pattern with all publicly known original patterns and map it to the most similar one that has not been matched previously with other recovered patterns. After the matching steps, the rearranged order of original illumination patterns is known and the key is recovered.

IV. COA TO AN ENCRYPTED SPI SYSTEM

In a KPA, multiple pairs of plaintext images and ciphertext intensity sequences are known and the illumination patterns (i.e. the encryption/decryption key) are recovered. In a COA, only a certain number of single-pixel intensity sequences are available and it is a challenging task to directly recover the illumination patterns. In this work, only a COA to a Type-II encrypted SPI system under certain conditions is attempted. It is assumed that SPI is performed repetitively for the same category of object images (e.g. images of different handwritten numbers). The attacker cannot access any of the original object images (plaintexts). However, the attacker may collect a large number of exemplar images similar to the actual object images.

The basic idea is that the single-pixel intensity values recorded with the same illumination pattern for the same category of object images follow a certain statistical distribution. The attacker may be able to figure out the illumination patterns by comparing the histograms of single-pixel intensity values generated from the actual object images with those virtually generated from the exemplar object images he has collected.

For a Type-II system, the goal of an attack is to find the order in which the original sequence of illumination patterns is permutated. From Q object images, Q single pixel intensity sequences $C_q(m)$ (q = 1, 2, . . ., Q) can be recorded with the m_{th} rearranged illumination pattern in the key. The attacker also collects Q exemplar images, and then Q single-pixel intensity sequences $C_q^{'}(m)$ (q = 1, 2, . . ., Q) can be virtually generated with the m_{th} original illumination pattern. The attacker can generate the intensity sequences $C_q^{'}(1)$, $C_q^{'}(2), \ldots, C_q^{'}(M)$ (q = 1, 2, . . . , Q) for all M original illumination patterns. For the m_{th} illumination on the actual object images, the attacker compares the statistical distribution of $C_q(m)$ with $C_q^{'}(1)$, $C_q^{'}(2), \ldots C_q^{'}(m)$ and (q = 1, 2, . . ., Q) and finds the best match. As an example, if $C_q(1)$ is most similar to $C_q^{'}(5)$, then the attacker can conclude the fifth original illumination pattern is arranged as the first one in the encryption key. After a mapping for each $C_q(m)$ to $C_q^{'}(m)$ (m = 1,2, . . . , M), the attacker can obtain the correct permutation of the illumination patterns and recover the key.

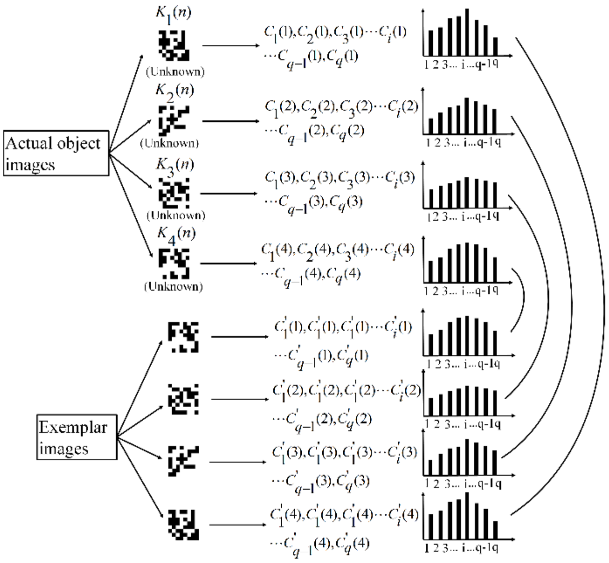
$K_1(n)$
(Unknown)
$K_2(n)$
(Unknown)
$K_3(n)$
(Unknown)
$K_4(n)$
(Unknown)
Actual object images
Exemplar images
$C_1(1), C_2(1), C_3(1) \cdots C_i(1)$
$\cdots C_{q-1}(1), C_q(1)$
$C_1(2), C_2(2), C_3(2) \cdots C_i(2)$
$\cdots C_{q-1}(2), C_q(2)$
$C_1(3), C_2(3), C_3(3) \cdots C_i(3)$
$\cdots C_{q-1}(3), C_q(3)$
$C_1(4), C_2(4), C_3(4) \cdots C_i(4)$
$\cdots C_{q-1}(4), C_q(4)$
$C_1^{'}(1), C_1^{'}(1), C_1^{'}(1) \cdots C_i^{'}(1)$
$\cdots C_{q-1}^{'}(1), C_q^{'}(1)$
$C_1^{'}(2), C_1^{'}(2), C_1^{'}(2) \cdots C_i^{'}(2)$
$\cdots C_{q-1}^{'}(2), C_q^{'}(2)$
$C_1^{'}(3), C_1^{'}(3), C_1^{'}(3) \cdots C_i^{'}(3)$
$\cdots C_{q-1}^{'}(3), C_q^{'}(3)$
$C_1^{'}(4), C_1^{'}(4), C_1^{'}(4) \cdots C_i^{'}(4)$
$\cdots C_{q-1}^{'}(4), C_q^{'}(4)$
1 2 3... i...q-1q

FIGURE 5. Proposed COA model for encrypted SPI.

