American Journal of Optics and Photonics
2021; 9(4): 55-58
http://www.sciencepublishinggroup.com/j/ajop
doi: 10.11648/j.ajop.20210904.12
ISSN: 2330-8486 (Print); ISSN: 2330-8494 (Online)

Scattering of Perfect Optical Vortex Beams: Physical Unclonable Function

Bikash Kumar Das

Department of Physics, Technion-Israel Institute of Technology, Haifa, Israel

Email address:
Bikash.das@campus.technion.ac.il

To cite this article:
Bikash Kumar Das. Scattering of Perfect Optical Vortex Beams: Physical Unclonable Function. *American Journal of Optics and Photonics.* Vol. 9, No. 4, 2021, pp. 55-58. doi: 10.11648/j.ajop.20210904.12

Received: October 25, 2021; **Accepted**: November 16, 2021; **Published**: December 29, 2021

Abstract: Now-a-days, data security has become an important part for anyone connected to the web. Data security ensures that data is getting transmitted securely without any modifications or alterations to the intended receiver**.** To achieve data security, we have focused on the cryptography which helps to protect our information from being stolen or third-party attacks. Encryption techniques demonstrate an excellent deal of data security when implemented in an optical system such as Holography due to the inherent physical properties of light and the precision it demands. Such systems are somehow vulnerable during their digital implementation under various attacks called crypt-analysis due to the predictable nature of security keys used for the encryption. In this work, we are presenting a Physically Unclonable Functions (PUFs) for producing a robust (stable over time) security key for digital encryption systems. More specifically, we have used the correlation functions of scattered perfect optical vortex beams for the generation of keys which can be used for encryption of data. Here, we convert the 2-D correlation function to 1-D key and digitize based on the average value which will be the random sequence of 1s and 0s. In the best of our knowledge, we are reporting this work for the first time. The experiment and simulation results are well matched.

Keywords: Cryptography, Encryption, Decryption, PUF, Security, Cipher, Optical System

1. Introduction

Since last several decades, Cryptography has acquired much popularity for secured transmission of information over an insecure channel like the internet. Information, which needs to be sent, is encrypted in the transmission end and is decrypted in the receiving end using appropriate keys (encrypted and decrypted keys may be same or different depending on the type). An algorithm is usually written for encryption of the information which unites original information with certain number of keys (string of bits) and this algorithm is popularly known as cipher [1]. Initially, classical cryptographic techniques such as symmetric key cryptography (Data Encryption Standard or Data Encryption Algorithm) and asymmetric or public key cryptography (RSA) were employed. In symmetric key cryptography, same key is used for encryption as well as decryption. So, some major difficulties get noticed with this cryptographic technique such as the distribution of key and detection of third parties i.e., eavesdropper which was later solved by quantum cryptography. In public key cryptography, the sender uses public key of the receiver to encrypt the information which is decrypted only with the receiver's private key. Optical encryption of the information offers a low complexity and higher data rates as compared to electronic encryption. Now-a-days, cryptography is commonly used in various fields such as secured bank transactions, health care, social media, the Internet of Things (IoT), government, security protocols etc. For the first time in 1882, Miller introduced the One Time Pad (OTP) technique which basically uses a perfect random key that is at least as long as the original information. Presently, we are witnessing a constant evolution and change in the field of encryption.

Basically, Physical Unclonable Functions (PUFs) is a physical object that for a given input and conditions (challenges) provides a physically defined "digital fingerprint" output (responses) which serves a unique identifier. PUFs are based on unique physical variations (microstructure) which occur naturally during manufacturing. Advantages of PUFs include (1) easy to evaluate (2) stability

over time (3) difficult to replicate (4) impossible to duplicate (cloning of PUFs is impossible). These characteristics of PUFs make us believe that ground glass plate, which is being used for scattering of perfect optical vortex beam, can be used as a PUF device which produces a speckle pattern that can never be cloned.

The correlations in light beams are becoming one of the promising fields of study as it plays a vital role in certain applications such as communication [2-3]. The correlation functions that have singularities are named as "coherent vortices" [4-5]. Recently, these coherent vortices are realized in the intensity correlation of two speckle patterns of different orders [5-6].

As a fundamental attribute that describes statistical properties of random light fields, optical coherence has played an important role in understanding and tailoring light-matter interactions [2, 9]. Information encryption with the help of optical technologies has been studied extensively in the past decade due to remarkable multidimensional capabilities and ultrafast modulation speed afforded by the light fields [10, 11]. Numerous protocols for optical information encryption have been proposed since the double random phase encoding (DRPE) was developed by Refregier and Javidi [12]. Rigorous research on optical information encryption has been carried out till now using the DRPE or DRPE related techniques such as a fractional Fourier domain DRPE [13]. Other techniques include lens less DRPE in the Fresnel domain and multidimensional random phase encoding [14-15]. Recent progress in the light field structure engineering has highlighted the degrees of freedom of a structured light field as the powerful tools for information encoding [16, 18, 19]. The optical encryption protocols based on the phase structure modulation, OAM and polarization state MDM have been developed lately [19-26].

