Optical image encryption via photon-counting imaging and compressive sensing based ptychography

To cite this article: Nitin Rawat et al 2015 J. Opt. 17 065704

View the article online for updates and enhancements.

Related content
- Roadmap on optical security
  Bahram Javidi, Artur Carnicer, Masahiro Yamaguchi et al.
- Securing information using optically generated biometric keys
  Gaurav Verma and Aloka Sinha
- Optical multiple-image authentication scheme based on the phase retrieval algorithm in gyrator domain
  Liansheng Sui, Xiao Zhang and Ailing Tian

Recent citations
- Encryption method based on pseudo random spatial light modulation for single-fibre data transmission
  Marcin Kowalski and Marek Zyczkowski
- Joint encryption and compression of 3D images based on tensor compressive sensing with non-autonomous 3D chaotic system
  Qingzhu Wang et al
- Optical image hiding based on dual-channel simultaneous phase-shifting interferometry and compressive sensing
  Jiaosheng Li et al
Optical image encryption via photon-counting imaging and compressive sensing based ptychography

Nitin Rawat¹, In-Chul Hwang², Yishi Shi³,⁴ and Byung-Geun Lee¹

¹School of Mechatronics, Gwangju Institute of Science and Technology, Gwangju 500-712, Korea
²Department of Electrical & Electronics Engineering, Kangwon National University, Chuncheon, Korea
³College of Material Science and Opto-Electronic Technology, University of Chinese Academy of Sciences, Beijing 100049, People’s Republic of China
⁴State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, People’s Republic of China

E-mail: bglee@gist.ac.kr

Received 5 February 2015, revised 22 April 2015
Accepted for publication 23 April 2015
Published 27 May 2015

Abstract

In this study, we investigate the integration of compressive sensing (CS) and photon-counting imaging (PCI) techniques with a ptychography-based optical image encryption system. Primarily, the plaintext real-valued image is optically encrypted and recorded via a classical ptychography technique. Further, the sparse-based representations of the original encrypted complex data can be produced by combining CS and PCI techniques with the primary encrypted image. Such a combination takes an advantage of reduced encrypted samples (i.e., linearly projected random compressive complex samples and photon-counted complex samples) that can be exploited to realize optical decryption, which inherently serves as a secret key (i.e., independent to encryption phase keys) and makes an intruder attack futile. In addition to this, recording fewer encrypted samples provides a substantial bandwidth reduction in online transmission. We demonstrate that the fewer sparse-based complex samples have adequate information to realize decryption. To the best of our knowledge, this is the first report on integrating CS and PCI with conventional ptychography-based optical image encryption.

Keywords: optical security and encryption, photon-counting imaging, coherence imaging, compressive sensing

1. Introduction

In the past two decades, information security has become an essential research subject where optical encryption techniques have substantiated their predominant role [1–3]. One of the most extensively analyzed, as well as robust, encryption algorithms is double random phase encryption (DRPE) [4]. This system encodes an image into stationary white noise by adopting two random phase masks in spatial and Fourier domains, respectively. This phenomenal approach further gave an extension for encrypting information in other transformation domains such as fractional Fourier domain (FrFT) [5–8], Fresnel domain (FST) [9, 10], and gyrator domain [11, 12]. Similarly, many extensions have been introduced in the DRPE scheme; for instance, DRPE has been implemented in the joint transform correlate architecture [13]. Further, it is well known that FrFT and FST are special cases of the classical linear canonical transform (LCT); thus, the use of the LCT has also been proposed for the optical encryption techniques using quadratic phase systems (QPS) [14]. In addition to these studies, owing to the greater security of conventional DRPE, recently, other approaches that were originally regarded for coherent imaging were also proposed for optical encryption systems [15, 16, 18–20]. Among them, one of the
emerging techniques, ptychography, has gained much attention in optical encryption where amplitude and phase information can be imaged with an unlimited size and better quality [17–24]. A movable aperture is used to scan the object in ptychography and further reconstructs it by a series of recorded diffractive patterns. The object beam is enlightened by multiple probes, thus it generates multiple diffraction patterns in the far field region. By utilizing all these probes, the original information of the complex-valued specimen can be retrieved [24]. The aperture movement enlightens the object and overlaps with its neighbors. Thus, ptychography not only simplifies the architecture of the classical encryption system, but also enhances its security by enlarging the key space. The cipher texts are generated through series of probes and decryption can be retrieved through a phase retrieval algorithm [20].