Mathematically, the similarity in the statistical distributions between $[C_1(m), C_2(m), \ldots, C_Q(m)]$ (m = 1, 2, . . ., M) and $[C_1^{'}(m^{'}), C_2^{'}(m^{'}), \ldots, C_Q^{'}(m^{'})]$ (m = 1, 2, . . ., M) can be evaluated in the following way. The intensity values of $C_q(m)$ and $C_q^{'}(m)$ (q = 1, 2, . . ., Q) are statistically distributed within a certain range (e.g. [0 20]). The range can be divided into uniform intervals with certain bin size. For example, if the bin size is 5, there will be four intervals, namely [0 5], [5 10], [10 15] and [15 20]. The number of intensity values falling into each interval is then counted and a vector containing these numbers (e.g. [7 13 16 8]) as a histogram is obtained. The difference between two number-count vectors can be measured by using Euclidean distance. $C_q(m)$ will be map to $C_q^{'}(m^{'})$ if the Euclidean distance between the number-count vectors of $C_q(m)$ and $C_q^{'}(m^{'})$ is smallest, indicating that their statistical distributions are most similar.

V. RESULTS AND DISCUSSIONS

A. KPA

In the simulation of a KPA, there are N = 32 × 32 pixels in the object image and in each illumination pattern. Three different numbers of binary random illumination patterns, corresponding to three different sampling ratios M/N = 0.4, M/N = 0.7 and M/N = 1, are tested in a Type-I encrypted SPI system. The object image is reconstructed with the total-variation regularization algorithm [43], [46] from the illumination patterns and single-pixel intensity sequences. It is assumed that a varying number of plaintext images and corresponding ciphertext intensity sequences are available to the attacker. The plaintext images are all human-face images taken from UTKFace dataset [48] and some examples shown in Fig. 6(a). The illumination patterns, as the encryption and decryption key, are not known by the attacker originally.

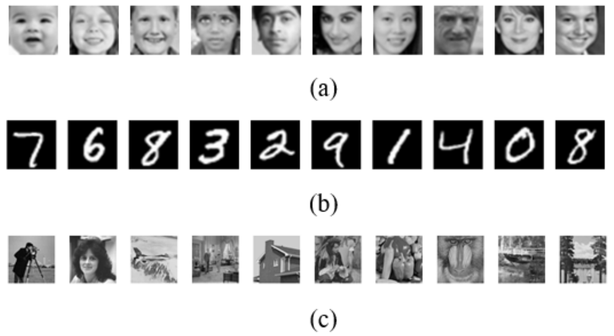

FIGURE 6. Object images in simulation: (a) examples of plaintext images in the UTKFace dataset [39]; (b) examples of plaintext images in the MISNT database [40]; (c)Ten testing images for KPA.

TABLE 1. Results of our proposed KPA scheme for A Type-I encrypted SPI system.

N	M (M/N)	Q (Q/N)	Cracking Correct Rate
32×32	410 (0.4)	1024(1)	0.9668
		2048(2)	0.9935
		3072(3)	0.9978
		4096(4)	0.9991
32×32	717 (0.7)	1024(1)	0.9655
		2048(2)	0.9957
		3072(3)	0.9974
		4096(4)	0.9983
32×32	1024 (1)	1024(1)	0.9683
		2048(2)	0.9944
		3072(3)	0.9976
		4096(4)	0.9982

With these available plaintext-ciphertext pairs, the attacker can crack the encryption system and recover the illumination patterns by adopting the KPA method described in Section 3.

The accuracy of the attacking results is evaluated in two ways. First, all binary pixels in the illumination patterns of the correct key and in the cracked illumination patterns after the attack are compared and the correct rate of cracking (i.e. the percentage of correct pixels) is calculated. Second, the ten test images shown in Fig. 6(c), which are completely different from the plaintext images used in the attack, are encrypted using the patterns in the correct key and then decrypted with both the correct key and the cracked key using our proposed KPA scheme. The average peak signal-to-noise ratio (PSNR) values are calculated and compared for these two cases. The attacking results for a Type-I encrypted SPI system are given in Table 1 and some examples of final recovered images are shown in Fig.7.

The results in Table 1 and Fig. 7 show that the pixels in the illumination patterns can be recovered with high accuracy (e.g. the correct rate of cracking exceeding 99.8%) and the test images can be reconstructed with acceptable visual quality (e.g. a PSNR of over 16dB) using the recovered key, if the attacker has a sufficient number of plaintext-ciphertext pairs. In Fig. 7(a), the decrypted (or reconstructed) images with the correct key have good fidelity. The decrypted images with random wrong keys appear like noise and no information about the actual object image can be visually perceived, as shown in Fig. 7(b). This indicates that an encrypted SPI system has a substantial level of security when the key is not known. However, after our proposed KPA is performed, the decrypted images with the recovered key are close to the original plaintext images, if the number of plaintext-ciphertext pairs available is adequate, as shown in Fig. 7(c), Fig. 7(d) and Fig. 7(e).

