ap

Asian Journal of Physics
Vol. 27, Nos 9-12 (2018) 597-602
Available on: www.asianjournalofphysics.in

Photon-counting and sparsity-based optical authentication and verification schemes

Areeba Fatima and Naveen K Nishchal
Department of Physics, Indian Institute of Technology Patna
Bihar, Patna-801 103, India

This article is dedicated to Prof T Asakura

Optical information security is a widely researched field and optical authentication and verification schemes form an integral part of it. This paper reviews the two most widely used approaches to develop the authentication systems, namely, the photon-counting technique and the sparsity-based technique. The methodology of each category is discussed with its benefits.

Keywords: Authentication, Sparsity of matrices, Photon counting, Nonlinear correlator

1 Introduction

The field of optical information security has seen a tremendous advancement in the past decades and continues to grow owing to the advantages offered by multiple degrees of freedom of light [1]. Authentication systems form a major part of the information security schemes wherein, the authenticity of any information is established without revealing the complete information to the receivers. In literature, different optical pattern recognition schemes have been used to set up authentication systems [2-6]. One of the main principles employed for these validation systems is the joint transform correlator (JTC) [2]. Authentication based on the conventional JTCs evaluates the joint power spectrum of the target and the reference image, which is then inverse Fourier transformed. A conspicuous peak denotes validation of the target with respect to the reference, while, a noisy distribution denotes inauthentic target [2]. Different types of JTCs have been reported in the optical information security literature that establish the validity of any given image [1-5]. With time two different broad categories of authentication system have evolved which aim at authentication without revealing the content of the plaintext. These two categories involve the photon-counting method [7-14] and the sparse matrix-based method [15-21]. The former category involves recording of the ciphertext under low light illumination and has come to be a widely studied technique. Perez-Cabre *et al* [8] for the first time introduced the photon counting based image authentication system and since then many variants using this technique has been reported.

The second category consists of rendering any of the measurements of the optical field as sparse and this sparse data, such as the sparse phase or the sparse ciphertext is then utilized to set up authentication system. This technique too has been widely studied for authentication systems [15-21]. Various encryption strategies have been used to develop the sparse data, so as to get a robust authentication system. The two techniques offer greater security because the entire information is not revealed to the receiver. This paper reviews the basic idea underlying the two techniques used for image authentication by studying examples of the two methods.

Corresponding author :
e mail: nkn@iitp.ac.in; (Naveen K Nishchal); Tel.: + 91-612-3028027; Fax: + 91-612-3028111

2 Photon counting technology for image authentication

Photon counting technology involves recording with few photons under low illumination condition in the process of imaging. Pattern recognition has emerged as one of the applications of photon counting detection [7]. It has been shown that object recognition can be carried out using as low as hundreds of detected photons. Different image classification techniques at low light levels have been proposed [7-14]. Perez-Cabre *et al* [8]. integrated the well known double random phase encoding (DRPE) technique with the photon counting method to get a photon-limited encrypted image [8]. This ciphertext on being decrypted does not reveal any information about the plaintext. However, the recorded information with the limited photons is sufficient to establish authenticity.

In any photon counting-based encrypted image authentication scheme, a photon-limited ciphertext is obtained by evaluating the probability of counting photons at the *j*th pixel, which is described by the Poisson distribution [8]:

$$P_d(l_j;\lambda_j)=\frac{[\lambda_j]^{l_j}e^{-\lambda_j}}{l_j!}, \qquad l_j=0,1,2,..... \tag{1}$$

here l_j is the number of photons detected at *j*th pixel. λ_j is the Poisson parameter, given by $\lambda_j = N_p x_j$ with x_j representing the normalized irradiance at *j*th pixel and $\sum_{j=1}^{M} x_j = 1$. M is equal to the total number of pixels in the scene. N_p is the number of counts in the entire scene.