On the other hand, in practice, the encryption algorithms can also be realized and implemented in digital forms. In such scenarios, the conventional optical encryption system has shown to be vulnerable to some formulated attacks [25–31]. To alleviate the aforementioned problem, recently, we have proposed a robust approach that is based on CS framework [32]. By using this approach, only a few random measurements of the encrypted complex samples will be retrieved, while all other samples would be discarded to achieve decryption. Nevertheless, a proper reconstruction algorithm is exploited to reconstruct the original samples with small or zero errors [33, 34]. Therefore, combining CS with an optical image encryption system would effectively reduce the data rate while not compromising either higher security or better image quality; thus, such an approach could be widely utilized in applications of optics. In recent years, CS-based encryption techniques have been widely proposed and analyzed [35–37], to cite a few.

In a different context, low light level illumination using the PCI technique introduces a paradigm shift in many fields, as the capturing PCI is highly a nonlinear process [35–44]. In particular, the photon-limited version of the encrypted complex distribution (i.e., a sparse representation of the complex data) has been recorded in order to achieve an additional layer security to the conventional DRPE [39, 42]. Recently, one of our coauthors has demonstrated such an integration of PCI with classical encryption systems for multispectral-image-based scenes [40, 43]. It is worth mentioning the fact that both CS and PCI possess some greater properties, such as higher security and online bandwidth reduction. Further, from all the background studies that we have done, there have been no reports claimed on combining CS and PCI with a conventional ptychography-based encryption system. Therefore, in this paper, we specifically examine the advantages of combining both the CS and PCI with a conventional ptychography-based encryption system to achieve an additional layer of security. Our encryption system is optically implemented, whereas the decryption procedure is carried out by virtual optics.

This paper is organized as follows: section 2 briefly reviews the classical ptychography-based DRPE. The proposed encryption method is explained in section 3. To validate our proposed technique, numerous experiments as well as a series of simulations were carried out in section 4. Further, the security analyses are discussed in section 5 and finally we conclude our discussions in section 6.

2. Ptychography using DRPE

The baseline method considered here is the ptychography-based DRPE [4]. As illustrated in figure 1, an optical 4f-based encryption system via the ptychography technique is presented. As it can been seen, the whole system is being illuminated with four different probes via a collimated, linearly polarized laser beam. The first probe \( P_1 \) covering the upright portion of the secret image \( f(x) \) passes through the optical domain that is attached with a random phase mask \( M_1 \) represented as \( \exp[iM_1] \). Subsequently, the synthesized diffraction pattern transverses through a Fourier lens that is kept at the focal length \( f \) and further multiplied with the second random phase mask \( M_2 \), given as \( \exp[iM_2] \). Finally, the encrypted image can be recorded after passing by another Fourier lens. Thus, all the applied probes from \( P_1 \) to \( P_4 \) are partially overlapped and create a complex intensity pattern IN (i.e., cipher text) eventually; the final encryption process is numerically expressed as follows:

\[
IN = \left| \text{FT} \left\{ \text{FT} \left\{ P_1 \cdot f(x) \exp[iM_1] \cdot \exp[iM_2] \right\} \right\} \right|^2 \tag{1}
\]

where FT is the Fourier transform and \( P_4 \) stands for the probe that enlightens the secret image, respectively. It can be noticed from equation (1) that the security of an encrypted image \( \text{IN}(x, y) \) depends not only on the random phase masks \( (M1, M2) \) but also on the intensity of multiple probes.