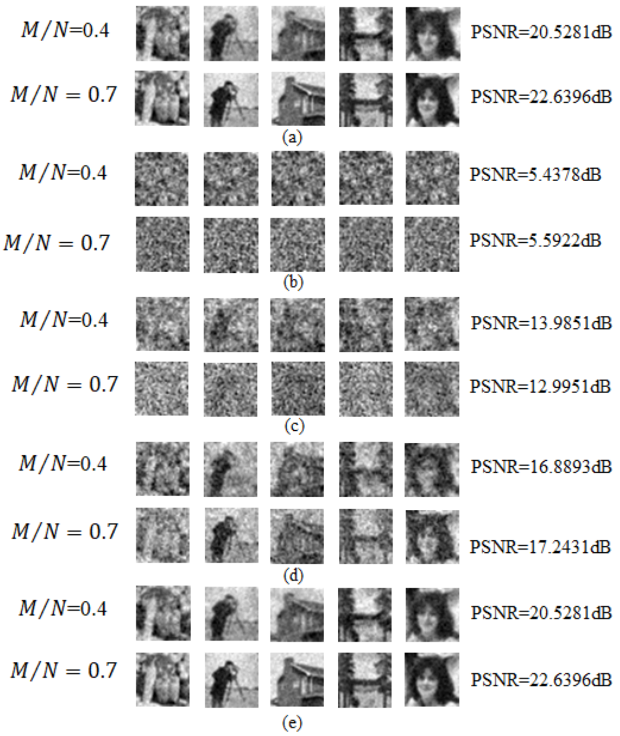

FIGURE 7. KPA results when N = 32 × 32 and the sampling rate M/N is 0.4 (upper) or 0.7 (lower) for a Type-I encrypted SPI system: (a) Decryption with the correct key; (b) Decryption with a random wrong key; (c) Decryption with the recovered key when q = 2048; (d) Decryption with the recovered key when q = 3072; (e) Decryption with the recovered key when q = 4096.

The results reveal that our proposed KPA scheme is an effective approach for cracking a Type-I encrypted SPI system. It is observed that when most pixels in the illumination patterns are successfully recovered (e.g. the correct rate is around 97%), the object image reconstructed using recovered patterns is still rather poor (e.g. 12dB or 13dB) owing to the small percentage of error bits. The encryption system can be truly cracked only when the illumination patterns are recovered with very high accuracy (e.g. over 99.6%) for complicated grayscale plaintext images as in Fig. 6(c). Each illumination pattern in the key is recovered independently one by one in our scheme, and the number of plaintext-ciphertext pairs required for a successful attack thus does not evidently increase when the sampling

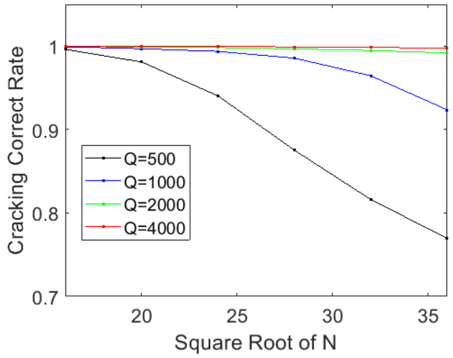

FIGURE 8. Performance of our proposed KPA scheme for a Type-I encrypted SPI system when the image size varies (the sampling rate M/N = 0.7).

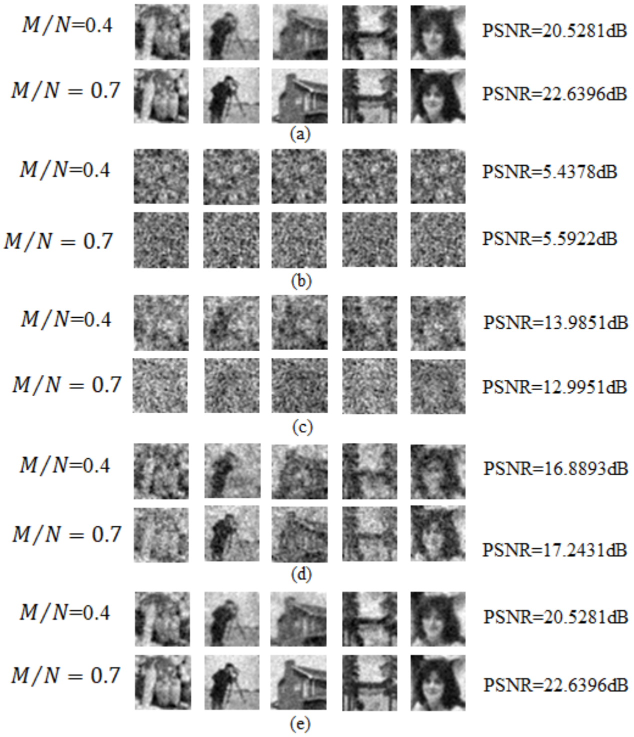

FIGURE 9. KPA results when N = 32 × 32 and the sampling rate (*M*/*N*) is 0.4 (upper) or 0.7 (lower) for a Type-II encrypted SPI system: (a) decryption with the correct key; (b) decryption with a random wrong key; (c) decryption with the recovered key when q = 31; (d) decryption with the recovered key when q = 72; (e) decryption with the recovered key when q = 92.