The ciphertext denoted by $\psi(x, y)$ is obtained through any encryption architecture and then subjected to the photon counting method based on the probability distribution described in Eq (1). The photon-limited ciphertext $\psi_{ph}(x, y)$ is sent to the receiver where it is decrypted using all correct keys. The decrypted information is compared with the original information by evaluating the nonlinear correlation $c(x,y)$, given in [2,16,20]:

$$c(x,y)=IFT\left\{\left|T(u,v)R(u,v)\right|^{k}\exp\left\{i\varphi_T(u,v)-\varphi_R(u,v)\right\}\right\} \tag{2}$$

where, $T(u,v)$ and $R(u,v)$ are the two-dimensional Fourier transforms of the photon-limited decrypted image $t(x,y)$ and the original image $r(x,y)$, respectively. The parameter k defines the degree of non-linearity, which decides the efficiency of the correlator. The photon counting technique when used with the DRPE method increased the robustness of the latter because the photon-limited information was not sufficient to retrieve the plaintext information. Figure 1 shows the results of photon-counting based authentication results using the DRPE architecture.

The input image is taken to be a 256 × 256 pixel size gray-scale image as shown in Fig 1 (a). This image is subjected to the DRPE. The ciphertext thus obtained is shown in Fig. 1(b). A low light illumination condition is simulated and the ciphertext recorded in the photon counting process is shown in Fig 1(c). The photon-limited ciphertext is then decrypted using all correct keys and this decrypted image is shown in Fig 1(d). It can be seen that information about the plaintext is not revealed. The nonlinear correlation peak of the decrypted image with the original image is shown in Fig 1(e). The photon counting method combined with DRPE does not give the plaintext information on decryption but it is sufficient to give sharp peak during nonlinear correlation which demonstrates the authenticity.

Following Perez-Cabre *et al* [8] work, different encryption architectures have been proposed to carry out photoncounting based authentication. Rajput *et al* [9]. proposed a multiple images authentication scheme based on phase mask multiplexing and photon count imaging .The scheme consisted of multiplexing the phase-only masks corresponding to each images and then encoding the multiplexed information using

known encryption architecture. The ciphertext thus obtained was subjected to photon counting imaging. It was shown that the photon-limited ciphertext carried sufficient information for authentication of the multiple images. Polarization-based encoding has also been integrated with the photon counting method for securing image verification [10]. In another work, Maluenda *et al* [11] proposed a polarimetric optical encoder that used photoncounting method. The initial work combining the DRPE and the photon counting had employed the complete complex ciphertext generated from the DRPE system to get the photon-limited function. However, it was demonstrated in a subsequent work that using only the amplitude of the ciphertext for photon counting imaging results in enough information to establish the authenticity of the image [12]. This established the photon counting technique as strong tool to develop secured image authentication systems. Markman *et al* [13]. carried out full phase DRPE followed by photon-counting technique. The sparse image thus generated is decrypted and its statistical parameters are used for authentication

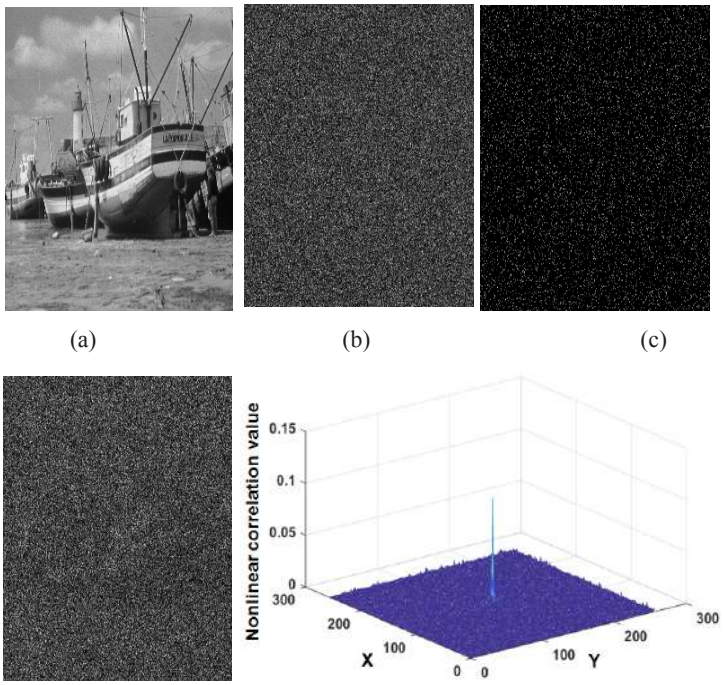

Fig 1 (a) Input image, (b) encrypted image using DRPE scheme, (c) photon-limited encrypted image, (d) decrypted image with correct key using the photon-limited ciphertext, (e) authentication peak obtained with nonlinear correlator.

