photonics

MDPI

Article

Optical Image Encryption System Using Several Tilted Planes

Juan M. Vilardy O. [1,*], Carlos J. Jimenez [1] and Cesar O. Torres M. [2]

[1] Grupo de Investigación en Física del Estado Sólido (GIFES), Faculty of Basic and Applied Sciences, Universidad de La Guajira, Riohacha (La Guajira) 440007, Colombia; cjimenez@uniguajira.edu.co

[2] Grupo de óptica e informática, Department of electronic engineering, Universidad Popular del Cesar, Valledupar (Cesar) 200001, Colombia; cesartorres@unicesar.edu.co

* Correspondence: jmvilardy@uniguajira.edu.co

Received: 25 September 2019; Accepted: 28 October 2019 ; Published: 7 November 2019

Abstract: A well-known technique for optical image encryption is the double random phase encoding (DRPE) technique, which uses two random phase masks (RPMs), one RPM at the input plane of the encryption system and the other RPM at the Fourier plane of the optical system, in order to obtain the encrypted image. In this work, we propose to use tilted planes for the Fourier and the output planes of the optical DRPE encryption system with the purpose of adding two new security keys, which are the angles of the tilted planes. The optical diffraction on a tilted plane is computed using the angular spectrum of plane waves and the coordinate rotation in the Fourier domain. The tilted distributions at the intermediate and output planes of the optical DRPE encryption system are the second RPM and the encrypted image, respectively. The angles of the tilted planes allow improvement to the security of the encrypted image. We perform several numerical simulations with the purpose of demonstrating the validity and feasibility of the proposed image encryption system.

Keywords: optical image encryption; double random phase encoding (DRPE); tilted plane

1. Introduction

The double random phase encoding (DRPE) technique is a very important technique for optical image encryption [1–5]. Initially, the DRPE technique was optically implemented using a 4*f*-processor in the Fourier domain [6]. Later, the DRPE was extended to the Fresnel [7,8] and the fractional Fourier domains [9], to increase the security level of the encryption and decryption systems.

We propose to use tilted planes for the optical DRPE technique in the Fresnel domain, with the purpose of encrypting and decrypting images. The proposed tilted planes for the optical DRPE encryption system are the intermediate and output planes. The tilted planes contain the second RPM used in the DRPE technique and the encrypted image, respectively. The use of the tilted planes for the optical DRPE technique allows to introduction of new security keys, given by the two tilt angles. The proposed DRPE encryption system of this work uses the free optical propagation on tilted planes and this propagation is computed by using the angular spectrum of plane waves and the coordinate rotation in the Fourier domain [10]. The two tilt angles and the propagations distances are security keys that permit improvements to the security of the encrypted image. The proposed security system is verified by using numerical simulations of the encryption and decryption systems.

2. Optical Diffraction on Tilted Planes

We use the technique based on the angular spectrum of plane waves and coordinate rotation in the Fourier domain described in reference [10] in order to compute the optical diffraction on tilted planes. Let $g(x, y)$ and $G(u, v)$ be a source field and its spectrum, in the source plane; the coordinates

of the source plane are denoted by x and y. The distance between the source plane and the reference plane is $d > 0$ and the optical propagation of the source field is along the z axis. Let $G_d(u, v)$ be the source spectrum in an intermediate plane or reference plane, which is parallel to the source plane, and that its coordinates share the origin with the reference coordinates; the coordinates of the reference plane are represented by x' and $y' = \hat{y}$. Figure 1 shows the optical scheme for the diffraction on a tilted plane where the coordinates of the observation plane are denoted by $\hat{x}$ and $\hat{y}$. Using the standard formula of the angular spectrum of plane waves [6], we can obtain

$$G_d(u, v) = G(u, v) \exp\left\{ i2\pi d \left(\lambda^{-2} - u^2 - v^2 \right)^{1/2} \right\}, \tag{1}$$

where u and v are the spatial frequency coordinates and λ is the wavelength. The rotation matrix $\mathbf{T}$ can be used to transform the reference coordinates into the observation coordinates. Therefore, the wave vectors of these coordinates can also be transformed into each other by

$$\hat{\boldsymbol{k}} = \mathbf{T}\boldsymbol{k}, \quad \boldsymbol{k} = \mathbf{T}^{-1}\hat{\boldsymbol{k}}, \tag{2}$$