ratio increases. However, the number of plaintext-ciphertext pairs required for a successful attack depends on the number of pixels N (or the image size). The relationship between the correct rate of cracking and the image size is presented in Fig. 8. The results indicate that more plaintext-ciphertext pairs are required for cracking one illumination pattern containing more pixels.

Our proposed KPA scheme is also implemented for a Type-II encrypted SPI system. The parameters in the simulation are basically the same as above except that the number of plaintext-ciphertext pairs attempted is much smaller.f The results are presented in Table 2 and Fig. 9.

TABLE 2. Results of our proposed KPA scheme for a Type-II encrypted SPI system.

N	M (M/N)	Q (Q/N)	Cracking Correct Rate
32×32	410 (0.4)	31 (0.03)	0.9434
		51 (0.05)	0.9929
		72 (0.07)	0.9977
		92 (0.09)	1
32×32	717 (0.7)	31 (0.03)	0.9219
		51 (0.05)	0.9972
		72 (0.07)	0.9986
		92 (0.09)	1
32×32	1024 (1)	31 (0.03)	0.8975
		51 (0.05)	0.9936
		72 (0.07)	0.9980
		92 (0.09)	1

The results above show that our proposed scheme can be used to crack a Type-II system. Far fewer plaintext-ciphertext pairs are required for a successful attack to a Type-II system than a Type-I system. As stated in Section 2, the number of possible combinations in the key space is for a Type-I system and M! for a Type-II system. The attacker needs to recover every pixel in the illumination pattern for a Type-I system but only needs to recover the pattern permutation for a Type-II system. The security of a Type-II system is weaker and relatively crack. When the entire order of permutation is fully recovered (e.g. when Q = 92 in Table 2), all the original illumination patterns can be recovered correctly and all pixels in the recovered key will have correct values (i.e. the correct rate of cracking is 100%). In comparison, for a Type-I system, the majority of pixel values can be recovered with our proposed KPA scheme but it is difficult to achieve a 100% correct rate.

B. COA

In the simulation of a COA, there are N = 8 × 8, 12 × 12 and 16 × 16 pixels in the object image and in each illumination pattern. There are M = 64 binary random illumination patterns. The plaintext images are resized digital images of numerals taken from the MISNT database [49], as shown in Fig. 6(b). It is assumed that there are totally Q plaintext images and Q corresponding single-pixel sequences. The Q single-pixel sequences are the only data available to an attacker. A Type-II encrypted SPI system is considered and the 64 original illumination patterns are randomly permutated by rearranging the order. In addition, it is assumed that the attacker can collect Q exemplar images similar to the actual plaintext images. It shall be noted that the exemplar images also belong to the MINST database but they are different from the Q plaintext images. Both the plaintext images and exemplar images are randomly chosen from the MINST database.

TABLE 3. Results of our proposed COA scheme for a Type-II encrypted SPI system.

N	M	Q	Cracking Correct Rate
8×8	64	6000	0.8854
		10000	0.9427
		14000	1
12×12	64	6000	0.7813
		10000	0.9063
		14000	1
16×16	64	6000	0.5469
		10000	0.6875
		14000	0.8438
32×32	64	6000	0.03125
		10000	0.046875
		14000	0.0625

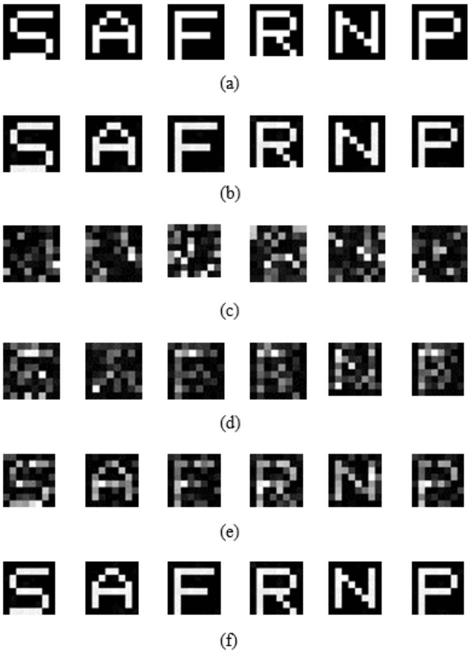

FIGURE 10. COA results when the N = 8 × 8 and M = 64 for a Type-II encrypted SPI system: (a) original plaintext images; (b) Decryption with the correct key; (c) Decryption with a random wrong key; (d) Decryption with the recovered key when q = 6000; (e) Decryption with the recovered key when q = 10000; (f) Decryption with the recovered key when q = 14000.

