sensors

MDPI

Article

Nonlinear Encryption for Multiple Images Based on a Joint Transform Correlator and the Gyrator Transform

Ronal A. Perez [1], Juan M. Vilardy [1,*], Elisabet Pérez-Cabré [2], María S. Millán [2] and Cesar O. Torres [3]

[1] Grupo de Investigación en Física del Estado Sólido (GIFES), Faculty of Basic and Applied Sciences, Universidad de La Guajira, Riohacha 440007, La Guajira, Colombia
[2] Applied Optics and Image Processing Group, Universitat Politècnica de Catalunya · BarcelonaTech, 08222 Terrassa, Barcelona, Spain
[3] Grupo de Óptica e Informática, Department of Physics, Universidad Popular del Cesar, Valledupar 200001, Cesar, Colombia
* Correspondence: jmvilardy@uniguajira.edu.co; Tel.: +57-605-584-3596

Abstract: A novel nonlinear encryption–decryption system based on a joint transform correlator (JTC) and the Gyrator transform (GT) for the simultaneous encryption and decryption of multiple images in grayscale is proposed. This security system features a high level of security for the single real-valued encrypted image and a high image quality for the multiple decrypted images. The multispectral or color images are considered as a special case, taking each color component as a grayscale image. All multiple grayscale images (original images) to encrypt are encoded in phase and placed in the input plane of the JTC at the same time without overlapping. We introduce two random-phase masks (RPMs) keys for each image to encrypt at the input plane of the JTC-based encryption system. The total number of the RPM keys is given by the double of the total number of the grayscale images to be encrypted. The use of several RPMs as keys improves the security of the encrypted image. The joint Gyrator power distribution (JGPD) is the intensity of the GT of the input plane of the JTC. We obtain only a single real-valued encrypted image with a high level of security for all the multiple grayscale images to encrypt by introducing two new suitable nonlinear modifications on the JGPD. The security keys are given by the RPMs and the rotation angle of the GT. The decryption system is implemented by two successive GTs applied to the encrypted image and the security keys given by the RPMs and considering the rotation angle of the GT. We can simultaneously retrieve the various information of the original images at the output plane of the decryption system when all the security keys are correct. Another result due to the appropriate definition of the two nonlinear operations applied on the JGPD is the retrieval of the multiple decrypted images with a high image quality. The numerical simulations are computed with the purpose of demonstrating the validity and performance of the novel encryption–decryption system.

Keywords: optical multiple-image encryption–decryption system; joint transform correlator (JTC); Gyrator transform; multispectral images; nonlinear image processing

Citation: Perez, R.A.; Vilardy, J.M.; Pérez-Cabré, E.; Millán, M.S.; Torres, C.O. Nonlinear Encryption for Multiple Images Based on a Joint Transform Correlator and the Gyrator Transform. *Sensors* **2023**, *23*, 1679. https://doi.org/10.3390/s23031679

Academic Editors: Manuel Filipe P. C. M. Costa, Orlando Frazão and Rogerio Nogueira

Received: 30 November 2022
Revised: 27 January 2023
Accepted: 29 January 2023
Published: 3 Febraury 2023

1. Introduction

The research field of optical image encryption has shown an intense development due to the advantages provided by the optical processing systems, such as a high parallel processing capacity, an ultrafast computing speed and the wide variety of controllable physical parameters of these optical systems, and also because of the several applications in optical security published in the last years [1–7]. The most known optical technique for image encryption is the double random-phase encoding (DRPE) proposed by Réfrégier and Javidi [8]. The DRPE can be optically implemented using a classical 4*f*-processor [9] or a joint transform correlator (JTC) [10]. The image to encrypt by the optical DRPE is converted into a stationary white noise image (encrypted image) by using two random-phase masks (RPMs). Initially, the DRPE was proposed in the Fourier domain using the 4*f*-processor.

Later, the DRPE was extended from the Fourier domain to the Fresnel domain [11], the fractional Fourier domain (FrFD) [12] and the Collins diffraction domain [13], with the purpose of increasing the security of the DRPE technique.

Nowadays, the DRPE is implemented by using a JTC architecture [1,4–7,10,14–17] due to the following advantages: the compact size of the experimental setup, a less strict setup alignment requirement, the encrypted image is a real-valued distribution and the security key used in the encryption system is exactly the same to be used in the decryption system. The first implementations of the DRPE using a JTC architecture were proposed in the Fourier domain. The DRPE implemented with a JTC architecture was also extended from the Fourier domain to the Fresnel domain [18–20], the FrFD [21–24], the Gyrator domain (GD) [25,26] and the Collins diffraction domain [27] in order to either simplify the experimental setup and/or to increase the security of the encryption system.

The security of the optical architectures that implement the DRPE based on a 4*f*-processor were analyzed and it was shown that these optical implementations are vulnerable to chosen-plaintext attacks (CPA) [28,29], known-plaintext attacks (KPA) [29,30] and ciphertext-only attacks (COA) [31]. The linear property of the 4*f*-processor is the main reason for these vulnerabilities of the DRPE technique [29]. Some papers have proved that the optical DRPE implemented by using a JTC architecture is also vulnerable to CPA [32], KPA [33,34] and COA [35]. The initial JTC architecture used to implement the DRPE was nonlinear modified and extended to several optical processing domains in order to improve the security of the encryption system and the quality of the decrypted image [15–27]. The encryption–decryption system based on a nonlinear JTC in the GD has shown a higher sensitivity for the rotation angle of the GT with respect to the resulting decrypted images in comparison to the sensitivity for the fractional order of the encryption–decryption system based on a nonlinear JTC in the FrFD [26]. The rotation angle of the GT can be considered as a security key of the encryption system. Therefore, the nonlinear JTC-based encryption system in the GD can be considered more secure with respect to other encryption systems that use other optical processing domains.

The optical DRPE was originally designed to encrypt either a single binary or grayscale image [8]. Later, the DRPE based on the 4*f*-processor was used to perform color image encryption [36,37]. Some implementations to encrypt color images by using the DRPE on a JTC were presented in [21,38]. The multiple-image encryption (for instance, various frames of a video sequence) by using an optical JTC architecture was also presented in some contributions [39,40]. These optical color image and multiple-image encryption systems use different input illumination wavelengths and several key codes or RPMs that can be utilized as new security keys to improve the security level of the encryption system. Optical encryption methods recently included the ability to cipher multiple images [41–47]. In general, this approach achieves a higher level of security because two or more pieces of information are encoded in the encryption procedure, and their decryption allows for the validation of more than one signal, unlike the first systems that dealt with a unique primary image. Different techniques were explored to achieve a successful multiple-image optical encryption and decryption. For instance, reference [41] presents a multiple-image encryption system based on a linear JTC in the Fourier domain. In [42], a modified iterative phase retrieval algorithm with a structured phase mask was used in the Fresnel domain to encrypt multiple images. Reference [43] implements a multiple-image encryption method by using phase jump gradient factors based on orbital angular momentum and multiplexing holography. Recently, a multiple-image compression, encryption and reconstruction scheme based on deep learning-assisted single-pixel imaging and orthogonal coding was presented in [44]. A sequential multiple-image encryption based on quick response (QR) codes and a modified DRPE in the FrFD was developed in [45], where each image to encrypt was converted into a QR and then this converted image was encrypted. The multiple-image encryption system in [46] was based on the optical interference by wavelength multiplexing in the Fresnel domain in order to generate two encrypted images. A nonlinear multiple-

image encryption method was described in [47] by using optical scanning holography with a random-phase mask (RPM) and orthogonal compressive sensing.