with

$$\begin{aligned} \hat{\boldsymbol{k}} &= 2\pi \begin{bmatrix} \hat{u} & \hat{v} & \hat{w}(\hat{u}, \hat{v}) \end{bmatrix}, \quad \hat{w}(\hat{u}, \hat{v}) = \left(\lambda^{-2} - \hat{u}^2 - \hat{v}^2 \right)^{1/2}, \\ \boldsymbol{k} &= 2\pi \begin{bmatrix} u & v & w(u, v) \end{bmatrix}, \quad w(u, v) = \left(\lambda^{-2} - u^2 - v^2 \right)^{1/2}, \\ \mathbf{T}^{-1} &= \begin{bmatrix} a_1 & a_2 & a_3 \\ a_4 & a_5 & a_6 \\ a_7 & a_8 & a_9 \end{bmatrix}, \end{aligned} \tag{3}$$

where $2\pi w(u, v)$ represents the component in z direction of the wave vector. The spatial frequency coordinates (u, v) and $(\hat{u}, \hat{v})$ are related to the source spectrum in the reference (without tilt) and observation (with tilt) planes, respectively. The rotation matrices $\mathbf{T}^{-1}$ that produce a tilted plane for Figure 1 are

$$\mathbf{T}_x^{-1}(\theta_x) = \begin{bmatrix} 1 & 0 & 1 \\ 0 & \cos\theta_x & -\sin\theta_x \\ 0 & \sin\theta_x & \cos\theta_x \end{bmatrix}, \quad \mathbf{T}_y^{-1}(\theta_y) = \begin{bmatrix} \cos\theta_y & 0 & \sin\theta_y \\ 0 & 1 & 0 \\ -\sin\theta_y & 0 & \cos\theta_y \end{bmatrix}, \tag{4}$$

where the rotation matrix $\mathbf{T}_x^{-1}(\theta_x)$ is a rotation around the x axis, which produces a tilted plane with respect to the y axis and the rotation matrix $\mathbf{T}_y^{-1}(\theta_y)$ is a rotation around the y axis and this produces a tilted plane with respect to the x axis. The tilted plane of Figure 1 is described by the rotation matrix $\mathbf{T}_y^{-1}(\theta_y)$.

The Fourier frequencies in the reference coordinates are related to those in the observation coordinates in the following form

$$u = \alpha(\hat{u}, \hat{v}) = a_1\hat{u} + a_2\hat{v} + a_3\hat{w}(\hat{u}, \hat{v}), \quad v = \beta(\hat{u}, \hat{v}) = a_4\hat{u} + a_5\hat{v} + a_6\hat{w}(\hat{u}, \hat{v}). \tag{5}$$

The spectrum in the observation coordinate is given by the spectrum in the reference coordinate according to

$$F(\hat{u}, \hat{v}) = G_d(\alpha(\hat{u}, \hat{v}), \beta(\hat{u}, \hat{v})). \tag{6}$$

The complex amplitudes of the field in the observation coordinates with the same energy as the complex amplitudes of the field in the reference coordinates are given by

$$f(\hat{x},\hat{y}) = \int_{-\infty}^{+\infty}\int_{-\infty}^{+\infty} F(\hat{u},\hat{v})|J(\hat{u},\hat{v})|\exp\{i2\pi(\hat{x}\hat{u}+\hat{y}\hat{v})\}\mathrm{d}\hat{u}\mathrm{d}\hat{v} = \mathscr{F}^{-1}\{F(\hat{u},\hat{v})|J(\hat{u},\hat{v})|\}, \tag{7}$$

where the Jacobian is

$$J(\hat{u},\hat{v}) = \frac{\partial\alpha}{\partial\hat{u}}\frac{\partial\beta}{\partial\hat{v}} - \frac{\partial\alpha}{\partial\hat{v}}\frac{\partial\beta}{\partial\hat{u}} = \frac{1}{\hat{w}(\hat{u},\hat{v})}\left[(a_2a_6 - a_3a_5)\hat{u} + (a_3a_4 - a_1a_6)\hat{v}\right] + (a_1a_5 - a_2a_4). \tag{8}$$