Our proposed COA scheme is based on statistical features and the number Q has to be sufficiently large, as governed by the law of large numbers. In the simulation, Q is set at 6000, 10000 and 14000. In the comparison of single-pixel intensity distributions, the intensity value range is [0 15] and the bin size is 0.5. The COA results are presented in Table 3 and Fig. 10.

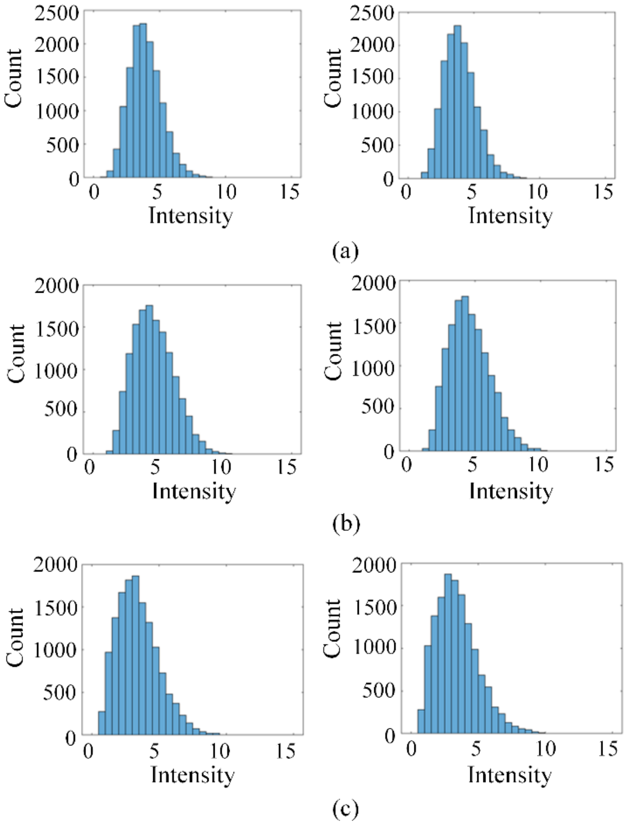

FIGURE 11. Examples of the histograms for recorded single-pixel intensity values from 14000 actual plaintext images (left) and 14000 exemplar images collected by the attacker (right) in COA for three different illumination patterns: (a) Pattern 1; (b) Pattern 2; (c) Pattern 3.

Table 3 shows that our proposed COA scheme can fully crack a Type-II encrypted SPI system when the image size is sufficiently small, and the number of plaintexts Q is sufficiently large. The order of rearranged illumination patterns in the key can be possibly fully recovered (with a correct rate of cracking =100%). As the image size increases, the performance of our proposed COA scheme degrades but the scheme still partially recovers the key. In Fig. 10(a), several English letter images are used as the test plaintext images. After these images are encrypted with the original key, they can be successfully decrypted with our recovered key, as shown in Fig. 10.

In Fig. 11, the histograms of recorded single-pixel intensity values from 14000 actual plaintext images and 14000 exemplar images collected by the attacker for three different illumination patterns are presented. The distributions of single-pixel intensities generated with the same illumination pattern for two different object image sets (belonging to the same image category) are similar statistically. However, the intensity value distributions clearly differ between different patterns. This important property is used to match the unknown pattern with a list of original patterns in recovering the order of permutation.

Our proposed COA scheme performs well under some circumstances but may fail under other circumstances for the following reasons. First, all the plaintext images shall be similar and belong to the same category. Ideally, the intensity value at each pixel position follows a unique statistical distribution. In this way, the single-pixel intensity values will have different statistical features when these images are illuminated by different random patterns. If the plaintext images are random and have almost no common features in the pixel intensity distribution, it is difficult to observe distinguishable statistical features in the recorded single-pixel intensity values for varying illumination patterns. Second, the attacker needs to collect an adequate number of exemplar images similar to the actual images. Ideally, the intensity values of corresponding pixels in the actual images and exemplar images follows the same statistical distribution. In our simulation, when the exemplar images collected by the attacker are replaced with human-face images, instead of numeral images, none of the 64 patterns can be recovered in the correct order ($N = \mathbf{8} \times \mathbf{8}$, $M = 64$ and $Q = 14000$). Third, as shown in the results above, our proposed COA scheme works better for plaintext images with fewer pixels. The scheme may provide poor attacking results or even completely fail when N is large. The single-pixel intensity is a weighted sum of all the pixel values in one plaintext image, and the features of the intensity distributions for different pixels in the plaintext images are therefore more likely to be lost when many pixel values are combined into a single-pixel intensity value.