This paper aims to propose a novel approach to multiple-image encryption with several differences with respect to the previously reported works. We propose a nonlinear JTC-based encryption system in the GD to encrypt multiple images in grayscale. The color or multispectral images are considered as a special case, taking each color or spectral component as a grayscale image. We present a modification of the nonlinear JTC-based encryption system proposed in [26] with the purpose of achieving the simultaneous encryption of multiple grayscale images. All the multiple grayscale images to encrypt are encoded in phase and placed in the input plane of the JTC without overlapping. We introduce a new RPM key for each image to encrypt. The total number of the RPM keys is given by the double of the total number of the grayscale images to be encrypted. The use of several RPMs as keys improves the security of the encrypted image. The joint Gyrator power distribution (JGPD) is the intensity of the Gyrator transform (GT) of the input plane of the JTC. The single real-valued encrypted image is computed by using two new nonlinear terms applied to the JGPD. The proposed multiple-image encryption system based on a nonlinear JTC in the GD retains the following advantages of the security system proposed in [26]: the improved quality of the decrypted images; shift-invariance property with respect to the lateral displacements of the RPM key in the decryption process and the retrieval of the primary images; an additional key given by the value of the rotation angle of the GT; the use of a simplified JTC in the GD that avoids the beam splitting required by other optical JTC implementations; and there is not a significant increase in the amount of information to be transmitted because the resulting encrypted function has the same size as its original version.

The proposed encryption technique allows a fast encryption time in comparison to previous proposals that sequentially encrypt multiple grayscale images [39,40]. This is because we simultaneously encrypt all the primary images, and the optical schematic of the encryption system is performed thrice in order to obtain only a single encrypted image with the hidden information of the whole set of images to encrypt (in the following example, it is up to eight signals). The multiple grayscale images encryption system of this work shows an improved security over the encrypted distribution because the nonlinear modifications of the JTC architecture in the GD depend on the number and the values of the RPM keys utilized for the encryption process. Finally, the proposed security system allows a simultaneous encryption and decryption of multiple images with a high level of security for the single real-valued encrypted image and a retrieval with a high image quality for the multiple decrypted images, due to the phase encoding of the multiple images to encrypt and the two new nonlinear operations applied on the JGPD. We point out that these two nonlinear terms are specially designed for a satisfactory multiple-image encryption and decryption, and they differ from the nonlinear modifications presented in [26].

2. Multiple-Image Encryption System Based on a Nonlinear JTC Architecture and the Gyrator Transform

2.1. Encryption Scheme

In this section, we describe the encryption scheme using the equations of a nonlinear JTC architecture in the GD [26], with the purpose of encrypting p grayscale images. Each grayscale image to be encrypted is denoted by a real-valued function $f_j(x,y)$ with values in the interval [0, 1] and $j = 1, 2, 3, \ldots, p$; each grayscale image is encoded in phase

$$f_{j,Ph}(x,y) = \exp\{i2\pi f_j(x,y)\}. \tag{1}$$

We use two different RPMs, $r_j(x,y)$ and $h_j(x,y)$, for each grayscale image to encrypt. These two RPMs are defined by

$$r_j(x,y) = \exp\{i2\pi s_j(x,y)\}, \quad h_j(x,y) = \exp\{i2\pi n_j(x,y)\}, \tag{2}$$

where $s_j(x,y)$ and $n_j(x,y)$ are normalized positive functions randomly generated, statistically independent and uniformly distributed in the interval [0, 1]. The functions $f_j(x,y)$, $s_j(x,y)$ and $n_j(x,y)$ are grayscale images with $M \times N$ pixel size. We define the new function $g_j(x,y) = f_{j,Ph}(x,y)r_j(x,y)$ given by a grayscale image encoded in phase $f_{j,Ph}(x,y)$ bonded to an RPM $r_j(x,y)$, with the purpose of simplifying the following equations.

The input plane of the JTC is composed of two non-overlapping data distributions for each grayscale image to be encrypted. These two data distributions are the new function $g_j(x,y)$ and the RPM $h_j(x,y)$ placed anti-symmetrically side by side at the input plane of the JTC by means of the generalized shift operators $\mathrm{GS}_{a_j,b_j;\alpha}$ and $\mathrm{GS}_{-a_j,-b_j;\alpha}$, respectively, where a_j and b_j are real values and α is the rotation angle of the GT operator. The operators of GT and generalized shift are described in Appendixes A and B, respectively. The values of a_j and b_j are the central points of each data distribution $g_j(x,y)$ and we define a_j and b_j proportionally to $N/2$ and $M/2$ depending on the location of each function $g_j(x,y)$. The distributions contained in the input plane of the JTC for all the grayscale images to be encrypted are depicted in Figure 1. The GT at parameter α of the distributions $g_j(x,y)$ and $h_j(x,y)$ are denoted by $g_{j,\alpha}(u,v) = \mathscr{G}^{\alpha}\{g_j(x,y)\}$ and $h_{j,\alpha}(u,v) = \mathscr{G}^{\alpha}\{h_j(x,y)\}$, respectively.

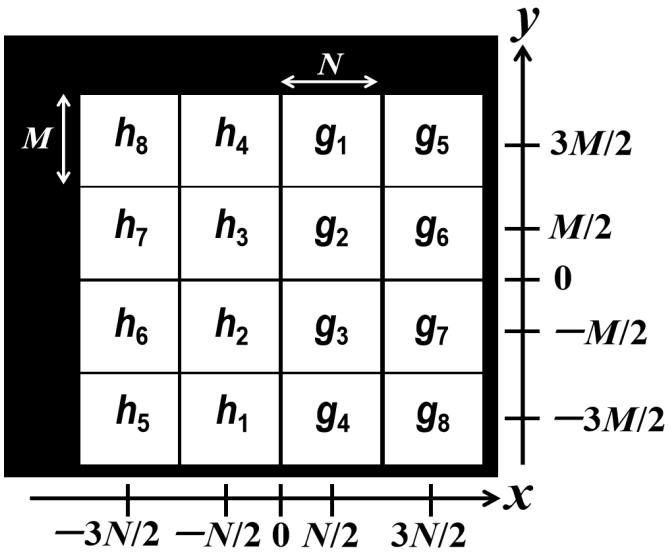


Figure 1. Data distributions placed at the input plane of the JTC for the $p = 8$ grayscale images to be encrypted. The values of a_j and b_j with $j = 1, 2, \ldots, 8$ for this figure are $a_1 = a_2 = a_3 = a_4 = N/2$, $a_5 = a_6 = a_7 = a_8 = 3N/2$, $b_1 = b_5 = 3M/2$, $b_2 = b_6 = M/2$, $b_3 = b_7 = -M/2$ and $b_4 = b_8 = -3M/2$.

