Augmenting data security: Physical Unclonable Functions for digital holography based quadratic phase cryptography

Patnala Vanitha
SRM University-AP
Bhargavi Manupati
SRM University-AP
Inbarasan Muniraj
SRM University-AP
Satish Anamalamudi
SRM University-AP
Salla Gangi Reddy (gangireddy.s@srmap.edu.in)
SRM University-AP
R. P. Singh

Research Article

Keywords: Optical Encryption, Linear Canonical Transform, Perfect Optical vortices, Physical Unclonable Functions

Posted Date: April 5th, 2022

DOI: https://doi.org/10.21203/rs.3.rs-1509081/v1

Augmenting data security: Physical Unclonable Functions for digital holography based quadratic phase cryptography.

Patnala Vanitha[1], Bhargavi Manupati[1], Inbarasan Muniraj[1], Satish Anamalamudi[1], Salla Gangi Reddy[1*], and R. P. Singh[2]

[1]School of Engineering and Applied Sciences, SRM University-AP, Neerukonda, Andhra Pradesh 522240, India.

[2]Physical Research Laboratory, Navarangpura, Ahmedabad, India-380009.

Abstract

In (Appl. Opt. 55, 4720-4728 (2016)) authors demonstrated the vulnerability of Linear Canonical Transform (LCT) based optical encryption system. One of the primary reasons for this is the predictable nature of the security keys (i.e., simulated random keys) used in the encryption process. To alleviate, in this work, we are presenting a Physically Unclonable Function (PUF) for producing a robust encryption key for the digital implementations of any optical encoding systems. We note, a correlation function of the scattered perfect optical vortex (POV) beam is utilized to generate the encryption keys. To the best of our knowledge, this is the first report on properly utilizing a scattered POV for the optical encryption systems. To validate the generated secret keys, the standard Linear Canonical Transform based Double Random Phase Encoding (LCT-DRPE) technique is used. Experimental and simulation result validates the proposed key generation method as an effective alternative to the digital encryption keys.

Keywords: Optical Encryption; Linear Canonical Transform; Perfect Optical vortices, Physical Unclonable Functions.

1. Introduction

Ever-increasing demand for the Internet of Things (IoT) devices mandate the voluminous data transfer over the communication channels. In this context, securing private data i.e.,

authenticating the users to access the sensitive (personal) information, becomes necessary. Several mathematics-based security approaches (i.e., cryptography) have been demonstrated in the literature to secure the systems and networks from malicious attacks. Henceforth, the cryptographic algorithms play a vital role in digitized and datafied era. In general, information that needs to be sent from a sender end is encrypted (i.e., input data is converted into an unreadable format) using secret keys. At the receiver end, by appropriately using the keys, encoded information can be retrieved (without loss) and this process is known as decryption. It is known that, depends on the cryptographic algorithm used, the keys for both the encryption and decryption process can be same or different [1, 2]. Owing to this capability, cryptographic algorithms are widely used in various fields, such as banking, healthcare, social media, emails, and military communication, to name a few. In general, cryptographic algorithms are designed to withstand cyberattacks. However, the recent advancements in high-performance computers made the cryptographic methods more vulnerable [2]. Several investigations have been carried out in the literature to augment the digital cryptography systems. For instance, to improvise the security, Frank Miller introduced the One Time Pad (OTP) technique which basically uses a perfect random key to ensure the security [3].

In a different context, Optical Signal Processing (OSP) based encryption methods shown to be offering a great deal of security with lower computational complexity when compared to the digital encryption approaches e.g., Advanced Encryption Standard (AES), Data Encryption Standard (DES), and Rivest-Shamir-Adleman (RSA) [4]. In this context, Double Random Phase Encoding (DRPE) [5] is one of the widely used optical information security methods that demonstrates remarkable advantages, such as extended degrees of freedom, system flexibility, multi-dimensional capabilities, and high encryption density [6]. In addition to these, DRPE encrypts both the real and phase information independently and also shown to encrypting information based on amplitude, polarization, and wavelength etc [7]. Since it's initial inception, DRPE i.e., Fourier transform based encryption, several other variations have also been examined that includes Fresnel transform (FST) [8], Fractional Fourier transform (FrFT) [9], Hartley Transform (HT) [10], and Linear Canonical Transform (LCT) [11]. In addition to these, some new types of encryption systems have also been demonstrated such as compressive sensing-based encryption [12], 4D light field based microscopic encryption [13], and photons-counting imaging based optical encryption [14], to cite a few. In general, it is known that the robustness of

a crypto system relies on the secret key that is being used and the randomness of ciphertext it generates. Thus, the linearity of DRPE mechanism have been exploited to show the vulnerability of LCT based DRPE scheme against chosen-plaintext and known-plaintext attacks [15].