VI. CONCLUSION

In many previous works, a SPI system is constructed as an optical image encryption system. In such systems, the object image is employed as the plaintext, the illumination pattern is employed as the encryption and decryption key and the recorded single-pixel intensity sequence is employed as the ciphertext. Having a shield and spear relationship, encryption methods and attacking methods play equally critical roles in the investigation of certain types of cryptosystems. Most previous works focused on the design of an encrypted SPI system but there has been little corresponding cryptanalysis. In this work, we propose a KPA scheme and a COA scheme for an encrypted SPI system for the first time. The KPA is implemented by interchanging the roles of illumination patterns and object images in a SPI model. The secret illumination patterns can be recovered from a set of known plaintext images and ciphertext intensity sequences. The COA is implemented on the basis of statistical features in the distribution of single-pixel intensity values when the SPI is performed on the same category of images. The attacker can compare the statistical distributions of single-pixel intensity values generated from actual object images and values virtually generated from the collected exemplar images. The unknown illumination patterns can be recovered after being mapped to known original patterns. Simulation results verify the effectiveness of our proposed attacking schemes. The two schemes can crack encrypted SPI systems and successfully recover the key containing correct illumination patterns. Our proposed attacking schemes reveal security flaws of an encrypted SPI system under certain circumstances. In addition, our proposed attacking algorithms may be meaningful for other applications similar to the cryptoanalysis of an optical encryption system, such as scattering imaging.

ACKNOWLEDGMENT

(Shuming Jiao and Ting Lei contributed equally to this work.)

REFERENCES

[1] B. Javidi *et al.*, "Roadmap on optical security," *J. Opt.*, vol. 18, no. 8, Aug. 2016, Art. no. 083001.

[2] S. Liu, C. Guo, and J. T. Sheridan, "A review of optical image encryption techniques," *Opt. Laser Technol.*, vol. 57, pp. 327–342, Apr. 2014.

[3] S. Jiao, C. Zhou, Y. Shi, W. Zou, and X. Li, "Review on optical image hiding and watermarking techniques," *Opt. Laser Technol.*, vol. 109, pp. 370–380, Jan. 2019.

[4] P. Refregier and B. Javidi, "Optical image encryption based on input plane and Fourier plane random encoding," *Opt. Lett.*, vol. 20, no. 7, pp. 767–769, Apr. 1995.

[5] E. Tajahuerce and B. Javidi, "Encrypting three-dimensional information with digital holography," *Appl. Opt.*, vol. 39, no. 35, pp. 6595–6601, Dec. 2000.

[6] B. Javidi and T. Nomura, "Securing information by use of digital holography," *Opt. Lett.*, vol. 25, no. 1, pp. 28–30, Jan. 2000.

[7] X. Li, M. Zhao, Y. Xing, L. Li, S. T. Kim, X. Zhou, and Q. H. Wang, "Optical encryption via monospectral integral imaging," *Opt. Express*, vol. 25, no. 25, pp. 31516–31527, Dec. 2017.

[8] X. W. Li, S. J. Cho, and S. T. Kim, "High security and robust optical image encryption approach based on computer-generated integral imaging pickup and iterative back-projection techniques," *Opt. Laser. Eng.*, vol. 55, pp. 162–182, Apr. 2014.

[9] H. Li, C. Guo, I. Muniraj, B. C. Schroeder, J. T. Sheridan, and S. Jia, "Volumetric light-field encryption at the microscopic scale," *Sci. Rep.*, vol. 7, Jan. 2017, Art. no. 40113.

[10] Y. Shi, T. Li, Y. Wang, Q. Gao, S. Zhang, and H. Li, "Optical image encryption via ptychography," *Opt. Lett.*, vol. 38, no. 9, pp. 1425–1427, May 2013.

[11] A. Pan, K. Wen, and B. Yao, "Linear space-variant optical cryptosystem via Fourier ptychography," *Opt. Lett.*, vol. 44, no. 8, pp. 2032–2035, Apr. 2019.

[12] P. Clemente, V. Durán, V. Torres-Company, E. Tajahuerce, and J. Lancis, "Optical encryption based on computational ghost imaging," *Opt. Lett.*, vol. 35, no. 14, pp. 2391–2393, Jul. 2010.

[13] M. Tanha, R. Kheradmand, and S. Ahmadi-Kandjani, "Gray-scale and color optical encryption based on computational ghost imaging," *Appl. Phys. Lett.*, vol. 101, no. 10, Sep. 2012, Art. no. 101108.

[14] W. Chen and X. Chen, "Ghost imaging using labyrinth-like phase modulation patterns for high-efficiency and high-security optical encryption," *Europhys. Lett.*, vol. 109, no. 1, 2015, Art. no. 014001.

[15] Y. Qin and Y. Zhang, "Information encryption in ghost imaging with customized data container and XOR operation," *IEEE Photon. J.*, vol. 9, no. 2, Apr. 2017, Art. no. 7802208.