Hence, many photon-counting techniques have been utilized to process the encrypted image for securing image authentication. However, in a different approach of authentication systems, sparse information introduced computationally, have been used. This technique has been discussed in the next section.

3 Sparse images for authentication

The photoncounting scheme described in the previous section may complicate the optical cryptosystem. Therefore, in a simpler approach, a different technique of image authentication has been developed which randomly selects only partial information of the ciphertext to be sent to the receiver. The sparsity percentage, which is the percentage of information retained, is so chosen that there is enough

information to match the data with the reference information, yet, the original information is not revealed on decryption. Many variants of this approach have been reported in the literature [15-20]. Gong *et al* [15] demonstrated multiple images authentication using sparse ciphertexts. The redundant spaces in the sparse matrices of the ciphertexts have been employed to multiplex different images. Sparse phase information corresponding to the images has been used to develop authentication systems. In one of the works, phase-only functions corresponding to the images have been evaluated using the Gerchberg-Saxton algorithm [16]. These phase-only functions are then made sparse by randomly selecting appropriate amount of pixel values of the phase matrix, while rendering rest of the pixel values as zero. These sparse phase-only functions are encoded into the phase of a vector beam followed by Stokes parameters measurement of the vector beam. One of the Stokes parameters is used as key and the other parameter is used as ciphertext. This sparse ciphertext is used for validating the authenticity of the images. Figure 2 depicts the results of authentication using sparse matrix approach. The input image shown in Fig 1(a) has been used for this study. Phase-only function corresponding to this image has been evaluated. Only 20 percent of the pixel values of the phase-only function is randomly selected and retained, while the rest are set to zero. This sparse phase-only function is shown in Fig 2(a). The decrypted image with the sparse ciphertext using all correct keys is shown in Fig 2(b), which shows that plaintext information is not revealed. The correlation peak establishing the authenticity is shown in Fig 2(c).

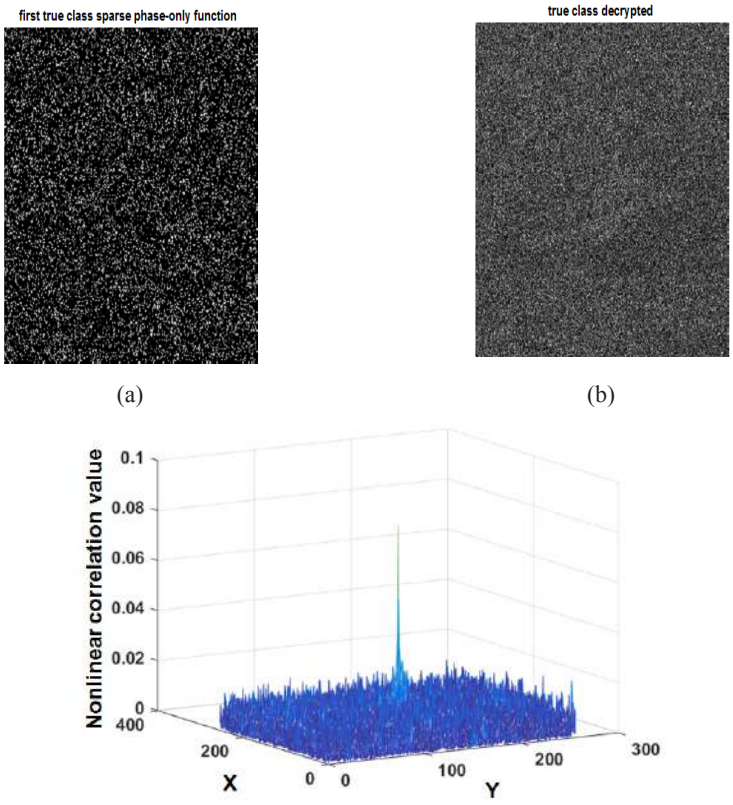

Fig 2. (a) Phase-only function made sparse with sparsity percentage 20%, (b) decrypted image with all correct keys ,and (c) authentication peak obtained with nonlinear correlator.

Chen *et al* [17,18]. developed the technique of using sparse matrices for image authentication in a series of studies. Other authentication set ups have integrated sparsity constraints technique with phase retrieval [18] and fractional Fourier domain encoding [19]. Three-dimensional image authentication has been studied using sparse matrices which contain limited information of the encrypted ciphertext [20]. Being a simpler process, sparse information based authentication systems continue to be widely studied technique [21].