The decryption procedure can be carried out with the proper cipher text and the correct phase keys. The plaintext can be extracted through an iterative algorithm [20]. First, the intensity is acquired after guessing the complex value of the secret image \( f(x) \). For the \( k \)th iteration, \( f(x) \) is illuminated by...
the \(i\)th probe, which is modulated with \(M1\) and \(M2\) in the input and Fourier planes; the intensity is acquired as:

\[
IN = \left| \text{FT} \left\{ P \cdot f \exp [i M1] \right\} \cdot \exp [i M2] \right|^2
\] (2)

By substituting the amplitude term of \(IN^I_i(x, y)\) with the detected intensity \(IN_m(x, y)\), while preserving the phase:

\[
IN^I_i = \left| \text{IN}_m \right|^2 \cdot |\text{IN} / |\text{IN}| |
\] (3)

Now, the inverse Fourier transform of \(IN^I_i(x, y)\) has been taken to the Fourier plane. Divide it by \(M2\), further with inverse Fourier transform, and then divide by \(M1\):

\[
f_i^k = \text{FT}^{-1} \left\{ \text{FT}^{-1} \text{IN}^I_i \cdot \exp [-i M2] \right\} \cdot \exp [-i M1]
\] (4)

Further, renewing the \(f_i^k (x, y)\) with \(f_i^k + f_{i+1}^k (x, y)\)

\[
f_i^{(l+1)} = f_i^k + \beta \left( \frac{f_i^k + f_i^{k+1} P}{P + \alpha} \right)
\] (5)

where \(\alpha\) and \(\beta\) are the adjustment factors. The preceding process is carried for all the probes, simultaneously. The decryption process can be recovered digitally by using ptychographic iterative reconstruction [20]. The decryption process follows equations (2)–(5) until it reaches the correlation coefficient between the retrieved image and the secret image

\[
C(f, f') = \text{cov}(f, f') \left( \sigma_f, \sigma_{f'} \right)^{-1}
\] (6)

Where \(f\) and \(f'\) stand for the retrieved image and the original counterpart, respectively. \(C(f, f')\) is the cross covariance between \(f\) and \(f'\), and \(\sigma_f\) is the standard deviation. The value of \(C_o\) varies in \([0, 1]\) and gives the best decryption when it reaches 1.

3. Sparse-based optical image reconstruction

Sparse-based encryption approaches have proven to provide more robust, feasible, and effective results [34–43]. As mentioned previously, in this study, we specifically focus on combining two classical approaches, i.e., CS and PCI techniques, with a conventional ptychography-based encryption system. The detailed description, as well as a feasible optical setup for each combination, is presented in this section.

3.1. CS

To sample a signal or an image, conventional approaches follow Shannon’s theorem (also known as Nyquist rate), which states that the sampling rate must be at least twice the maximum frequency present in the signal [31, 32]. Recently, a new sampling paradigm also known as CS combines the sampling and compression into a single non-adaptive linear measurement process [31]. The theory of CS suggests that most of the natural images are sparse in certain basis and have adequate information in order to reconstruct the original image perfectly with small or zero errors [30]. Sparsity determines how efficiently one can acquire signals non-adaptively. For brevity, we assume an image \(f\) can be organized into a vector form in the lexicographical order \(f \in \mathbb{R}^{N^2}\) and can be written mathematically by the relation [31]

\[
y = Hf + e = \Phi f
\] (7)

where \(y\) is the collection of having \(M \times 1\) measurements, \(H\) is the \(M \times N\) measurement matrix, \(f\) is considered as the image to be compressed, \(e\) is the noise vector, and \(\Phi\) is the measurement matrix. The image \(f\) is said to be \(K\)-sparse if only \(K\) of the \(f\) coefficients in equation (7) are non-zeros, while the remaining \((N-K)\) coefficients are zeros. For the optimum recovery of an image, there are certain conditions to guarantee the signal recovery; one is the transform sparsity, which means that the image vector \(f\) is \(K\)-sparse or can be sparsified in some basis such as wavelet transform. It has been demonstrated that we can use \(K\)-sparse vectors and closely approximate compressible vectors by using just \(M \geq O(K \log(n))\) random measurements. The other criteria are the sensing operator \(\Phi \in \mathbb{R}^{M \times N}\) and the sparse representation operator satisfying the restricted isometry property (RIP) [31]. Such system is said to be underdetermined because the number of measurements \(M\) is lower than the number of \(N\) of an image. Further, the reconstruction is recovered by solving the optimization problem [32].

\[
\min \| \alpha \|, \text{ such that } y = \Phi \Phi \alpha,
\] (8)

where \(\| \alpha \| = \sum |\alpha_i|\) is the \(l_1\) norm, which measures the non-zero entries of the vector \(\alpha\).