In this paper, a simple and effective method for the generation of Perfect Optical Vortex (POV) speckle pattern by scattering of POV beams through a Ground Glass Plate (GGP) has been proposed and correlated the generated speckle patterns i.e. 2-D correlation from which 1-D key has been generated and is used for encryption purpose [7]. For efficient generation of keys, we have used Physically Unclonable Functions (PUFs) and then digitize based on average value which will be random sequence of 1s and 0s. Now-a-days, researchers are using optical technologies for encryption of sensitive information due to multidimensional capabilities of light field. In this work, an optical encryption protocol has been used where the information to be sent is encoded with the correlation image of a structured POV beam.

2. Experiment

In this experiment, one of the simplest methods has been proposed to generate a perfect optical vortex beam. Figure 1 shows the experimental set up to generate a perfect optical vortex beam and figure 2 shows the scattering of perfect optical vortex beam through a ground glass plate (GGP) in order to produce perfect optical vortex speckle pattern. A He-Ne laser with a wavelength of 632nm has been used as an optical source which will generate Gaussian beam. The laser beam is made to fall on a reflecting mirror which will be reflected from it and will incident on an unpolarized beam splitter. A spatial light modulator (SLM) in phase only mode has been used which will introduce an optical vortex onto the laser beam. When the spatial light modulator is illuminated by laser beam, an optical vortex beam is produced. The desired beam selected with an aperture (A) is passed through an axicon of apex angle 178° in order to convert the vortex beam into a non-diffracting Bessel-Gauge (BG) beam. An axicon has been placed at a distance of 50cm from the spatial light modulator. In order to obtain perfect optical vortex beam from Bessel-Gauge beam, a lens of focal length 30cm has been used which will simply perform the Fourier transform (image will be obtained at a very large distance) of BG beam. The intensity distribution of POV beam is recorded through a CCD Camera (FLIR, pixel size 3.45μm) which is placed at the Fourier plane.

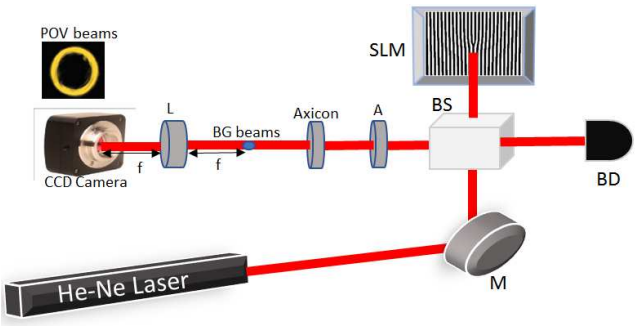

Figure 1. *(Color line) Experimental setup for the generation of perfect optical vortex (POV) beams using a spatial light modulator (in phase only mode) and an axicon. M-Mirror, BD-Beam Dumper, BS-Beam Splitter, SLM-Spatial Light Modulator, A-Aperture, BG-Bessel Gauge, L-Lens, f-Focal Length, CCD-Charge Couple Device.*

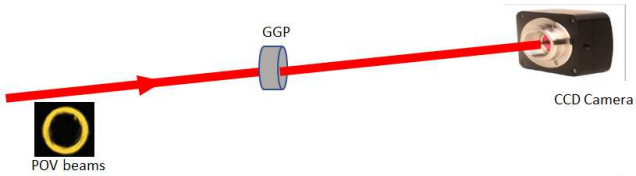

Figure 2. *(Color line) Experimental set up for generation of speckle from POV beams using ground glass plate and recording the speckle pattern using CCD camera.*

The generated POV beams are allowed to pass through a ground glass plate (GGP) (DG10-600, from Thorlabs) for scattering. Ground glass plate is placed at a distance of 72.5 cm from the axicon. Due to interference of many scattered wave fronts, which arise due to the presence of inhomogeneities in GGP, a fine granular pattern of light having randomness is produced and is called as the speckle pattern. Speckle patterns have been recorded at different propagation distances using a CCD camera.