To prevent from these attacks, a physical one-way function has been introduced in cryptographic systems which can be (physically) realized using the scattering of light beams [16]. Such functions have two distinct properties (i) they are impossible to duplicate (due to the unique manufacturing process of materials such as silicon chip or ground glass) and (ii) has no compact mathematical representation. Owing to these intrinsic characteristics, this approach was shown to be a robust alternate to the standard cryptosystems [17, 18]. These functions are, in general, known as Physical Unclonable Functions (PUFs) and can be embedded into any optical systems for data authentication as this involves a scattering of light beams which results in a highly complex and random output i.e., speckles [19]. It is known that the distribution and size of speckle is very sensitive to the input laser parameters such as beam width, angle of incidence as well as on the scattering surface and thus it can act as optical PUFs [20, 21, 23]. Some of the advantages of PUF includes (i) low cost, (ii) high output complexity, (iii) difficult to replicate, and (iv) high security against attacks [19]. Despite all these benefits, the proper demonstration of PUFs, to the best of authors knowledge, has not yet been done. Therefore, in this work, for the first time, we demonstrate an encryption system (i.e., LCT based DRPE) using PUFs that generated by taking a correlation function between two speckle patterns obtained after scattering the POV beams through a ground glass plate.

Rest of this paper is organized as follows: Section 2 describes the methodology used to generate the proposed encryption key and the basics of LCT-DRPE scheme is given in Section 3. We discussed the experimental and simulation results in Section 4. Finally, Section 5 concludes the paper.

2. Generation of encryption keys

In this work, as aforementioned, the encrypted keys are generated using a correlation function obtained from two scattered POV light beams i.e., speckles. The experimental set up for generating POV beams, and the corresponding speckle patterns is shown in Fig. 1

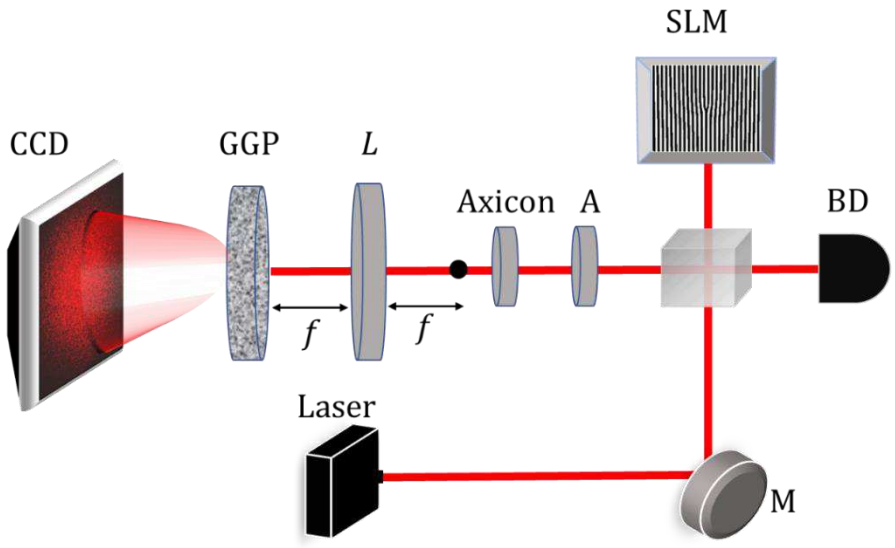

Figure 1. *(Color online) Experimental setup for the generation of perfect optical vortex (POV) beams and the corresponding speckle patterns. Here, M-Mirror; BD-Beam Dumper; BS-Beam Splitter; SLM-Spatial Light Modulator; A-Aperture; L-Lens and f-focal length of L. A black dot at the back focal plane of Axicon represents the formation of Bessel-Gaussian beam.*