Therefore, the input plane of the JTC-based encryption scheme for all the p grayscale images to be encrypted is

$$\begin{aligned} t(x,y) &= \sum_{j=1}^{p} \left\{ \mathrm{GS}_{a_j,b_j;\alpha}\left[g_j(x,y)\right] + \mathrm{GS}_{-a_j,-b_j;\alpha}\left[h_j(x,y)\right] \right\} \\ &= \sum_{j=1}^{p} \left\{ \exp\left\{ -i2\pi \left[b_j\left(x - \frac{a_j}{2}\right) + a_j\left(y - \frac{b_j}{2}\right) \right] \cot\alpha \right\} g_j(x - a_j, y - b_j) \right. \\ &\quad \left. + \exp\left\{ i2\pi \left[b_j\left(x + \frac{a_j}{2}\right) + a_j\left(y + \frac{b_j}{2}\right) \right] \cot\alpha \right\} h_j(x + a_j, y + b_j) \right\}. \end{aligned} \tag{3}$$

Equation (3) is mathematically compact due to the chosen location of each data distribution in the input plane of the JTC (Figure 1). Other ways of placing the data distributions at the input plane of the JTC would be possible, but the resulting mathematical expression

of Equation (3) would be longer and more complicated. The JGPD at parameter α for Equation (3) is the intensity of the GT of the input plane of the JTC given by [26]

$$\begin{aligned}\mathrm{JGPD}_\alpha(u,v) &= |\mathscr{G}^\alpha\{t(x,y)\}|^2 = \left|\sum_{j=1}^{p}\mathscr{G}^\alpha\left\{\mathrm{GS}_{a_j,b_j;\alpha}[g_j(x,y)]+\mathrm{GS}_{-a_j,-b_j;\alpha}[h_j(x,y)]\right\}\right|^2\\ &= \left[\sum_{j=1}^{p}\left\{e^{-T_j}g_{j,\alpha}(u,v)+e^{T_j}h_{j,\alpha}(u,v)\right\}\right]\left[\sum_{k=1}^{p}\left\{e^{T_k}g^*_{k,\alpha}(u,v)+e^{-T_k}h^*_{k,\alpha}(u,v)\right\}\right]\\ &= \sum_{j=1}^{p}\sum_{k=1}^{p}\{e^{-T_j+T_k}g_{j,\alpha}(u,v)g^*_{k,\alpha}(u,v)+e^{T_j-T_k}h_{j,\alpha}(u,v)h^*_{k,\alpha}(u,v)\\ &\quad+e^{T_j+T_k}g^*_{k,\alpha}(u,v)h_{j,\alpha}(u,v)+e^{-T_j-T_k}g_{j,\alpha}(u,v)h^*_{k,\alpha}(u,v)\},\end{aligned} \tag{4}$$

where the variables u and v are the output coordinates in the GD, $T_j = i2\pi(b_j u + a_j v)\csc\alpha$, $T_k = i2\pi(b_k u + a_k v)\csc\alpha$ and the superscript * denotes the complex conjugation operation. The JGPD is a positive real-valued distribution and it has $4p^2$, being p the total number of original images to encrypt. The four general terms of the double summation in Equation (4) are composed of the multiplication of different pure linear phase terms and the products between the data distributions $g_{j,\alpha}(u,v)$ and $g^*_{k,\alpha}(u,v)$, $h_{j,\alpha}(u,v)$ and $h^*_{k,\alpha}(u,v)$, $g^*_{k,\alpha}(u,v)$ and $h_{j,\alpha}(u,v)$, and $g_{j,\alpha}(u,v)$ and $h^*_{k,\alpha}(u,v)$, respectively. We define the intensities $I_1(u,v)$ and $I_2(u,v)$ as

$$\begin{aligned}I_1(u,v) &= \left|\sum_{j=1}^{p}\mathscr{G}^\alpha\left\{\mathrm{GS}_{a_j,b_j;\alpha}[g_j(x,y)]\right\}\right|^2 = \sum_{j=1}^{p}\sum_{k=1}^{p}e^{-T_j+T_k}g_{j,\alpha}(u,v)g^*_{k,\alpha}(u,v),\\ I_2(u,v) &= \left|\sum_{j=1}^{p}\mathscr{G}^\alpha\left\{\mathrm{GS}_{-a_j,-b_j;\alpha}[h_j(x,y)]\right\}\right|^2 = \sum_{j=1}^{p}\sum_{k=1}^{p}e^{T_j-T_k}h_{j,\alpha}(u,v)h^*_{k,\alpha}(u,v).\end{aligned} \tag{5}$$

The specific location of each data distribution depicted in Figure 1 for the input plane of the JTC allows an easy computation of the intensities $I_1(u,v)$ and $I_2(u,v)$ defined in Equation (5) by using a GT implemented optically or numerically. The next step in the encryption scheme is to subtract the intensities $I_1(u,v)$ and $I_2(u,v)$ from the JGPD. Then, the previous modification of the JGPD is divided by the intensity $I_2(u,v)$ with the purpose of obtaining the encrypted image

$$\begin{aligned}e_\alpha(u,v) &= \frac{\mathrm{JGPD}_\alpha(u,v)-I_1(u,v)-I_2(u,v)}{I_2(u,v)}\\ &= \frac{1}{I_2(u,v)}\sum_{j=1}^{p}\sum_{k=1}^{p}\left\{e^{T_j+T_k}g^*_{k,\alpha}(u,v)h_{j,\alpha}(u,v)+e^{-T_j-T_k}g_{j,\alpha}(u,v)h^*_{k,\alpha}(u,v)\right\}.\end{aligned} \tag{6}$$

The encrypted image $e_\alpha(u,v)$ is a real-valued distribution that has $2p^2$ terms and it is computed from the following three intensities: $\mathrm{JGPD}_\alpha(u,v)$, $I_1(u,v)$ and $I_2(u,v)$. The two general terms of the double summation in Equation (6) are noisy data distributions that represent the DRPE in the GD for all the original images to encrypt along with the $2p$ RPMs, $r_j(x,y)$ and $h_j(x,y)$. Figure 2 shows the optical encryption scheme (part I) based on a fully phase nonzero-order JTC architecture in the GD and the optical decryption scheme (part II) based on two successive GTs. The security keys of the encryption scheme are the $2p$ RPMs $r_j(x,y)$ and $h_j(x,y)$ and the rotation angle of the GT operator. The RPM $r_j(x,y)$ is used to spread the information content of each grayscale image $f_j(x,y)$ encoded in phase onto the encrypted distribution $e_\alpha(u,v)$.

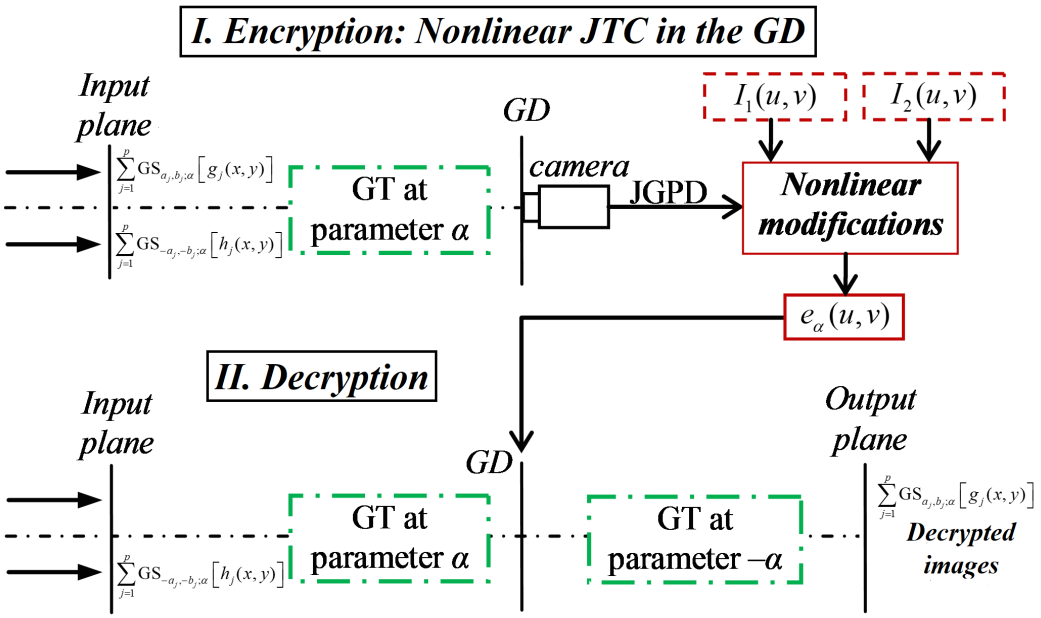


Figure 2. Schematic representation of the optical setup. The encryption scheme is based on a JTC in the GD and the decryption scheme is composed of two successive GTs.