The field which hoists a POV beam having thin annular ring of order m is given by this formula [8],

$$E(\rho, \theta) = \delta(\rho-\rho_0)\, e^{im\theta} \quad (1)$$

Where ρ_0 is the POV beam radius and δ represents the Dirac Delta function having the following properties:

$$\delta(\rho-\rho_0) = 0, \text{ if } \rho \neq \rho_0$$

$$= \infty, \text{ if } \rho = \rho_0$$

A random phase function of $e^{i\varphi}$ gets introduced in the beam when it is allowed to scatter through a ground glass plate. After scattering of the POV beam through GGP, field distribution of the speckle can be represented as,

$$U(\rho, \theta) = \delta\ (\rho-\rho_0)\, e^{im\theta}\, e^{i\varphi} \quad (2)$$

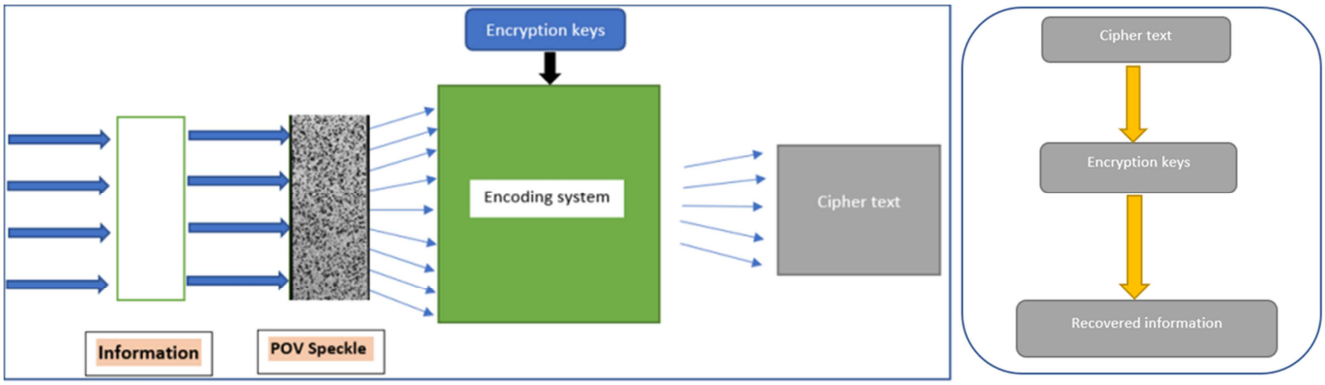

Figure 3. *Represents a new optical encryption protocol named as Saroj-Bikash (SB Protocol) Protocol based on correlation function taken for perfect optical vortex speckles. An information with the correlation function combines with encryption keys forms an encoding system. We generate 2-D correlation image for correlation functions of different order POV beams using MATLAB coding and generate 1-D key from 2-D correlation image using Python. So, after encryption of the piece of information to be sent, cipher text is produced. Same encryption key will be used for decryption of cipher text in order to recover the original information.*

3. Results and Discussion

In this work, a special class of coherence vortex beam is generated from the scattering of POV beams. The correlation function of the generated coherence vortex is generated by taking the intensity correlation of two speckle pattern corresponding to POV beams of different orders. The generated correlation function is given as,

$$\Gamma_{12}(\Delta r) = \frac{2\pi(-1)^{m_2-m_1}(\mathrm{i})^{m_2-m_1}e^{\frac{ik}{2z}}}{\lambda^2 z^2} e^{i(m_1-m_2)\varphi} \int_0^\infty \delta(\rho-\rho_0) J_{m_2-m,\left(\frac{k\rho\Delta r}{z}\right)}\, \rho\, d\rho \left(\frac{k\rho_0\Delta r}{z}\right) \quad (3)$$

Using equation (2) in the above equation with the help of Anger-Jacobi identity and integral properties of Dirac-Delta function, we get

$$\Gamma_{12}(\Delta r) = \frac{2\Pi(-i)^{m_2-m_1}e^{\frac{ik}{2z}\left(r_1^2-r_2^2\right)}}{\lambda^2 z^2} \cdot e^{i(m_1-m_2)\varphi} J_{m_2-m_1}\left(\frac{k\rho_0\Delta r}{z}\right) \quad (4)$$

From the above equation, it is clear that the correlation function of two speckle pattern of order m_1 and m_2 is completely dependent on the Bessel function of order m, where $m = m_2 - m_1$.

For $m_1 = m_2$, the cross-correlation function reduces to the auto-correlation function of order 0.

In this presented work, different values of m_1 and m_2 are taken for the generation of correlation image of the speckles and to generate 1-D key from this image. Recent report shows that the cross spectral density (CSD) of a random beam can be viewed as an effective career of an optically encoded information.