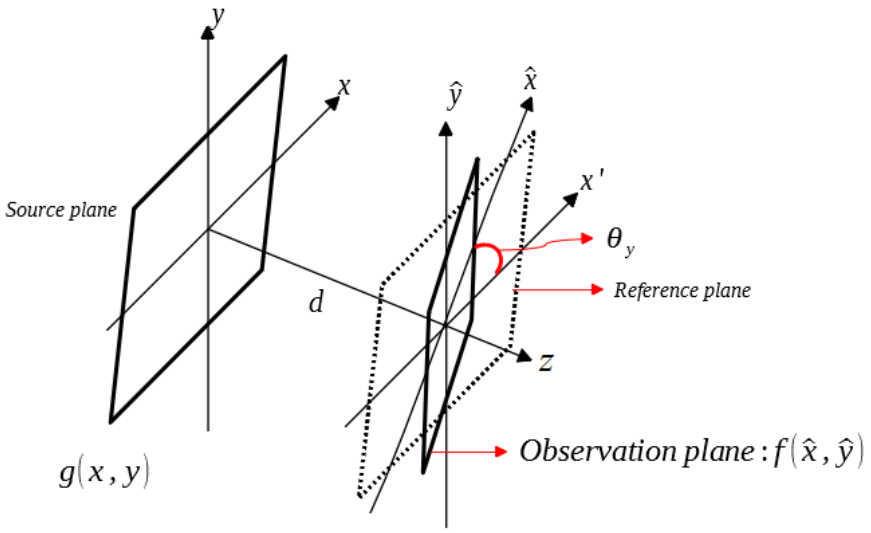


Figure 1. Optical scheme for the diffraction on a tilted plane.

3. DRPE Using Tilted Plane: Optical Image Encryption and Decryption Systems

The DRPE technique uses two RPMs in order to encrypt the information of the original image $f(x_1, y_1)$; the values of $f(x_1, y_1)$ are in the interval of [0, 1]. The two RPMs are represented by

$$r(x_1,y_1) = \exp\{i2\pi s(x_1,y_1)\}, \qquad h(x_2,y_2) = \exp\{i2\pi n(x_2,y_2)\}, \tag{9}$$

where x_1, y_1, x_2 and y_2 are spatial coordinates, $s(x_1, y_1)$ and $n(x_2, y_2)$ are normalized positive function generated randomly, independent statistically and their values are uniformly distributed in the interval of [0, 1] [1]. Figure 2 depicts the optical scheme based on the DRPE technique and the optical diffraction on two tilted planes.

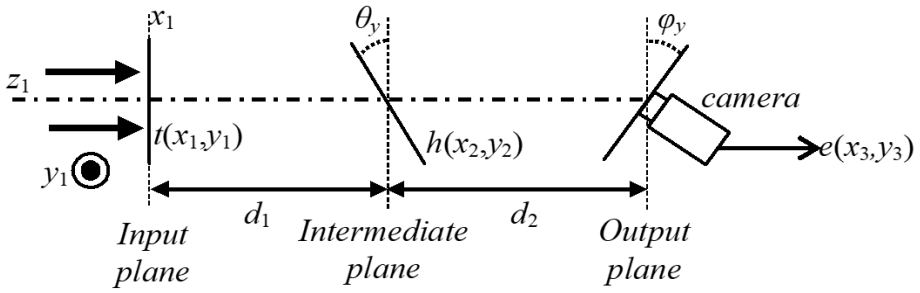


Figure 2. Optical scheme of the encryption system using the DRPE technique and the optical diffraction on two tilted planes.

The distribution $t(x_1, y_1)$ of the input plane of the encryption system of Figure 2 is composed by the original image $f(x_1, y_1)$ to encrypt placed against the RPM $r(x_1, y_1)$

$$t(x_1, y_1) = f(x_1, y_1) r(x_1, y_1) = f(x_1, y_1) \exp\{i2\pi s(x_1, y_1)\}. \tag{10}$$

The optical diffraction of the distribution $t(x_1, y_1)$ on the tilted plane placed at the distance d_1 with respect to the input plane of the encryption system is given by the distribution $p(x_2, y_2)$ and it is computed using the procedure described in Section 2. We use the following parameters and functions to compute $p(x_2, y_2)$

$$T_{d_1}(u, v) = \mathscr{F}\{t(x_1, y_1)\} \exp\left\{i2\pi d_1 \left(\lambda^{-2} - u^2 - v^2\right)^{1/2}\right\}, \tag{11}$$

$$\mathbf{T}_y^{-1}(\theta_y) = \begin{bmatrix} \cos\theta_y & 0 & \sin\theta_y \\ 0 & 1 & 0 \\ -\sin\theta_y & 0 & \cos\theta_y \end{bmatrix}, \tag{12}$$