A He-Ne laser having a wavelength of $632\ nm$ has been used to generate the vortex beam by combining the illuminated light field with a computer-generated hologram, which is displayed on spatial light modulator (SLM), via a beam splitter (BS). This combined light beam is then propagated through an Axicon of apex angle $178°$ to convert optical vortex beams to Bessel-Gaussian (BG) beam. To note, the formation of BG beams happens at $12.5\ cm$ from axicon (shown as a black colour dot in the optical path in Fig. 1) but that BG beam further travels to $60\ cm$ (focal length of the lens) to reach the Fourier lens (L). POV beam is generated at the back focal plane where we have placed a ground glass plate (GGP) to scatter the POV beam. Thus, the speckle images are produced and recorded using a charged-coupled device. To note, after recording the speckle patterns, we have determined the correlation function in MATLAB

and the same is used as encrypted keys in the LCT based DRPE scheme which is described in the Section 3. The field distribution of a POV beam with a thin annular ring of order m, is given as [22]:

$$E(\rho, \theta) = \delta(\rho - \rho_0) exp(im\theta) \tag{1}$$

where ρ_0 is the radius of the POV beam, and δ represents the Dirac delta function.

The scattering of POV beams through a GGP can be described with random phase function $e^{i\Phi}$, where Φ varies randomly and its value lies in between 0 to 2π. Now, the scattered light field is given by [23-25]:

$$U(\rho, \theta) = \delta(\rho - \rho_0) e^{im\theta} * e^{i\Phi} \tag{2}$$

Now, the mutual coherence function between the two scattered POV fields of same order is defined as $\Gamma(r_1, \theta_1, z) = < U_1(r_1, \theta_1, z) U_1^*(r_1, \theta_1, z) >$ where $< U_1(r_1, \theta_1, z) U_1^*(r_1, \theta_1, z) >$ denotes the ensemble average. After solving the above equation using Fresnel's diffraction integral, we get [26]:

$$\Gamma_{12}(\Delta r) = \frac{e^{\frac{ik}{2z}(r_1^2 - r_2^2)}}{\lambda^2 z^2} \iint U_1(\rho, \theta) U_1^*(\rho, \theta) e^{-\frac{ik}{z}(\rho \Delta r \cos(\varphi_s - \theta))} \rho d\rho d\theta \tag{3}$$

Where $\Delta r \cos(\varphi_s - \theta) = [(r_1 \cos(\varphi_1) - r_2 \cos(\varphi_2)) \cos\theta] + [(r_1 \sin(\varphi_1) - r_2 \sin(\varphi_2)) \sin\theta]$ and $\Delta r^2 = r_1^2 + r_2^2 - 2 r_1 r_2 \cos(\varphi_2 - \varphi_1)$.

With the help of Anger-Jacobi Identity along with the integral properties of Dirac - delta function [27], we get the auto-correlation function as:

$$\Gamma_{12}(\Delta r) = \frac{2\pi \rho_0 \, e^{\frac{ik}{2z}(r_1^2 - r_2^2)}}{\lambda^2 z^2} J_0\left(\frac{k \rho_0}{z} \Delta r\right) \tag{4}$$

The normalized intensity distribution of the auto-correlation function can be evaluated in terms of time averaged intensity I_0 as [28]:

$$I(\Delta r) = I_0 \left(1 + J_0^2\left(\frac{k \rho_0}{z} \Delta r\right)\right) \tag{5}$$

Figure 2 (a), (b) shows the speckle patterns obtained by the scattering of POV beam of order zero and the corresponding auto-correlation function (Fig. 2(c)). As discussed above, this correlation function is then used as the encryption key and the keys for decryption are generated as explained in Section 3.

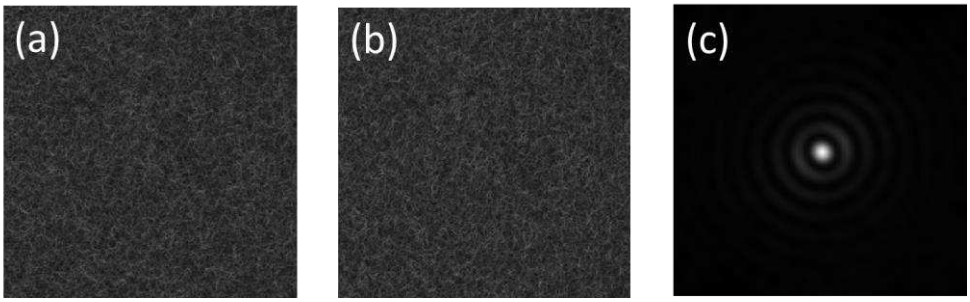

Figure 2. (a), (b) represents the speckle patterns obtained by scattering a POV beam of order zero and (c) depicts the corresponding correlation function between them.