2.2. Decryption Scheme

In the decryption scheme (Figure 2, part II), the p RPMs $h_l(x,y)$ are placed at the input plane of the decryption scheme by using the generalized shift operators $\mathrm{GS}_{-a_l,-b_l;\alpha}$. Then, the encrypted image $e_\alpha(u,v)$ located in the GD is multiplied by the GT of the input plane of the decryption scheme and the result is

$$\begin{aligned} d_\alpha(u,v) &= e_\alpha(u,v)\sum_{l=1}^{p}\mathscr{G}^\alpha\{\mathrm{GS}_{-a_l,-b_l;\alpha}[h_l(x,y)]\} = e_\alpha(u,v)\sum_{l=1}^{p}e^{T_l}h_{l,\alpha}(u,v) \\ &= \frac{1}{I_2(u,v)}\sum_{j=1}^{p}\sum_{k=1}^{p}\sum_{l=1}^{p}\{e^{T_j+T_k+T_l}g^*_{k,\alpha}(u,v)h_{j,\alpha}(u,v)h_{l,\alpha}(u,v) \\ &\quad + e^{-T_j-T_k+T_l}g_{j,\alpha}(u,v)h^*_{k,\alpha}(u,v)h_{l,\alpha}(u,v)\}, \end{aligned} \tag{7}$$

where $T_l = i2\pi(b_l u + a_l v)\csc\alpha$ and this equation has $2p^3$ terms. The two general terms of the triple summation in Equation (7) are composed of the multiplication of different pure linear phase terms and the products between the data distributions $g^*_{k,\alpha}(u,v)$, $h_{j,\alpha}(u,v)$ and $h_{l,\alpha}(u,v)$, and $g_{j,\alpha}(u,v)$, $h^*_{k,\alpha}(u,v)$ and $h_{l,\alpha}(u,v)$, respectively. Each general term of this triple summation is divided by the nonlinear term $I_2(u,v)$. The first general term of Equation (7) corresponds to different noisy data distributions at the output plane of the decryption system, and the second general term of Equation (7) allows the separation of the data distribution $g_{j,\alpha}(u,v)$ from the product given by the multiplication of the data distributions $g_{j,\alpha}(u,v)$, $h^*_{k,\alpha}(u,v)$ and $h_{l,\alpha}(u,v)$, when $l=j$. The output plane of the decryption scheme is given by the GT at parameter $-\alpha$ of Equation (7). The resulting output plane has several distributions spatially separated. The second term of the triple sum on the right side of Equation (7) retains the most relevant information in order to retrieve the p grayscale images that were encrypted. The p decrypted grayscale images are centered at coordinates (a_j,b_j) and the other distributions in the output plane of the decryption scheme are spatially separated distributions from these p decrypted grayscale images. Therefore, the GT at parameter $-\alpha$ of the second term of the triple sum on the right side of Equation (7) is

$$\hat{d}(x,y) = \mathscr{G}^{-\alpha}\left\{\frac{\left[\sum_{j=1}^{p} e^{-T_j} g_{j,\alpha}(u,v)\right]\left[\sum_{l=1}^{p}\sum_{k=1}^{p} e^{T_l - T_k} h_{l,\alpha}(u,v) h^*_{k,\alpha}(u,v)\right]}{\sum_{j=1}^{p}\sum_{k=1}^{p} e^{T_j - T_k} h_{j,\alpha}(u,v) h^*_{k,\alpha}(u,v)}\right\}$$
$$= \sum_{j=1}^{p} \mathrm{GS}_{a_j,b_j;\alpha}\left[g_j(x,y)\right], \tag{8}$$

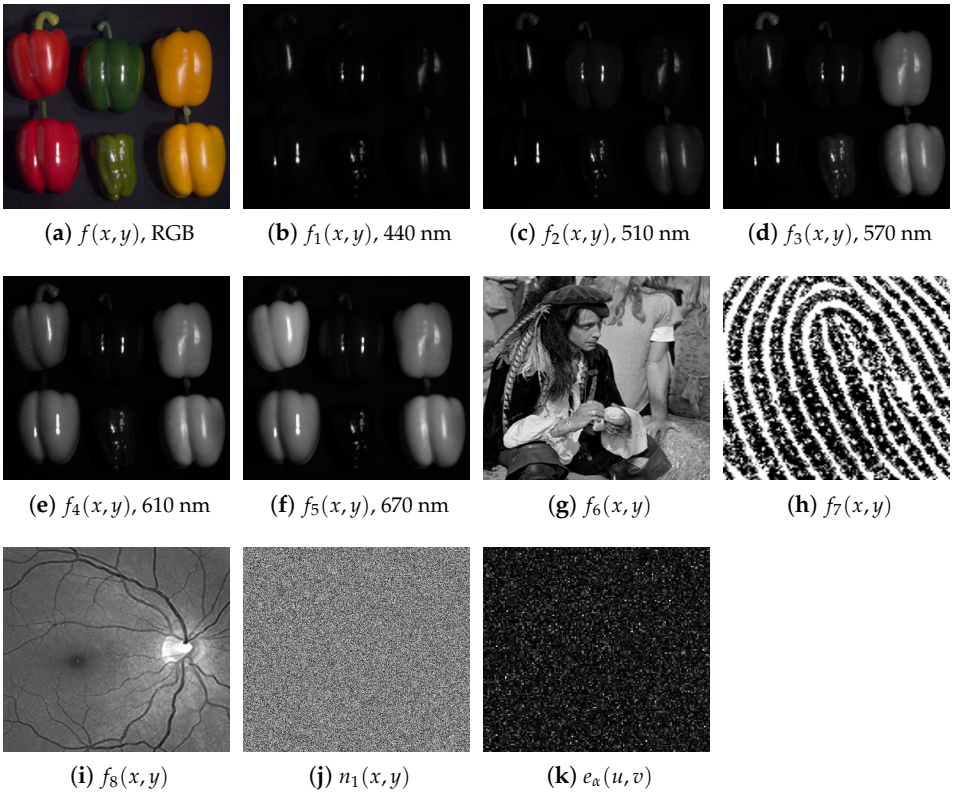
the result of this equation is obtained when $-a_l = -a_j$, $-b_l = -b_j$ and $l = j$. Each term of the Equation (8) is multiplied by a linear phase term and the complex conjugate of $r_j(x - a_j, y - b_j)$ in order to obtain a version of the decrypted grayscale image $\hat{f}_j(x,y)$ at coordinate (a_j, b_j) given by

$$2\pi\hat{f}_j(x - a_j, y - b_j) = \arg\left\{\exp\left\{i2\pi\left[b_j\left(x - \frac{a_j}{2}\right) + a_j\left(y - \frac{b_j}{2}\right)\right]\cot\alpha\right\}\right.$$
$$\left.\times\, \mathrm{GS}_{a_j,b_j;\alpha}\left[g_j(x,y)\right] r^*_j(x - a_j, y - b_j)\right\}, \tag{9}$$

where arg is the phase of a complex-valued function. If the p keys RPMs $h_j(x,y)$ and the key RPM $r_j(x,y)$ applied in the decryption scheme are the same keys used in the encryption system, the decrypted grayscale image $\hat{f}_j(x,y)$ is a replica of the grayscale image $f_j(x,y)$ that was encrypted. The nonlinear modifications of the JGPD at the output plane of the encryption scheme allow obtaining a correct retrieval of the original grayscale image in the decryption scheme.