[16] Z. Pan and L. Zhang, "Optical cryptography-based temporal ghost imaging with chaotic laser," *IEEE Photon. Technol. Lett.*, vol. 29, no. 16, pp. 1289–1292, Aug. 15, 2017.

[17] K. Yi, Z. Leihong, and Z. Dawei, "Optical encryption based on ghost imaging and public key cryptography," *Opt. Laser. Eng.*, vol. 111, pp. 58–64, Dec. 2018.

[18] Z. Zhang, S. Jiao, M. Yao, X. Li, and J. Zhong, "Secured single-pixel broadcast imaging," *Opt. Express*, vol. 26, no. 11, pp. 14578–14591, May 2018.

[19] S. Jiang, Y. Wang, T. Long, X. Meng, X. Yang, R. Shu, and B. Sun, "Information security scheme based on computational temporal ghost imaging," *Sci. Rep.*, vol. 7, no. 1, Aug. 2017, Art. no. 7676.

[20] J. Wu, Z. Xie, Z. Liu, L. Wei, Z. Yan, and S. Liu, "Multiple-image encryption based on computational ghost imaging," *Opt. Commun.*, vol. 359, pp. 38–43, Jan. 2016.

[21] S. Jiao, C. Zhou, W. Zou, and X. Li, "Non-destructive ghost authentication for single-pixel imaging in mass user environment," *Laser Phys.*, vol. 28, no. 9, Sep. 2018, Art. no. 096203.

[22] M. P. Edgar, G. M. Gibson, and M. J. Padgett, "Principles and prospects for single-pixel imaging," *Nature Photon.*, vol. 13, pp. 13–20, Jan. 2019.

[23] M. J. Sun and J. M. Zhang, "Single-pixel imaging and its application in three-dimensional reconstruction: A brief review," *Sensors*, vol. 19, no. 3, p. 732, Feb. 2019.

[24] N. Radwell, K. J. Mitchell, G. M. Gibson, M. P. Edgar, R. Bowman, and M. J. Padgett, "Single-pixel infrared and visible microscope," *Optica*, vol. 1, no. 5, pp. 285–289, Nov. 2014.

[25] M. Li, D. Lu, W. Wen, H. Ren, and Y. Zhang, "Cryptanalyzing a color image encryption scheme based on hybrid hyper-chaotic system and cellular automata," *IEEE Access*, vol. 6, pp. 47102–47111, 2018.

[26] M. Li, H. J. Fan, Y. Xiang, Y. Li, and Y. Zhang, "Cryptanalysis and improvement of a chaotic image encryption by first-order time-delay system," *IEEE Multimedia*, vol. 25, no. 3, pp. 92–101, Sep. 2018.

[27] M. Li, D. D. Lu, Y. Xiang, Y. Zhang, and H. Ren, "Cryptanalysis and improvement in a chaotic image cipher using two-round permutation and diffusion," *Nonlinear Dyn.*, vol. 96, no. 1, pp. 31–47, Apr. 2019.

[28] L. Y. Zhang, Y. Liu, C. Wang, J. Zhou, Y. Zhang, and G. Chen, "Improved known-plaintext attack to permutation-only multimedia ciphers," *Inf. Sci.*, vol. 430, pp. 228–239, Nov. 2017.

[29] Y. Zhang, D. Xiao, W. Wen, and H. Nan, "Cryptanalysis of image scrambling based on chaotic sequences and Vigenère cipher," *Nonlinear Dyn.*, vol. 78, no. 1, pp. 235–240, Oct. 2014.

[30] G. Situ and J. Zhang, "Double random-phase encoding in the Fresnel domain," *Opt. Lett.*, vol. 29, no. 14, pp. 1584–1586, Jul. 2004.

[31] G. Unnikrishnan, J. Joseph, and K. Singh, "Optical encryption by double-random phase encoding in the fractional Fourier domain," *Opt. Lett.*, vol. 25, no. 12, pp. 887–889, Jun. 2000.

[32] E. Pérez-Cabré, H. C. Abril, M. S. Millán, and B. Javidi, "Photon-counting double-random-phase encoding for secure image verification and retrieval," *J. Opt.*, vol. 14, no. 9, Sep. 2012, Art. no. 094001.

[33] S. Jiao, Z. Zhuang, C. Zhou, W. Zou, and X. Li, "Security enhancement of double random phase encryption with a hidden key against ciphertext only attack," *Opt. Commun.*, vol. 418, pp. 106–114, Jul. 2018.

[34] J. Chen, Y. Zhang, J. Li, and L.-B. Zhang, "Security enhancement of double random phase encoding using rear-mounted phase masking," *Opt. Laser. Eng.*, vol. 101, pp. 51–59, Feb. 2018.