2. Linear Canonical Transform based Double Random Phase Encoding

The LCT is a three-parameter class of linear integral transform and defined as follows [14]:

$$\Psi_{\alpha,\beta,\gamma}\{f(x,y)\} = C_1 \iint_{-\infty}^{\infty} f(x,y) exp\{i\pi[\alpha(x^2+y^2) - 2\beta(ux+vy) + \gamma(u^2+v^2)]\} dxdy \quad (6)$$

where α, β, γ are the real-valued parameters that are independent of the coordinates that is applied symmetrically in both horizontally (x) and (y), i.e., 2D separable LCT. It is known that these parameters are directly related to propagation distance [15]. In general, to note, DRPE can be classified based on ① Amplitude Encoding (AE), and ② Phase Encoding (PE). In this work, we are discussing LCT based AE-DRPE which is depicted here in Fig. 3.

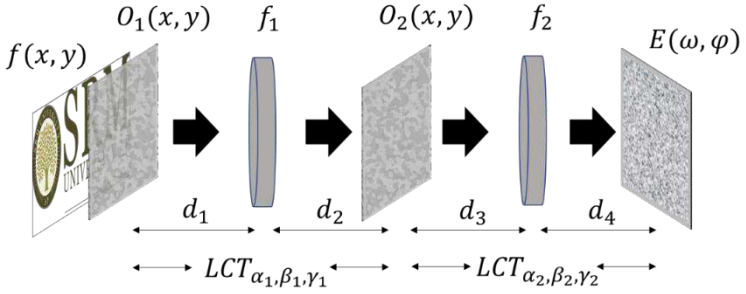

Figure 3. *(Color online) The schematic for LCT based DRPE system.*

A function $f(x,y)$ represents a 2D image which is to be encrypted. In this process, two Random Phase Masks (RPMs) $O_1(x,y)$ and $O_2(x,y)$ are considered as secret keys which is generated the process explained in Section 2. A collimated input light field passes through a first random phase mask $O_1(x,y)$, then the resulting mixed data propagates through the first QPS i.e., $LCT_{\alpha_1,\beta_1,\gamma_1}$. The resultant spectrum is modulated by the second mask $O_2(x,y)$ and propagates through second QPS i.e., $LCT_{\alpha_2,\beta_2,\gamma_2}$. To note, the RPMs apply the random phases $exp\{j2\pi n_1(x,y)\}$ and $exp\{j2\pi n_2(x,y)\}$ which are statistically independent but uniformly distributed in $[0,1]$. Mathematically, the encrypted (output) image $E(\omega,\varphi)$ can be expressed as follows [14]:

$$E(\omega,\varphi) = LCT_2\{LCT_1\{f(x,y) \times O_1(x,y)\} \times O_2(x,y)\} \tag{7}$$

It is known that the resultant encrypted image resembles a white noise i.e., speckle image, therefore it does not disclose any of the input information. Nevertheless, to note, the input data is just scrambled but not lost. It is therefore possible to reverse this process and get the original image back without loss. The process of reversing an encrypted data into a readable one is known as decryption. It is worth to mention that fact that $E(\omega,\varphi)$ is a complex-valued image therefore to record an encrypted image, an optical holographic imaging setup is preferred [4]. A method of capturing encrypted holograms is presented in Ref [14].

4. Experiments and simulation results

In our experiments, we have used ground glass plate of DG-10-600, from Thorlabs and imaging camera is from FLIR camera, pixel size of $3.45\ \mu m$. The speckle images are recorded in the size of 1000×1000 pixels but resized to 256×256 pixels for easier computations. The LCT parameters alpha, beta and gamma are set as $10, 100, 1$, respectively. Fig. 4(a) depicts the test image used (i.e., reconstructed hologram of a 3D object) as in input in our experiments [30]. Hologram generation and reconstruction is beyond the scope of this article, therefore not discussed in great detail here. Fig. 4(b) shows the amplitude of the complex encrypted image using generated POV and as can be seen from the encrypted image (Fig. 4b), information

contained is very difficult to be observed. Fig. 4(c) shows the decrypted image using appropriate secret keys. To evaluate the decrypted image quality, we used the classical mean squared error (MSE) metric which is calculated between the input image and decrypted image and the values are given in figure caption.