3. Numerical Simulations

In this section, we compute the numerical simulations of the encryption and decryption schemes for multiple images presented in Section 2. The resolution of the grayscale images used in these numerical simulations is 512×512 pixels ($M = N = 512$). The images in Figure 3 show the results for the encryption scheme described in Section 2.1. We have selected eight original grayscale images to encrypt ($j = 1, 2, 3, ..., 8$ and $p = 8$). These images have different details and frequency spectra, and they could be used for different purposes. The first five grayscale images correspond to a multispectral image of peppers; each color component of this multispectral image is processed as a grayscale image. The original image related to the multispectral image of peppers in the RGB color space is shown in Figure 3a, and the five grayscale images $f_j(x,y)$ at $j = 1, 2, 3, 4, 5$ taken from the multispectral image are depicted in Figure 3b–f. These first five grayscale images were taken from [48]. The five color (wavelength, λ) channels captured for the multispectral image of peppers are $f_1(x,y)$ at $\lambda = 440$ nm, $f_2(x,y)$ at $\lambda = 510$ nm, $f_3(x,y)$ at $\lambda = 570$ nm, $f_4(x,y)$ at $\lambda = 610$ nm and $f_5(x,y)$ at $\lambda = 670$ nm. The remaining three original grayscale images to encrypt correspond to the photo of a person and two biometric signals given by the images of a fingerprint and a retina. These last three original grayscale images are displayed in Figure 3g–i. The image for the random code $n_1(x,y)$ of the RPM $h_1(x,y)$ is presented in Figure 3j. The random codes $s_j(x,y)$ of the RPMs $r_j(x,y)$ and $n_j(x,y)$ of the RPM $h_j(x,y)$ with $j \neq 1$ have different values but a similar appearance to the random code $n_1(x,y)$. The encrypted image $e_\alpha(u,v)$ for the rotation angle $\alpha = 0.775\pi$ is shown in Figure 3k, which is a noisy distribution that does not reveal any information of the original images $f_j(x,y)$. The security keys of the encryption scheme are represented by the sixteen RPMs ($r_j(x,y)$ and $h_j(x,y)$) and the rotation angle of the GT operator.



(a) $f(x,y)$, RGB **(b)** $f_1(x,y)$, 440 nm **(c)** $f_2(x,y)$, 510 nm **(d)** $f_3(x,y)$, 570 nm

(e) $f_4(x,y)$, 610 nm **(f)** $f_5(x,y)$, 670 nm **(g)** $f_6(x,y)$ **(h)** $f_7(x,y)$

(i) $f_8(x,y)$ **(j)** $n_1(x,y)$ **(k)** $e_\alpha(u,v)$

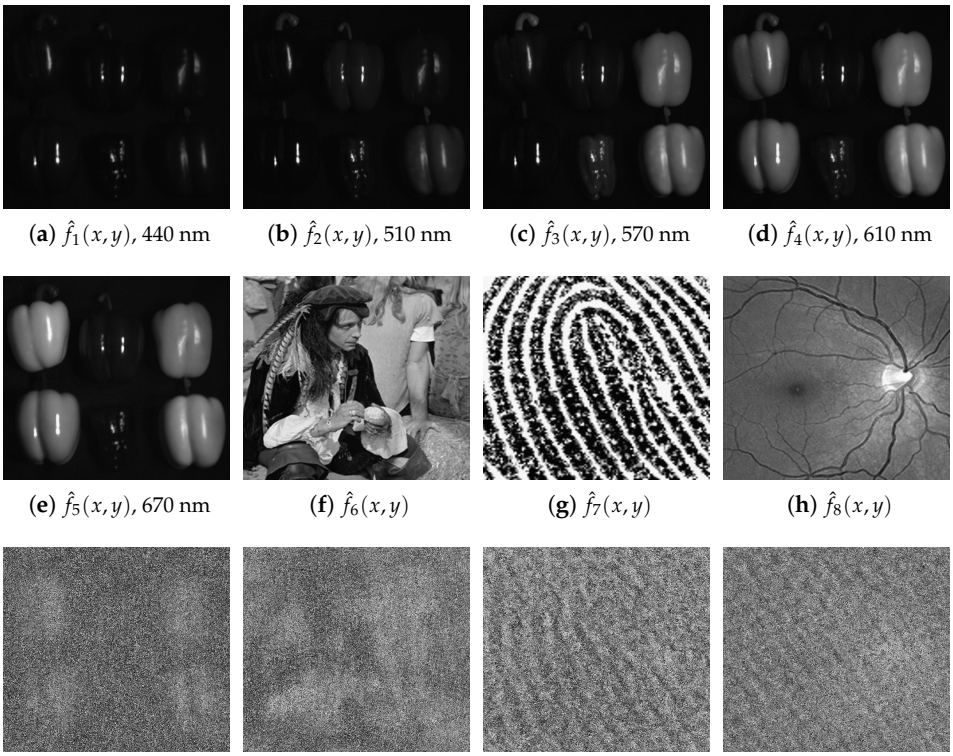
Figure 3. (**a**) Original image $f(x,y)$ in the RGB color space. Multispectral image to encrypt corresponding to $f(x,y)$ with five different color (wavelength, λ) channels: (**b**) $f_1(x,y)$ at $\lambda = 440$ nm, (**c**) $f_2(x,y)$ at $\lambda = 510$ nm, (**d**) $f_3(x,y)$ at $\lambda = 570$ nm, (**e**) $f_4(x,y)$ at $\lambda = 610$ nm and (**f**) $f_5(x,y)$ at $\lambda = 670$ nm. Color image $f(x,y)$ and its multispectral components were obtained from [48]. The remaining original grayscale images to encrypt: (**g**) $f_6(x,y)$, (**h**) $f_7(x,y)$ and (**i**) $f_8(x,y)$. (**j**) Image of the random distribution $n_1(x,y)$ of the RPM $h_1(x,y)$. (**k**) Encrypted image $e_\alpha(u,v)$ for the rotation angle $\alpha = 0.775\pi$.

Initially for the decryption computation, we use the same values of the security keys given by the sixteen RPMs ($r_j(x,y)$ and $h_j(x,y)$) and the rotation angle of the GT operator, which were used in the encryption computation. Therefore, the right decrypted images $\hat{f}_j(x,y)$, which are replicas of the original images $f_j(x,y)$, are displayed in Figure 4a–h. If a wrong security key, for instance, the RPM $h_7(x,y)$, and the other sixteen correct security keys (the remaining fifteen RPMs and the rotation angle of the GT operator) are used in the decryption scheme, we obtain the noisy decrypted images depicted in Figure 4i–l. For the last numerical simulation, the decrypted images $\hat{f}_j(x,y)$ with $j = 1,2,3,4$ are also noisy random distributions with a similar appearance to the decrypted image shown in Figure 4i. When another security key different from the RPM $h_7(x,y)$ is wrong for the decryption computation, we will also obtain noisy decrypted images very similar to the distributions displayed in Figure 4i–l. If the new nonlinear terms $I_1(u,v)$ and/or $I_2(u,v)$ defined in Equation (5) were not applied to compute the encrypted image of Equation (6) or the definitions of these two nonlinear terms were different from those in Equation (5), we would obtain multiple noisy decrypted images very alike to the images depicted in Figure 4i–l. Thus, the correct simultaneous retrieval of the original images at the output plane of the decryption scheme is only possible when all the security keys have the same values for the encryption and decryption computations, and the two nonlinear terms $I_1(u,v)$ and $I_2(u,v)$ of Equation (5) are applied in the definition of the encrypted image given by Equation (6).