[35] U. Gopinathan, D. S. Monaghan, T. J. Naughton, and J. T. Sheridan, "A known-plaintext heuristic attack on the Fourier plane encryption algorithm," *Opt. Express*, vol. 14, no. 8, pp. 3181–3186, Apr. 2006.

[36] X. Peng, H. Wei, and P. Zhang, "Chosen-plaintext attack on lensless double-random phase encoding in the Fresnel domain," *Opt. Lett.*, vol. 31, no. 22, pp. 3261–3263, Nov. 2006.

[37] Y. Frauel, A. Castro, T. J. Naughton, and B. Javidi, "Resistance of the double random phase encryption against various attacks," *Opt. Express*, vol. 15, no. 16, pp. 10253–10265, Aug. 2007.

[38] C. Guo, S. Liu, and J. T. Sheridan, "Iterative phase retrieval algorithms. Part II: Attacking optical encryption systems," *Appl. Opt.*, vol. 54, pp. 4709–4718, May 2015.

[39] X. Liu, J. Wu, W. He, M. Liao, C. Zhang, and X. Peng, "Vulnerability to ciphertext-only attack of optical encryption scheme based on double random phase encoding," *Opt. Express*, vol. 23, pp. 18955–18968, Jul. 2015.

[40] G. Li, W. Yang, D. Li, and G. Situ, "Cyphertext-only attack on the double random-phase encryption: Experimental demonstration," *Opt. Express*, vol. 25, pp. 8690–8697, Apr. 2017.

[41] S. Jiao, G. Li, C. Zhou, W. Zou, and X. Li, "Special ciphertext-only attack to double random phase encryption by plaintext shifting with speckle correlation," *J. Opt. Soc. Amer. A, Opt. Image Sci.*, vol. 35, pp. A1–A6, Jan. 2018.

[42] S. Yuan, J. Yao, X. Liu, X. Zhou, and Z. Li, "Cryptanalysis and security enhancement of optical cryptography based on computational ghost imaging," *Opt. Commun.*, vol. 365, pp. 180–185, Apr. 2016.

[43] L. H. Bian, J. L. Suo, Q. H. Dai, and F. Chen, "Experimental comparison of single-pixel imaging algorithms," *J. Opt. Soc. Amer. A, Opt. Image Sci.*, vol. 35, no. 1, pp. 78–87, Jan. 2018.

[44] Z. Zhang, X. Wang, G. Zheng, and J. Zhong, "Hadamard single-pixel imaging versus Fourier single-pixel imaging," *Opt. Express*, vol. 25, no. 16, pp. 19619–19639, 2017.

[45] Z. Zhang, X. Wang, G. Zheng, and J. Zhong, "Fast Fourier single-pixel imaging via binary illumination," *Sci. Rep.*, vol. 7, no. 1, Sep. 2017, Art. no. 12029.

[46] J. Suo, L. Bian, F. Chen, and Q. Dai, "Signal-dependent noise removal for color videos using temporal and cross-channel priors," *J. Vis. Commun. Image Represent.*, vol. 36, pp. 130–141, Apr. 2016.

[47] M. R. Hestenes and E. Stiefel, "Methods of conjugate gradients for solving linear systems," *J. Res. Nat. Bureau Standards*, vol. 49, no. 6, pp. 409–436, Dec. 1952.

[48] Z. Zhang, Y. Song, and H. Qi, "Age progression/regression by conditional adversarial autoencoder," in *Proc. IEEE Conf. Comput. Vis. Pattern Recognit.*, Jul. 2017, pp. 5810–5818.

[49] Y. LeCun, L. Bottou, Y. Bengio, and P. Haffner, "Gradient-based learning applied to document recognition," *Proc. IEEE*, vol. 86, no. 11, pp. 2278–2324, Nov. 1998.

SHUMING JIAO received the Ph.D. degree in electronic engineering from the City University of Hong Kong, in 2016. He is currently a Research Fellow with the Nanophotonics Research Center, Shenzhen University, China. His research interests include digital holography, single-pixel imaging, optical security, image processing, and machine learning.

TING LEI received the Ph.D. degree from the Hong Kong University of Science and Technology, in 2013. He is currently an Associate Professor with the Nanophotonics Research Center, Shenzhen University, China.

YANG GAO received the bachelor's degree in measurement technology and instrumentation from Lanzhou Jiaotong University, China, in 2017. He is currently pursuing the master's degree with the Nanophotonics Research Center, Shenzhen University, China.

ZHENWEI XIE received the Ph.D. degree from the Harbin Institute of Technology, China, in 2015. He is currently an Assistant Professor with the Nanophotonics Research Center, Shenzhen University, China.

XIAOCONG YUAN received the Ph.D. degree from the King's College London, U.K., in 1994. He was a Faculty with Nankai University, China, from 2008 to 2013, and Nanyang Technological University, Singapore, from 1999 to 2010. He has been a Professor and the Director of Nanophotonics Research Center, Shenzhen University, China, since 2013. He is a Fellow of OSA, SPIE, InstP, and COS.