$$u = \alpha(\hat{u}, \hat{v}) = \hat{u}\cos\theta_y + \hat{w}(\hat{u}, \hat{v})\sin\theta_y,\ v = \beta(\hat{u}, \hat{v}) = \hat{v},\ \hat{w}(\hat{u}, \hat{v}) = \left(\lambda^{-2} - \hat{u}^2 - \hat{v}^2\right)^{1/2}, \tag{13}$$

$$P(\hat{u}, \hat{v}) = T_d(\alpha(\hat{u}, \hat{v}), \beta(\hat{u}, \hat{v})) = T_d(\hat{u}\cos\theta_y + \hat{w}(\hat{u}, \hat{v})\sin\theta_y, \hat{v}), \tag{14}$$

$$p(x_2, y_2) = \int_{-\infty}^{+\infty}\int_{-\infty}^{+\infty} P(\hat{u}, \hat{v})|J(\hat{u}, \hat{v})| \exp\{i2\pi(x_2\hat{u} + y_2\hat{v})\} \mathrm{d}\hat{u}\mathrm{d}\hat{v} = \mathscr{F}^{-1}\{P(\hat{u}, \hat{v})|J(\hat{u}, \hat{v})|\}, \tag{15}$$

$$J(\hat{u}, \hat{v}) = \cos\theta_y - \frac{\sin\theta_y}{\hat{w}(\hat{u}, \hat{v})}\hat{u}. \tag{16}$$

The RPM $h(x_2, y_2)$ is multiplied by the image $p(x_2, y_2)$ with the purpose of obtaining the intermediate distribution $q(x_2, y_2) = h(x_2, y_2)p(x_2, y_2)$. The image $q(x_2, y_2)$ is optically tilted to the intermediate plane of the encryption system and the resulting image is the input for the second optical diffraction on the tilted plane placed at the distance d_2 with respect to the intermediate plane, which corresponds to the output plane of the encryption system. We apply again the approach described in Section 2 using the optically tilted distribution obtained from $q(x_2, y_2)$, the propagation distance d_2 and the rotation matrix $\mathbf{T}_y^{-1}(\varphi_y)$, in order to compute the encrypted image $e(x_3, y_3)$.

The RPM $h(x_2, y_2)$, the propagation distances d_1 and d_2, and the angles of the tilted planes θ_y and φ_y, are the security keys of the encryption system and the RPM $r(x_1, y_1)$ is used to spread the information content of the original image $f(x_1, y_1)$ onto the encrypted image $e(x_3, y_3)$ [1]. When the angles of the tilted planes are equal to $\theta_y = 0°$ and $\varphi_y = 0°$, the proposed encryption system in this work is reduced to the DRPE encryption system in the Fresnel domain [8].

The decryption system is performed by digital computations and it is computed in the reverse order of the encryption system using the encrypted image $e(x_3, y_3)$ and the method presented in Section 2 along with the following five security keys: the complex conjugated of the RPM $h(x_2, y_2)$, the propagation distances d_1 and d_2, and the two angles $-\theta_y$ and $-\varphi_y$. For the decryption system, the input and intermediate planes are tilted at an angle of $-\varphi_y$ and $-\theta_y$, respectively. The output plane of the decryption system is not tilted.

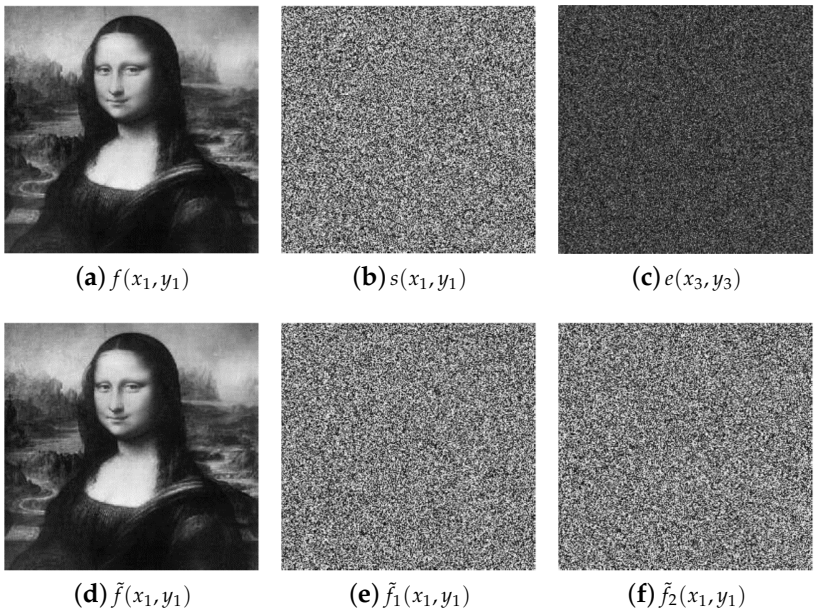
A second rotation around the x axis (θ_x or φ_x for the intermediate and output planes of the encryption system, respectively) produces a tilted plane with respect to the y axis and the method of Section 2 can be used in order to obtain the optical diffraction over the final tilted plane. The two new tilt angles θ_x and φ_x can be considered to be new security keys of the proposed encryption and decryption systems.