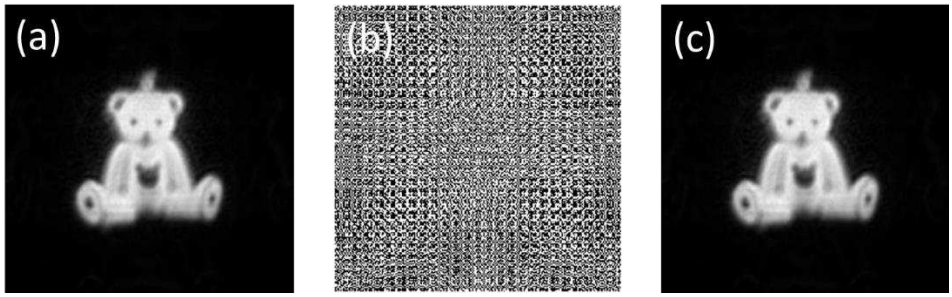

Figure 4. *(Color online) Simulation results: (a) Input grayscale image, (b) encrypted image and (c) decrypted image (MSE = 1.3685e-27).*

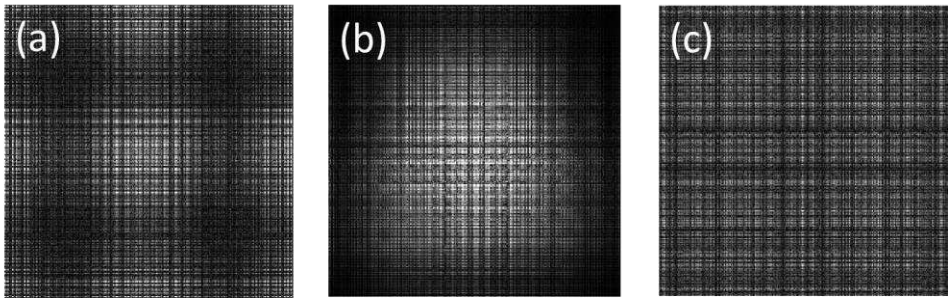

Figure 5. *Decryption with wrong LCT parameters: (a) alpha is wrong, (b) beta is wrong and (c) gamma is wrong.*

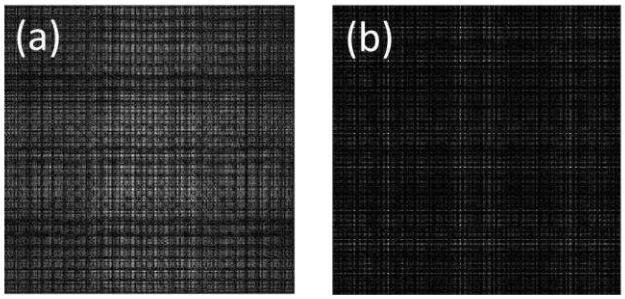

Figure 6. *Decryption with wrong keys: (a) changes in RPM_1, and (b) changes in RPM_2.*

As can be seen from Fig. 5 and Fig. 6, changes neither in the LCT parameter nor ion the encryption keys yield the fruitful results (i.e., encrypt images properly).

5. Conclusion

In this work, we have proposed a protocol for secret key generation for the digital implementation of the classical optical encryption systems. We encoded the light information with the correlation function of generated POV speckles and found that this method further augments the security as ground glass plate scrambles the light field and makes it as a physically unclonable function. We further note that huge amount of information is needed to reconstruct the cross spectral density distribution, therefore, the complexity in reconstruction of the cross spectral density distribution enhances the security of the encryption protocol. Our results demonstrate that the intensity correlation function of POV speckles of different orders serve as a tool in optical information security.

Acknowledgement

P. V, B. M, and S. A acknowledges the support of SRM University AP research fund. I. M and R. P. S acknowledges the Science and Engineering Research Board (SERB), Department of Science and Technology, Government of India. S. G. R likes to acknowledge the financial support of DST-SERB under grant number SRG/2019/000857.

Authors Contributions

P. V and B. M have performed optical experiments and P. V written the initial draft. S. G. R designed and formulated the ideas and was responsible for completion of the manuscript, I.M worked on encryption part. S. A and R. P. S critically examined/monitored each step of the work as the mentor and assisted in updating the manuscript.

Disclosures

Authors declare no conflicts of interest.

References

[1] S. Vaudenay, A classical introduction to cryptography, Springer International Edition (2008).

[2] W. Stallings, Cryptography and Network Security Principles and Practice, Prentice Hall, New York (2011).

[3] S. M. Bellovin, Frank Miller: Inventor of the One - Time pad, Cryptologia 35, 203-222 (2011).