In our study, the synthesized encrypted image is carried out with CS framework by random sampling. The sparse distributed version of the encrypted image is \(\text{IN}(x, y)\), retrieved by collecting only few linearly projected random encrypted samples. For decryption, the image is recovered by solving the optimization problem [32]. In order to recover the original signal from sparse encrypted samples, we have used the \(l_1\)–magic, which solves the standard basis pursuit problem using a primal-dual algorithm that can be performed by employing \(l_1\) norm optimization algorithms [30].

The schematic diagram of the experimental apparatus is explained in figure 2. The linearly polarized plane wave fronts are passed through a beam spatial filter that includes a pinhole for spatial filtering. The light beam is further divided into two beams by a beam splitter (BS) and reflected light wave from a mirror (\(M_1\)) strikes the object (O) and creates the complex diffraction pattern (i.e., encrypted data) after transverse through two identical Fourier lenses and two random phase masks (RPM1, RPM2), respectively. One of the arms is reflected through a mirror (\(M_2\)) and combines with a synthesized encrypted beam at BS2, creating an interference pattern \(\text{IN}_D(x, y)\). The ptychography probes scanning are carried out on an object that is placed on a motorized translation stage. Further, the corresponding combined pattern is reflected off by a digital micro-mirror device (DMD) which consists of an array of \(N\) tiny mirrors. An SLM can also be used for image generation. Due to ptychography probe scanning, the object is fully covered as the probe moves and combined to scan being overlapped with each other. Each
mirror in DMD independently oriented either towards the third lens (L3) or away from it. Thus, the reflected light is collected through the L3 and focused onto a single-pixel detector (PD). Finally, the random samples can be recorded. Analogously, the operation can also be implemented computationally and the samples can retrieve digitally [30]. For the practical implementation of CS acquisition in ptychography, it is important to determine the coherent basis where the Hadamard matrix can be interpreted as a rectangular wave (Walsh functions). The experimental process can be carried out through digital holography. Once the number of measurements are collected, the CS reconstruction of the original signal can be recovered by solving the optimization problem. It is worth mentioning that combining CS with the classical ptychography-based encryption system seems to be highly secure, because the ptychography probes and random masks act as the secret keys for the encryption system but also because the measurement matrix used in the CS approach makes the intruder attacks pointless. In general, the transformation from $I_N$ to $(IN)_y$ is a dimensionality reduction problem, thus it inevitably loses some primary information. Nevertheless, the sensing matrix $\Phi$ can be designed in such a way that would reproduce the original information exactly from the reduced measurements [32].

### 3.2. PCI

PCI-based studies have gained much attention, as they show a predominant role in estimating the irradiance from the photon counts [35–40]. Recently, we also have shown that the PCI technique can be embedded with the conventional encryption process where only a limited number of photons $N_p$ are recorded from the entire scene (i.e., sparse encrypted samples) to achieve an additional layer security and authentication results. The system was specifically designed to capture a multispectral scene in which a limited number of photons that strike the image sensors are being reserved after encryption [40]. In general, a statistical model of a photon-counting detector is assumed to follow a Poisson distribution [43].

$$P_d(l_j, \phi_j) = \frac{[\phi_j]^{l_j} e^{-\phi_j}}{l_j!}, \quad l_j = 0, 1, 2, \ldots, \quad (9)$$

where $l_j$ is the number of photons detected at pixels $j$ and the Poisson parameter $\phi_j$, given by $\phi_j = N_p x_j$, with normalized irradiance $x_j$ at pixels $j$, respectively. In case of ptychography image encryption, the encrypted image $IN_i(x)$ can be represented in a photon-limited version, denoted by $P_E(x)$ as

$$\lambda_E(x) = \frac{IN_i(x)}{\sum_{j=1}^{N_p} IN_j(x)} \quad (10)$$

where $N_p$ is the expected number of photons in the image, $N_i$ is the total number of pixels in the image, and $P_E(x)$ is the number of photons at pixel $x$, respectively.

In our study, the PCI approach is applied to the amplitude distribution of original encryption data $IN_i(x)$. The pixels receiving at least one photon are considered in the decrypted process with respective phase values. As a consequence, a noisy distributed image is retrieved, which cannot be recognized by direct visual inspection. Nevertheless, for image verification, the retrieved image is compared with the original image, considered as a reference by nonlinear correlation [43, 45]. Overall, the system creates a sparse white noise data that make the intruder attacks futile and reduce the bandwidth needed for data transmission.