4 Conclusion

Photon-counting technique has been used in conjunction with different optical encryption architectures to develop authentication systems. This technique involves recording the ciphertext with limited number of photons and hence the ciphertext carries less information. This photon-limited ciphertext is then used for authenticating the images using nonlinear correlators. In a different approach, secured image authentication has been proposed by using sparse information of phase or plaintext obtained computationally. This method randomly selects only a certain percentage of the information to serve as the ciphertext, and reduces the experimental complexity involved in photon counting technique. The selection of pixel values in photon counting method follows the Poisson distribution while, in sparse-matrix based method, the pixel values are retained randomly. The above two methods have become one of the most favored techniques for encrypted optical image authentication.

Acknowledgements

The authors acknowledge the funding from the Council of Scientific and Industrial Research, Government of India, under Grant No. 03/ (1351)/16/EMR-II.

References

1. Javidi B, Carnicer A, Yamaguchi M, Nomura T, Perez-Cabre E, Millan M S, Nishchal N K, Torroba R, Barrera J F, He W, Peng X, Stern A, Rivenson Y, Alfalou A, Brosseau C, Guo C, Sheridan J T, Situ G, Naruse M, Matsumoto T, Juvells I, Tajahuerce E, Lancis J, Chen W, Chen X, Pinkse P W H, Mosk A P, Markman A, *J Opt*, 18(2016) 083001; doi.org/10.1088/2040-8978/18/8/083001
2. Javidi B, *Appl Opt*, 28(1989)2358-2367.
3. Millan M S, Perez-Cabre E, Javidi B, *Opt Lett*, 31(2006)721-723.
4. Rajput S K, Nishchal N K, *Opt Lasers Eng*, 50(2012)1474-1483.
5. Rajput S K,Nishchal N K, *J Opt Soc Am A*, 31(2014)1233-1238.
6. CarnicerA, Hassanfiroozi A, Latorre-Carmona P, Huang Y, Javidi B, *Opt Lett*, 40(2015)135-138.
7. Watson E A, Morris G M, *Appl Opt*, 31(1992)4751-4757.
8. Perez-Cabre E, Cho M, Javidi B, *Opt Lett*, 36(2011)22-24.
9. Rajput S K, Kumar D, Nishchal N K, *Appl Opt*, 54(2015)1657-1666.
10. Rajput S K, Kumar D, Nishchal N K, *J Opt*, 16(2014)125406; doi.org/10.1088/2040-8978/16/12/125406
11. Maluenda D, Carnicer A, Herrero R M, Juvells I, Javidi B, *Opt Express*, 23(2015)655-666.
12. Wang Y, Markman A, Quan C, Javidi B, *J Opt Soc Am A*, 33(2016) 2158-2165.
13. Markman A, Javidi B, *J Opt Soc Am A*, 31(2014)394-403.
14. Perez-Cabre E, Mohammed E A, Millan M S, SaadonH L, *J Opt*, 17(2015)025706, doi.org/10.1088/2040-8978/17/2/025706
15. Gong Q, Liu X, Li G, Qin Y, *Appl Opt*, 52(2013)7486-7493.
16. Fatima A, Nishchal N K, *J Opt Soc Am A*, 35(2018)1053-1062.
17. Chen W, Chen X, Stern A, Javidi B, *IEEE Photon J*, 5(2013)6900113; doi:10.1109/JPHOT.2013.2258144.
18. Wang X, Chen W, Chen X, *IEEE Photon J*, 7 (2015) 7800310; doi: 10.1109/JPHOT.2015.2412936

19. Chen J, Zhu Z, Fu C, Zhang L, Zhang Y, *Optik*, 136(2017)1-7.
20. Yi F, JeoungY, Moon I, *Appl Opt*, 56(2017)4381-4387.
21. Mohammed E A, Saadon H L, *Appl Opt*, 55(2016)9939-9944.

[*Receieved*: 2.10. 2018; *Received*: 1.11.2018]

Areeba Fatima

Areeba Fatima is currently pursuing Ph D under the supervision of Prof Naveen K. Nishchal at IIT Patna, India. She received her Masters Degree in Science from the Patna University in the year 2011. Her research is focused on optical information security systems.