[4] I. Muniraj, and J. T. Sheridan, Optical Encryption and Decryption, SPIE PRESS BOOK (2019).

[5] P. Refregier, and B. Javidi, \Optical image encryption based on input plane and Fourier plane random encoding," Opt. Lett 20, 767-769 (1995).

[6] A. VanderLugt, Optical Signal Processing, Wiley Series in Pure and Applied Optics, New York (2005).

[7] S. Liu, C. Guo and J. T. Sheridan, \A review of optical image encryption techniques," Opt. Laser Technol 57, 327-342 (2014).

[8] O. Matoba and B. Javidi, \Encrypted optical memory system using three-dimensional keys in the Fresnel domain," Opt. Lett 24, 762-764 (1999).

[9] G. Unnikrishnan, J. Joseph, and K. Singh, \Optical encryption by double-random phase encoding in the fractional Fourier domain," Opt. Lett 25, 887-889 (2000).

[10] L. Chen, and D. Zhao, \Optical image encryption with Hartley transforms," Opt. Lett 31, 3438-3440 (2006).

[11] G. Unnikrishnan and K. Singh, \Optical encryption using quadratic phase systems," Opt. Commun 193, 51-67 (2001).

[12] N. Rawat, B. Kim, I. Muniraj, G. Situ, and B. G. Lee, \Compressive sensing based robust multispectral double-image encryption," Appl. Opt. 54, 1782-1793 (2015).

[13] 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 7, 40113 (2017).

[14] I. Muniraj, C. Guo, R. Malallah, J. P. Ryle, J. J. Healy, B. G. Lee, and J. T. Sheridan, \Low photon count based digital holography for quadratic phase cryptography," Opt. Lett. 42, 2774-2777 (2017).

[15] C. Guo, I. Muniraj, and J. T. Sheridan, \Phase-retrieval-based attacks on linear-canonical-transform-based DRPE systems," Appl. Opt. 55, 4720-4728 (2016).

[16] P. Ravikanth, B. Recht, J. Taylor, and N. Gershenfeld, Physical One-way functions, Science 297, 2026-2030 (2002).

[17] Y. Gao, S. F. Al-sarawi, and D.Abbott, Physical Unclonable functions, Nature Electronics **3**, 81-91 (2020).

[18] B. Gassend, D. E. Clarke, M. van Dijk, S. Devadas: Silicon physical random functions. ACM Conference on Computer and Communications Security, pp. 148-160, (2002).

[19] C. Bohm, and M. Hofer, Physical Unclonable functions in theory and practice, Springer Publishers (2013).

[20] U. R¨uhrmair, J. S¨olter, F. Sehnke: On the Foundations of Physical Unclonable Functions. IACR Cryptology ePrint Archive 2009:277, (2009).

[21] G. E. Suh, S. Devadas: \Physical Unclonable Functions for Device Authentication and Secret Key Generation," DAC 2007, 9-14.

[22] A. S. Ostrovsky, C. R. Parrao, and V. Arrizon, \Generation of the ‘perfect’ optical vortex using a liquidcrystalspatial light modulator," Opt. Lett. **38**,534(2013).

[23] J. Goodman, Speckle Phenomena in Optics: Theory and Applications (Springer, 1975).

[24] J. C. Dainty, Laser speckle and related phenomena (Springer, 1976).

[25] S. G. Reddy, P. Chithrabhanu, S. Prabhakar, A. Anwar, and R. P. Singh, \Recovering the vorticity of a light beam after scattering," Appl. Phys. Lett. **107**, 021104 (2015).

[26] C. H. Acevedo and A. Dogariu, \Non-evolving spatial coherence function," Opt. Lett. **43**, 5761 (2018).

[27] I. S. Gradshteyn and I. M. Ryzhik, Table of Integrals, Series, and Products (Academic, 2007).

[28] P. Vanitha, N. Lal, A. Rani, B. K. Das, S. G. Reddy and R.P. Singh, \Correlations in scattered perfect optical vortices," J. Opt. **23**,095601(2021).

[29] L. Mandel and E. Wolf, Optical Coherence and Quantum Optics, Cambridge University Press (1995).

[30] M. Wan, I. Muniraj, R. Malallah, N. Chen, J. J. Healy, J. P. Ryle, & J. T. Sheridan, Orthographic projection images-based photon-counted integral Fourier holography. Applied Optics, 58(10), 2656-2661 (2019).