In Figure 3, the process is similar but there is a PCI-based technique instead. The experimental process can be carried out through digital holography. One of the arms is reflected through a mirror (M2) and combines with a synthesized encrypted beam at BS2, creating an interference pattern $IN_E(x, y)$. Furthermore, the numbers of photons are controlled in the entire scene through the PCI-based approach. Once we get the encrypted image, verification is possible through nonlinear correlation.
Figure 3. Proposed model for photon-counting ptychography imaging encryption, (BSF: Beam spatial filter, O: Object (SLM), RPM1, RPM2: Random phase masks, L1, L2: Optical lens, PCI: Photon-counting imaging detector.

Figure 4. (a) Primary amplitude image, (b) full encryption image, (c) encrypted random measurements (20%), and (d) decryption image using CS reconstruction algorithm.
4. Numerical results

In order to investigate the effect of our proposed encryption-based method, we have completed our simulations using ‘virtual optics’. The sparse-based secured image reconstruction is carried out through MATLAB (R2013a), which is executed on a 32-bit window 7 OS that includes an i5-3470k processor of 3.2 GHz. The experimental arrangement is shown in figures 2 and 3, where a He-Ne laser (632.8 nm) of 15 mW is used as the coherent light source. A linearly polarized incident beam is separated by a non-polarized BS into two directions; one goes to the object and the other to the reference arm. In the object arm side, an expanded beam of light is incident on an SLM (Jenoptik), which is placed to generate a diffraction pattern of size 512 × 512 [figure 4(a)]. The encrypted image is captured by the CCD after passing through two phase masks, and finally CS and PCI techniques are carried out digitally.

The image to be encrypted is shown in figure 4(a). The complex diffraction pattern at the output plane is shown in figure 4(b), which shows no clue of the actual image. Finally, a random sampling is carried out using a CS framework, where only 20% of the measurement (figure 4(c)) is taken and the rest is thrown away to get the sparse encrypted image. Figure 4(d) shows the decryption process, which is carried out through l1−magic by only using a few random sporadic samples. The CS reconstructed image has a reasonable quality with a peak-signal-to-noise ratio (PSNR) value of 29.413 dB.

We have shown the PCI-based ptychography encryption results in figure 5. The photon-counted encrypted image is shown in figure 5(a). Further, the decryption is shown in figure 5(b), which is noisy and cannot be visually recognized with a limited number of photons. The decryption process can be recovered digitally by ptychography iterative reconstruction. The decryption process remains the same as in equations (2)–(4) until it reach the correlation coefficient between the retrieved image and the secret image is calculated (see figure 6). The value of Co varies in [0, 1] and the simulation is carried out 50 times to get the best decryption result.

5. Security analysis

In this section, we analyze the robustness of the proposed encryption-based technique. We carried out some standard analysis such as nonlinear correlation (NC) and PSNR to support our results.

5.1. NC for PCI-based encryption

Since the photon-limited decrypted image hardly reveals the information of the original image, the nonlinear cross correlation between the original image and the decrypted image is used for the image authentication. Thus we calculated the NC. The images to be compared are Fourier transformed, nonlinearly modified, and multiplied in the frequency domain. Further, an inverse Fourier transformation yields results.
where $D(\mu, \eta)$ and $F(\mu, \eta)$ are 2D transforms of the decrypted and reference images, $\phi_F(\mu, \eta)$ and $k$ is the strength of the applied nonlinearity. We estimated the best-suited value for $k$ is 0.3 from our previous experiments [40].

Figure 7 shows that when the two images are similar, the correlation (0.94) exhibits a sharp intense peak [figure 7(b)]. When different images are used, the correlations exhibit a random pattern with no peak value (0.06) for different images [figure 7(c)]. Therefore, the original image should be used to authenticate the information.