The most used metric to evaluate the quality of the decrypted images is the root mean square error (RMSE), which is defined by [15]

$$\mathrm{RMSE} = \left(\frac{\sum_{x=1}^{M} \sum_{y=1}^{N} [f(x,y) - \hat{f}(x,y)]^2}{\sum_{x=1}^{M} \sum_{y=1}^{N} [f(x,y)]^2} \right)^{\frac{1}{2}}. \tag{10}$$

On the one hand, the RMSE values close or equal to 0 correspond to decrypted images very similar to the original ones, thus indicating a good image quality for the retrieved signal. On the other hand, the RMSE values close to 1 usually correspond to noisy decrypted signals that do not resemble the original images. The RMSEs between the original images $f_j(x,y)$ of Figure 3b–i, and the right decrypted images of Figure 4a–h are values between 0.015 and 0.047. Finally, the RMSEs between the original images $f_j(x,y)$ of Figure 3f–i and the undisclosed decrypted images of Figure 4i–l are values between 0.817 and 0.924.



(a) $\hat{f}_1(x,y)$, 440 nm **(b)** $\hat{f}_2(x,y)$, 510 nm **(c)** $\hat{f}_3(x,y)$, 570 nm **(d)** $\hat{f}_4(x,y)$, 610 nm

(e) $\hat{f}_5(x,y)$, 670 nm **(f)** $\hat{f}_6(x,y)$ **(g)** $\hat{f}_7(x,y)$ **(h)** $\hat{f}_8(x,y)$

(i) Undisclosed $\hat{f}_5(x,y)$ **(j)** Undisclosed $\hat{f}_6(x,y)$ **(k)** Undisclosed $\hat{f}_7(x,y)$ **(l)** Undisclosed $\hat{f}_8(x,y)$

Figure 4. (**a**–**h**) Correct decrypted images $\hat{f}_j(x,y)$ at $j = 1,2,3,...,8$, when the correct seventeen security keys RPMs, given by the sixteen RPMs ($r_j(x,y)$ and $h_j(x,y)$) and the rotation angle of the GT operator, are used. (**i**–**l**) Wrong decrypted images $\hat{f}_5(x,y)$, $\hat{f}_6(x,y)$, $\hat{f}_7(x,y)$ and $\hat{f}_8(x,y)$, respectively, when the incorrect security key RPM $h_7(x,y)$ and the other correct sixteen security keys (the remaining fifteen RPMs and the rotation angle of the GT operator) are used in the decryption scheme.

Several possible drawbacks of the proposed multiple-image encryption–decryption scheme could arise when the total number p of images to encrypt is quite large, assuming that the resolution of each image remains unchanged. For example, in its optoelectronic implementation, the possibility to place a large number of images for encryption in the input plane of the JTC may be limited by the resolution of the display used in the input plane (e.g., a phase-only spatial light modulator). The computation time for the numerical simulations of the proposed encryption system will increase as the total number p of the original images to be encrypted increases, because the digital images needed to compute the three intensities ($\mathrm{JGPD}_\alpha(u,v)$, $I_1(u,v)$ and $I_2(u,v)$) of the encrypted image will have a bigger resolution. Finally, the management and distribution of the security keys of the

proposed encryption–decryption scheme can be a bit more complicated due to the large number of security keys given by the $2p$ RPMs.

We consider the key space of the proposed encryption and decryption schemes as all possible combinations of the seventeen security keys given by the sixteen RPMs ($r_j(x,y)$ and $h_j(x,y)$) and the rotation angle of the GT operator. In reference [26], it was found that the sensitivity on the values of the rotation of the GT operator in order to retrieve a good quality decrypted image was of the order of 4×10^7. All the sixteen RPMs are images with a resolution of 512×512 pixels and the possible values of these pixels are 256 different values. Therefore, the number of possible combinations of the sixteen RPMs is of the order of $256^{(16)(512)(512)} = 256^{4194304}$ [29]. Finally, the total key space of the proposed encryption and decryption schemes is given by the product of the sensitivity on the values of the rotation of the GT operator and the number of possible combinations of the sixteen RPMs: $(4 \times 10^7)(256^{4194304})$. This total key space is very large, and a brute force attack for the encryption and decryption schemes of this work would be impractical. An improvement in the security of the proposed encryption scheme against CPA, KPA and COA is obtained due to the nonlinear modifications applied in this work; such nonlinear modifications are the phase encoding of the original images and the operations performed on the JGPD in order to obtain the encrypted image. This fact was shown in references [15–19,22,23,26,27].

4. Conclusions

A new encryption–decryption scheme was proposed for multiple images based on a nonlinear fully phase JTC architecture in the GD. The proposed security system can encrypt multispectral or color images considering each color channel as a grayscale image. The encryption system can also protect binary and biometric images. The proposal incorporates two nonlinear modifications: the phase encoding of the original grayscale images to encrypt and the nonlinear operations introduced in the JGPD. The retrieval of multiple images due to the nonlinear modifications provides a highly secure encryption–decryption system, which achieves an excellent quality of the decrypted images. The security keys of the proposed encryption and decryption schemes are represented by the RPMs $r_j(x,y)$ and $h_j(x,y)$ and the rotation angle of the GT operator. Only the correct values of the security keys permit a proper simultaneous retrieval of the original images in the decryption scheme. The proposed simultaneous encryption scheme has a fast computation time in comparison to previous proposals that sequentially encrypt multiple grayscale images. In our proposal, the encryption of up to eight images is obtained by simultaneously displaying the whole set of signals in the input plane of the encryption stage. In addition, the final encrypted distribution is nonlinearly computed by using only three intensity distributions. The proposed encryption–decryption scheme is more secure against several plaintext attacks because of the phase encoding of the original images to encrypt, the nonlinear operations applied over the JGPD and the larger key space of the proposed encryption scheme.

Author Contributions: The work described in this article was the collaborative development of all the authors. Conceptualization, R.A.P., J.M.V., E.P.-C., M.S.M. and C.O.T.; methodology, R.A.P., J.M.V., E.P.-C., M.S.M. and C.O.T.; software, R.A.P. and J.M.V.; validation, J.M.V., E.P.-C., M.S.M. and C.O.T.; investigation, R.A.P., J.M.V., E.P.-C., M.S.M. and C.O.T.; writing—original draft preparation, R.A.P. and J.M.V.; writing—review and editing, J.M.V., E.P.-C., M.S.M. and C.O.T.; supervision, J.M.V., E.P.-C., M.S.M. and C.O.T. All authors have read and agreed to the published version of the manuscript.

Funding: This research has been funded by the Universidad de La Guajira (Riohacha), the Universidad Popular del Cesar (Valledupar) and the Universitat Politècnica de Catalunya · BarcelonaTech, SGR 2021 SGR 00388 and the Agencia Estatal de Investigación, Spanish Government (PID2020-114582RB-I00/AEI/10.13039/501100011033).

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The supporting information can be found from the corresponding author.