The results of the numerical simulations for the security system proposed in this section are shown in Figure 3. The original image $f(x_1, y_1)$ to encrypt and the random code image $s(x_1, y_1)$ of

the RPM $r(x_1, y_1)$ are depicted in Figure 3a,b, respectively. The random code image $n(x_2, y_2)$ of the RPM $h(x_2, y_2)$ has different values but the same appearance of the image shown in Figure 3b. The encrypted image $e(x_3, y_3)$ is presented in Figure 3c for the security keys: $d_1 = 200$ mm, $d_2 = 300$ mm, $\theta_y = 14.5^\circ$, $\varphi_y = 12.7^\circ$ and the RPM $h(x_2, y_2)$. This encrypted image is a noisy pattern that does not reveal any information of the original image $f(x_1, y_1)$. When the decryption system is performed using the encrypted image $e(x_3, y_3)$ and the five correct security keys (d_1, d_2, θ_y, φ_y and $h(x_2, y_2)$), the original image $f(x_1, y_1)$ is retrieved at the output plane of the decryption system. The decrypted image $\tilde{f}(x_1, y_1)$ is depicted in Figure 3d. We use the metric of the root mean square error (RMSE) between the decrypted images $\tilde{f}(x_1, y_1)$ and the original image $f(x_1, y_1)$

$$\text{RMSE} = \left(\frac{\sum_{x_1=1}^{M} \sum_{y_1=1}^{N} [f(x_1, y_1) - \tilde{f}(x, y)]^2}{\sum_{x_1=1}^{M} \sum_{y_1=1}^{N} [f(x_1, y_1)]^2} \right)^{\frac{1}{2}}, \tag{17}$$

with the purpose of evaluating the image quality of the decrypted images. The values of the RMSE metric to evaluate the image quality are values between 0 and 1; when the value of the RMSE is near or equal to 0, the image quality of the decrypted image is very good while the values of the RMSE near or equal to 1 represent a worse image quality of the decrypted image. The RMSE between the original image of Figure 3a and the decrypted image of Figure 3d is 0.027.



(a) $f(x_1, y_1)$ **(b)** $s(x_1, y_1)$ **(c)** $e(x_3, y_3)$

(d) $\tilde{f}(x_1, y_1)$ **(e)** $\tilde{f}_1(x_1, y_1)$ **(f)** $\tilde{f}_2(x_1, y_1)$

Figure 3. (**a**) Original image $f(x_1, y_1)$. (**b**) Random code image $s(x_1, y_1)$ of the RPM $r(x_1, y_1)$. (**c**) Encrypted image $e(x_3, y_3)$ for the security key $d_1 = 200$ mm, $d_2 = 300$ mm, $\theta_y = 14.5^\circ$, $\varphi_y = 12.7^\circ$ and the RPM $h(x_2, y_2)$ (**d**) Decrypted image $\tilde{f}(x_1, y_1)$ using the correct five security keys (d_1, d_2, θ_y, φ_y and $h(x_2, y_2)$). Decrypted images using the following wrong tilt angle in the decryption system: (**e**) $\theta_y = 14.4^\circ$ and (**f**) $\varphi_y = 12.8^\circ$.

The noisy images presented in Figure 3e,f correspond to the decrypted images when the wrong tilt angle $\theta_y = 14.4^\circ$ or $\varphi_y = 12.8^\circ$ are used in the decryption system, respectively. If the RPM $h(x_2, y_2)$ is wrong in the decryption system, the decrypted image obtained will be similar to the image shown in Figure 3e. The values of the RMSEs between the original image of Figure 3a and the decrypted images of Figure 3e,f are 0.91 and 0.87, respectively. When we use the correct values of the all five security keys in the decryption system, the properly retrieval of the original image at the output plane of the decryption system is possible.