5.2. PSNR graph for CS-based encryption

In this study, PSNR [46] analyses have done in figure 8, using the CS approach, to check the minimum amount of data required for the extraction of reasonable information. Approximately 20% of the information data is required to extract a PSNR value of 25.104 dB. Figure 8 shows the PSNR against different sampling levels,

$$PSNR = 10 \log_{10} \left( \frac{\hat{\epsilon}^2}{MSE} \right)$$

Figure 7. (a) NC. (a) Original decryption image, (b) correlation result of proper decryption (0.94), and (c) improper decryption using conventional ptychography (0.06).

Figure 8. PSNR using CS approach. (a) PSNR values of CS using approx. 20% of the measurements.
where $f_{\text{max}}$ is the maximum possible pixel value of the primary image and $MSE$ is computed mean squared error between the decrypted and original image. The information contained in the encrypted complex-image can be significantly compressed by discarding redundant pixels while retaining only the few appropriate sporadic encrypted samples up to 20% and the decryption process benefits from the reconstructed encrypted image.

5.3. Robustness to information occlusion and noise attack

In this section, we have tested the effect of information occlusion and noise attack. Figure 9 shows the retrieved images after some amount of encrypted pixels have been occluded for the decryption process. In the case of the CS-based information approach, the retrieved images are attacked by cropping the pixels. The more the pixels are occluded, the
more the information degrades, whereas in the case of the PCI-based approach, the decrypted image is intended not for direct visualization of the original image, but for verification of the information. It is impossible to extract the information in decryption as well as in the pixel occlusion stage.

Figure 10 shows the reconstruction analysis of the encrypted image using various noise types and conditions. A Gaussian white noise of mean 0 and variance 0.1 is added to the encryption result (figure 10(a)), where the PSNR of the corresponding result is 24.0421 dB. The encrypted image is exposed to salt and pepper (figures 10(b), (c)) by changing the density parameter, where the PSNR are 22.251 dB and 21.206 dB.

5.4. Robustness against various attacks

In this section, we discuss the feasibility and effectiveness of the proposed approach to organized attacks such as chosen-plaintext attacks (CPA) [24] and known-plaintext attacks (KPA) [25]. For these attacks, we presumed that intruders have some prior knowledge of the random sensing matrix, one of the ptychography probes that without which the attacks would be futile, as explained. In CPA, it’s assumed that the attacker has the ability to trick an authorized user and is able to retrieve the secured information by obtaining the cipher text corresponding to a Dirac delta function (i.e., impulse) as chosen plaintext. Figure 11 shows the retrieved images and the measured cross correlation values.

Similarly, in KPA, a cryptanalyst is assumed to have access to an original plaintext and the corresponding cipher text. Based on prior knowledge, attackers can retrieve any secured information through some classical phase retrieval algorithms. Figure 12 shows the retrieved images after several iterations (i.e., 300 iterations) of the Gerchberg–Saxton algorithm.

In summation, we could conclude by quoting that the proposed approach is immune to all these attacks because the decryption process depends not only on the probe keys and
number of photons, but also on the sensing matrix. Therefore, integrating CS and PCI with the conventional ptychography cryptographic systems could definitely enhance the security and provide the benefit of nullifying the bandwidth limitations.

6. Conclusion

In this study, we have investigated an approach integrated with PCI-based encryption and CS-based encryption for a conventional ptychography-based encryption system. The object is optically encrypted and recorded via a classical ptychography technique. Further, we have combined CS and PCI techniques with the primary encrypted image to get the minimum amount of information required for encryption. Such integration shows a number of advantages over the conventional ptychography encryption system. We show that only $10^7$ photons (less than 4% of image size) are sufficient in the case of the PCI encryption process and at maximum 20% of the random complex measurements are required in the case of the CS-based encryption system. Experimental results support that both approaches are more robust and feasible while enhancing the security of the system. In summary, the proposed system can totally remove the data reduction problem that exists in the previous image encryption techniques.

Acknowledgments

This work was supported by the Space Core Technology Development Program funded by the Ministry of Science, ICT, and Future Planning and the Center for Integrated Smart Sensors funded by the Ministry of Science, ICT, and Future Planning as Global Frontier Project CISS-2011-0031868.

References

[19] Hoppe W 1982 Trace structure analysis, psychotherapy, phase tomography Ultramicroscopy 10 187
[37] Lu P, Xu Z, Lu X and Liu X 2013 Digital image information encryption based on compressive sensing and double random-phase encoding technique Optik 124 2514–18