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

Abbreviations

The following abbreviations are used in this manuscript:

CPA	Chosen-Plaintext Attack
COA	Ciphertext-Only Attack
DRPE	Double Random-Phase Encoding
FrFD	Fractional Fourier Domain
GD	Gyrator Domain
GT	Gyrator Transform
KPA	Known-Plaintext Attack
JGPD	Joint Gyrator Power Distribution
JTC	Joint Transform Correlator
RPMs	Random-Phase Masks
RMSE	Root Mean Square Error

Appendix A. The Gyrator Transform Operator

The Gyrator transform (GT) operator is a linear integral transform that maps a two-dimensional function $f(x,y)$ onto function $f_\alpha(u,v)$, where the parameter α is the rotation angle. The GT operator at parameter α is defined by [49]

$$f_\alpha(u,v) = \mathscr{G}^\alpha\{f(x,y)\} = \int_{-\infty}^{+\infty}\int_{-\infty}^{+\infty} f(x,y)K_\alpha(u,v,x,y)\mathrm{d}x\mathrm{d}y, \tag{A1}$$

$$K_\alpha(u,v,x,y) = C_\alpha \exp\{i2\pi[(uv+xy)\cot\alpha - (vx+uy)\csc\alpha]\}, \quad C_\alpha = \frac{1}{|\sin\alpha|}, \tag{A2}$$

where K_α is the kernel of the GT operator, the values of the rotation angles are in the interval of $0 \le \alpha < 2\pi$, the variables x and y represent the coordinates at the spatial domain and the variables u and v denote the output coordinates in the Gyrator domain (GD). When $\alpha = 0$, the GT operator reduces to the identity transform. When $\alpha = \pi/2$, the GT operator corresponds to the direct Fourier transform with rotation of the coordinate at $\pi/2$. When $\alpha = \pi$, the reverse transform is derived from the GT operator. When $\alpha = 3\pi/2$, the GT operator is the inverse Fourier transform with rotation of the coordinate at $\pi/2$ [49]. The inverse GT operator corresponds to the GT operator at rotation angle $-\alpha$. The GT operator is additive with respect to the rotation angle, $\mathscr{G}^\alpha\mathscr{G}^\beta = \mathscr{G}^{\alpha+\beta}$.

The kernel of the GT operator is the product of the hyperbolic and plane waves, and the kernel of the fractional Fourier transform operator is the product of the spherical and plane waves [26]. The properties of the GT operator and the fractional Fourier transform operator have some aspects in common, because these operators are special cases of the linear canonical transforms [27].

The optical GT operator was implemented in [50,51] by means of a setup that uses three generalized lenses with a fixed distance between them. Each generalized lens is composed of two thin cylinder lenses and the rotation of these cylindrical lenses control the value of the rotation angle α.

Appendix B. Generalized Shift Operator

We use the definition of the generalized shift operator proposed in [52], which is a simultaneous application of a spatial shift and a modulation by a pure linear phase term over a function $f(x,y)$. The generalized shift operator at parameters x_0, y_0 and α is defined by

$$\mathrm{GS}_{x_0,y_0;\alpha} f(x,y) = \exp\left\{-i2\pi\left[y_0\left(x-\frac{x_0}{2}\right)+x_0\left(y-\frac{y_0}{2}\right)\right]\cot\alpha\right\} f(x-x_0,y-y_0). \quad \text{(A3)}$$

The generalized shift operator forms a commutative group for the rotation angle α. The composition law is $\mathrm{GS}_{x_1,y_1;\alpha}\mathrm{GS}_{x_2,y_2;\alpha} = \mathrm{GS}_{x_1+x_2,y_1+y_2;\alpha}$. The usual traslation operator is obtained from the generalized shift operator when the rotation angle is $\alpha = \pi/2$; hence, $\mathrm{GS}_{x_0,y_0;\pi/2} f(x,y) = f(x-x_0,y-y_0)$. The GT operator with the rotation angle α of the generalized shift operator presented in Equation (A3) is

$$\mathscr{G}^{\alpha}\{\mathrm{GS}_{x_0,y_0;\alpha} f(x,y)\} = \exp\{-i2\pi(y_0 u + x_0 v)\csc\alpha\} f_{\alpha}(u,v). \quad \text{(A4)}$$

The generalized shift operator does not introduce a shift over the result of the GT operator. This property is very useful for centered optical systems [52].

References

1. 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.: Weinheim, Germany, 2011; pp. 739–767.
2. Chen, W.; Javidi, B.; Chen, X. Advances in optical security systems. *Adv. Opt. Photonics* **2014**, *6*, 120–155. [CrossRef]
3. 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]
4. 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.
5. Cai, J.; Shen, X.; Fan, C.; Zhou, B. Security-enhanced optical encryption based on JTC architecture with confused ciphertext. *Optik* **2020**, *206*, 163742. [CrossRef]
6. Zhong, Y.; Chen, L.; Gan, W.; Liu, Y. Image Encryption System Based on Joint Transformation Correlation and Ptychography. *IEEE Photonics J.* **2020**, *12*, 2400110. [CrossRef]
7. Chen, Q.; Shen, X.; Cheng, Y.; Lin, C.; Liu, Y.; Zhou, B. A security-enhanced joint transform correlator optical encryption system with cropping operation. *Optik* **2021**, *245*, 167654. [CrossRef]
8. Réfrégier, P.; Javidi, B. Optical image encryption based on input plane and Fourier plane random encoding. *Opt. Lett.* **1995**, *20*, 767–769. [CrossRef]
9. Goodman, J.W. *Introduction to Fourier Optics*, 3rd ed.; Roberts & Company Publishers: Englewood, CO, USA, 2005.
10. Nomura, T.; Javidi, B. Optical encryption using a joint transform correlator architecture. *Opt. Eng.* **2000**, *39*, 2031–2035.
11. Situ, G.; Zhang, J. Double random phase encoding in the Fresnel domain. *Opt. Lett.* **2004**, *29*, 1584–1586. [CrossRef]
12. 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]
13. Kwak, C.H.; Javidi, B. Generalized description of double random phase encoding by Collins diffraction transformation. *J. Opt.* **2019**, *21*, 015703. [CrossRef]
14. Nomura, T.; Mikan, S.; Morimoto, Y.; Javidi, B. Secure Optical Data Storage with Random Phase Key Codes by use of a Configuration of a Joint Transform Correlator. *Appl. Opt.* **2003**, *42*, 1508–1514. [CrossRef] [PubMed]
15. Vilardy, J.M.; Millán, M.S.; Pérez-Cabré, E. Improved decryption quality and security of a joint transform correlator-based encryption system. *J. Opt.* **2013**, *15*, 025401. [CrossRef]
16. Vilardy, J.M.; Millán, M.S.; Pérez-Cabré, E. Experimental optical encryption scheme for the double random phase encoding using a nonlinear joint transform correlator. *Optik* **2020**, *217*, 164653.
17. Jaramillo-Osorio, A.; Barrera-Ramírez, J.F.; Mira-Agudelo, A.; Velez-Zea, A.; Torroba, R. High performance compact optical cryptosystem without reference arm. *J. Opt.* **2020**, *22*, 035702.
18. Vilardy, J.M.; Millán, M.S.; Pérez-Cabré, E. Nonlinear optical security system based on a joint transform correlator in the Fresnel domain. *Appl. Opt.* **2014**, *53*, 1674–1682.
19. Vilardy, J.M.; Millán, M.S.; Pérez-Cabré, E. Joint transform correlator-based encryption system using the Fresnel transform and nonlinear filtering. *Proc. SPIE* **2013**, *8785*, 87853J.
20. Barrera, J.F.; Jaramillo, A.; Vélez, A.; Torroba, R. Experimental analysis of a joint free space cryptosystem. *Opt. Lasers Eng.* **2016**, *83*, 126–130.
21. Lu, D.; Jin, W. Color image encryption based on joint fractional Fourier transform correlator. *Opt. Eng.* **2011**, *50*, 068201. [CrossRef]
22. Vilardy, J.M.; Torres, Y.; Millán, M.S.; Pérez-Cabré, E. Generalized formulation of an encryption system based on a joint transform correlator and fractional Fourier transform. *J. Opt.* **2014**, *16*, 125405. [CrossRef]