We evaluate the sensitivity on the tilt angles θ_y and φ_y for the decrypted images by introducing small errors in these and leaving fixed the other three security keys (d_1, d_2 and $h(x_2, y_2)$) with their correct values in the decryption system. The RMSEs between the original image and the decrypted images are computed to measure the level of protection on the encrypted image. For this deviation test of the tilt angles on their correct values for the decryption process, it is introduced a small error that varies between -1×10^{-5} and 1×10^{-5} and then, for each variation is calculated the RMSE. We use the right value for the tilt angle φ_y when a small error is introduced for the tilt angle θ_y, and vice versa. From these numerical simulations, it was found that the tilt angles φ_y and θ_y are sensitive to a variation of 1×10^{-4} and $1 \times 10^{-3.5}$, respectively. The tilt angle φ_y is more sensitive than the tilt angle θ_y, because the first optical diffraction in the decryption system is from the tilted plane with a tilt angle $-\varphi_y$.

4. Conclusions

We have proposed a new version of the DRPE encryption and decryption system using the optical diffraction on two tilted planes. The new security keys given by the angles of the tilted planes, permits increase in the security of the encrypted image. The security of the presented system was also increased due to the nonlinearity introduced by the tilt of the intermediate and output planes of the proposed encryption system. The encryption and decryption systems have five security keys represented by two propagation distances, two tilt angles, and one RPM. All these security keys allow improvement to the security of the encrypted image against to the brute force and plaintext attacks. Finally, the retrieval of the original image at the output plane of the decryption system is only possible when the values of the five security keys for the decryption system are the same that were used in the encryption system.

Author Contributions: The work described in this article is the collaborative development of all authors. Conceptualization, J.M.V.O., C.J.J. and C.O.T.M.; Methodology, J.M.V.O., C.J.J. and C.O.T.M.; Software, J.M.V.O. and C.J.J.; Validation, C.O.T.M.; Investigation, J.M.V.O., C.J.J. and C.O.T.M.; Writing–original draft preparation, J.M.V.O. and C.J.J.; Writing–review and editing, J.M.V.O. and C.O.T.M.; Supervision, C.O.T.M.

Funding: This research has been funded by the Universidad de La Guajira (Riohacha) and the Universidad Popular del Cesar from Valledupar (Cesar).

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Réfrégier, P.; Javidi, B. Optical image encryption based on input plane and Fourier plane random encoding. *Opt. Lett.* **1995**, *20*, 767–769. [CrossRef] [PubMed]
2. Javidi, B.; Carnicer, A.; Yamaguchi, M.; Nomura, T.; Pérez-Cabré, E.; Millán, M.; Nishchal, N.; Torroba, R.; Barrera, J.; He, W.; et al. Roadmap on optical security. *J. Opt.* **2016**, *18*, 083001. [CrossRef]
3. Chen, W.; Javidi, B.; Chen, X. Advances in optical security systems. *Adv. Opt. Photonics* **2014**, *6*, 120–155. [CrossRef]
4. Millán, M.S.; Pérez-Cabré, E. Optical data encryption. In *Optical and Digital Image Processing: Fundamentals and Applications*; Cristóbal, G., Schelkens, P., Thienpont, H., Eds.; Wiley-VCH Verlag GmbH & Co.: Hoboken, NJ, USA, 2011; pp. 739–767.
5. Millán, M.S.; Pérez-Cabré, E.; Vilardy, J.M. Nonlinear techniques for secure optical encryption and multifactor authentication. In *Advanced Secure Optical Image Processing for Communications*; Al Falou, A., Ed.; IOP Publishing: Bristol, UK, 2018; pp. 8-1–8-33.
6. Goodman, J.W. *Introduction to Fourier Optics*; McGraw-Hill: New York, NY, USA, 1996.
7. Matoba, O.; Javidi, B. Encrypted optical memory system using three-dimensional keys in the Fresnel domain. *Opt. Lett.* **1999**, *24*, 762–764. [CrossRef] [PubMed]
8. Situ, G.; Zhang, J. Double random phase encoding in the Fresnel domain. *Opt. Lett.* **2004**, *29*, 1584–1586. [CrossRef] [PubMed]

9. Unnikrishnan, G.; Joseph, J.; Singh, K. Optical encryption by double-random phase encoding in the fractional Fourier domain. *Opt. Lett.* **2000**, *25*, 887–889. [CrossRef] [PubMed]
10. Matsushima, K. Formulation of the rotational transformation of wave fields and their application to digital holography. *App. Opt.* **2008**, *47*, D110–D116. [CrossRef] [PubMed]