A ground glass plate is taken as a Physical Unclonable Function (PUF) device which is having random inhomogeneities which are introduced during its manufacturing. PUF devices are difficult to duplicate and Unclonable. So, producing two ground glass plates having same randomness is impossible. In this work, we are generating POV speckles by scattering of POV beams through a GGP. So, without the knowledge of the correlation function which depends on Bessel function of specific order and ground glass plate, an eavesdropper can't access the information which is being sent. In our work, we have used a single encryption key for encoding the information and same key will be used for decoding the information as well.

Figure 4. *Represents experimentally generated Bessel-Gauss coherence functions of order m=0-2 at a propagation distance of 20 cm from the ground glass plate.*

The complexity of measuring the correlation function makes our protocol the best fit for the encryption of the information.

4. Conclusion

In this work, a new protocol has been devised for optical information encryption into the fourth order correlation of the light fields expressed in terms of the cross spectral density function of the field. The information has been encoded with the correlation function of generated POV speckles and found that this protocol enhances the information security as we are taking the help of a ground glass plate as the Physical Unclonable Function device which cannot be cloned further. It is found that huge amount of information is needed to reconstruct the cross spectral density distribution. So, the complexity in reconstruction of the cross spectral density distribution enhances the security of the encryption protocol. These results show that the intensity correlation function of POV speckles of different orders serve as a tool in optical security and optical information security protocol.

References

[1] A. Goyal, S. Aggarwal, and A. Jain, 5th International Conference on Advanced Computing and Communication Technologies, 81-87885-03-3.

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

[3] P. Kumar, A. Fatima, and N. K. Nishchal, J. of Opt. 21 065701 (2019).

[4] W. Wang, S. G. Hanson, Y. Miyamoto, and M. Takeda, Phys. Rev. Lett. 94, 103902 (2005).

[5] C. R. Alves, A. J. Jesus-Silva, and E. J. Fonseca, Opt. Lett. 40, 2747 (2015).

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

[7] P. Vanitha, N. Lal, A. Rani, B. K. Das, S. G. Reddy, R. P. Singh, J. of Opt. (2021).

[8] A. S. Ostrovsky, C. R. Parrao, and V. Arrizon, Opt. Lett. 38, 534 (2013).

[9] A. T. Friberg and T. Setala, Electromagnetic theory of optical coherence (invited), J. Opt. Soc. Am. A 33, 2431-2442 (2016).

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

[11] W. Chen, B. Javidi, and X. Chen, Advances in optical security systems, Adv. Opt. Photon. 6, 120-155 (2014).

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

[13] 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).

[14] G. Situ and J. Zhang, Double random-phase encoding in the Fresnel domain, Opt. Lett. 29, 1584-1586 (2004).

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

[16] H. Rubinsztein-Dunlop, A. Forbes, M. V. Berry, et al., Roadmap on structured light, J. Opt. 19, 013001 (2017).

[17] C. Rosales-Guzman, B. Ndagano, and A. Forbes, A review of complex vector light fields and their applications, J. Opt. 20, 123001 (2018).

[18] A. Forbes, Structured light from Lasers, Laser Photon. Rev. 13, 1900140 (2019).

[19] G. Qu, W. Yang, Q. Song, Y. Liu, C.-W. Qiu, J. Han, D.-P. Tsai, and S. Xiao, Reprogrammable meta-hologram for optical encryption, Nat. Commun. 11, 5484 (2020).

[20] A. Trichili, A. B. Salem, A. Dudley, M. Zghal, and A. Forbes, Encoding information using Laguerre Gaussian modes over free space turbulence media, Opt. Lett. 41, 3086-3089 (2016).

[21] X. Fang, H. Ren and M. Gu, Orbital angular momentum holography for high-security encryption, Nat. Photon. 14, 102-108 (2019).

[22] Z. Qiao, Z. Wan, G. Xie, J. Wang, L. Qian, and D. Fan, Multi-vortex laser enabling spatial and temporal encoding, PhotoniX 1, 13 (2020).

[23] Y. Zhao, J. Wang, High-base vector beam encoding/decoding for visible-light communications, Opt. Lett. 40, 4843-4846 (2015).

[24] G. Milione, T. A. Nguyen, J. Leach, D. A. Nolan, and R. R. Alfano, Using the nonseparability of vector beams to encode information for optical communication, Opt. Lett. 40, 4887-4890 (2015).

[25] M. Xian, Y. Xu, X. Ouyang, Y. Cao, S. Lan, and X. Li, Segmented cylindrical vector beams for massively-encoded optical data storage, Sci. Bull. 65, 2072-2079 (2020).

[26] H. Larocque, A. D'Errico, M. F. Ferrer-Garcia, A. Carmi, E. Cohen, and E. Karimi, Optical framed knots as information carriers, Nat. Commun. 11, 5119 (2020).