23. Vilardy, J.M.; Millán, M.S.; Pérez-Cabré, E. Images encryption system based on a fractional joint transform correlator and nonlinear filtering. *Opt. Pura Apl.* **2014**, *47*, 35–41. [CrossRef]
24. Jaramillo, A.; Barrera, J.F.; Vélez, A.; Torroba, R. Fractional optical cryptographic protocol for data containers in a noise-free multiuser environment. *Opt. Lasers Eng.* **2018**, *102*, 119–125. [CrossRef]
25. Abuturab, M.R. Noise-free recovery of color information using a joint-extended Gyrator transform correlator. *Opt. Lasers Eng.* **2013**, *51*, 230–239. [CrossRef]
26. Vilardy, J.M.; Millán, M.S.; Pérez-Cabré, E. Nonlinear image encryption using a fully phase nonzero-order joint transform correlator in the Gyrator domain. *Opt. Lasers Eng.* **2017**, *89*, 88–94. [CrossRef]
27. Vilardy, J.M.; Perez, R.A.; Torres, C.O. Optical image encryption using a nonlinear joint transform correlator and the Collins diffraction transform. *Photonics* **2019**, *6*, 115. [CrossRef]
28. Carnicer, A.; Montes-Usategui, M.; Arcos, S.; Juvells, I. Vulnerability to chosen–cyphertext attacks of optical encryption schemes based on double random phase keys. *Opt. Lett.* **2005**, *30*, 1644–1646. [CrossRef]
29. Frauel, Y.; Castro, A.; Naughton, T.J.; Javidi, B. Resistance of the double random phase encryption against various attacks. *Opt. Express* **2007**, *15*, 10253–10265. [CrossRef]
30. Peng, X.; Zhang, P.; Wei, H.; Yu, B. Known-plaintext attack on optical encryption based on double random phase keys. *Opt. Lett.* **2006**, *31*, 1044–1046. [CrossRef]
31. Guo, C.; Liu, S.; Sheridan, J.T. Iterative phase retrieval algorithms. Part II: Attacking optical encryption systems. *Appl. Opt.* **2015**, *54*, 4709–4719. [CrossRef]
32. Barrera, J.F.; Vargas, C.; Tebaldi, M.; Torroba, R. Chosen-plaintext attack on a joint transform correlator encrypting system. *Opt. Commun.* **2010**, *283*, 3917–3921. [CrossRef]
33. Barrera, J.F.; Vargas, C.; Tebaldi, M.; Torroba, R.; Bolognini, N. Known-plaintext attack on a joint transform correlator encrypting system. *Opt. Lett.* **2010**, *35*, 3553–3555. [CrossRef]
34. Dou, S.; Shen, X.; Zhou, B.; Lin, C.; Huang, F.; Lin, Y. Known-plaintext attack on JTC-based linear cryptosystem. *Optik* **2019**, *198*, 163274. [CrossRef]
35. Zhang, C.; Liao, M.; He, W.; Peng, X. Ciphertext-only attack on a joint transform correlator encryption system. *Opt. Express* **2013**, *21*, 28523–28530. [CrossRef] [PubMed]
36. Mosso, F.; Tebaldi, M.; Barrera, J.F.; Bolognini, N.; Torroba, R. Pure optical dynamical color encryption. *Opt. Express* **2011**, *19*, 13779–13786. [CrossRef] [PubMed]
37. Qin, Y.; Wang, Z.; Pan, Q.; Gong, Q. Optical color-image encryption in the diffractive-imaging scheme. *Opt. Lasers Eng.* **2016**, *77*, 191–202. [CrossRef]
38. Tebaldi, M.; Horrillo, S.; Pérez-Cabré, E.; Millán, M.S.; Amaya, D.; Torroba, R.; Bolognini, N. Experimental color encryption in a joint transform correlator architecture. *J. Phys. Conf. Ser.* **2011**, *274*, 012054. [CrossRef]
39. Barrera, J.F.; Tebaldi, M.; Rios, C.; Rueda, E.; Bolognini, N.; Torroba, R. Experimental multiplexing of encrypted movies using a JTC architecture. *Opt. Express* **2012**, *20*, 3388–3393. [CrossRef]
40. Jaramillo-Osorio, A.; Velez-Zea, A.; Mira-Agudelo, A.; Barrera-Ramírez, J.F.; Torroba, R. Secure selective recovery protocol for multiple optically encrypted data. *Opt. Lasers Eng.* **2020**, *137*, 106383. [CrossRef]
41. Zhao, T.; Chi, Y. A multi-user encryption and authentication system based on joint transform correlation. *Entropy* **2019**, *21*, 850. [CrossRef]
42. Su, Y.; Wang, X.; Wang, Z.; Liu, C.; Li, J.; Xu, K.; Li, S.; Cai, Z.; Wan, W. Security-enhanced multiple-image encryption based on modified iterative phase retrieval algorithm with structured phase mask in Fresnel domain. *Optik* **2022**, *254*, 168649. [CrossRef]
43. Li, F.; Ding, H.; Nie, S.; Ma, J.; Yuan, C. Multiple-image encryption using phase jump gradient factors-based OAM multiplexing holography. *Opt. Lasers Eng.* **2023**, *160*, 107303. [CrossRef]
44. Wang, X.; Lin, S.; Xue, J.; Xu, B.; Chen, J. Information security scheme using deep learning-assisted single-pixel imaging and orthogonal coding. *Opt. Express* **2023**, *31*, 2402–2413. [CrossRef]
45. Wang, Z.; Su, Y.; Wang, X.; Wang, B.; Li, S.; Liu, C.; Li, J.; Cai, Z.; Wan, W. Security-enhanced multiple-image encryption based on quick response codes and modified double random phase encoding in the fractional Fourier transform domain. *App. Opt.* **2022**, *61*, 7255–7264. [CrossRef]
46. Shan, M.; Guo, J.; Zhong, Z.; Liu, B.; Yu, L.; Liu, L. Improved multiple-image authentication based on optical interference by wavelength multiplexing. *App. Opt.* **2022**, *61*, 6931–6938. [CrossRef] [PubMed]
47. Zhang, L.Z.; Zhou, X.; Wang, D.; Li, N.N.; Bai, X.; Wang, Q.H. Multiple-image encryption based on optical scanning holography using orthogonal compressive sensing and random phase mask. *Opt. Eng.* **2020**, *59*, 102411. [CrossRef]
48. Multispectral Image Database. Columbia Imaging and Vision Laboratory. Computer Science. Columbia University. Available online: https://cave.cs.columbia.edu/repository/Multispectral (accessed on 23 January 2023).
49. Rodrigo, J.A.; Alieva, T.; Calvo, M.L. Gyrator transform: properties and applications. *Opt. Express* **2007**, *15*, 2190–2203. [CrossRef]
50. Rodrigo, J.A.; Alieva, T.; Calvo, M.L. Optical system design for ortho-symplectic transformations in phase space. *J. Opt. Soc. Am. A* **2006**, *23*, 2494–2500. [CrossRef] [PubMed]

51. Rodrigo, J.A.; Alieva, T.; Calvo, M.L. Experimental implementation of the gyrator transform. *J. Opt. Soc. Am. A* **2007**, *24*, 3135–3139. [CrossRef]
52. Perez, R.A.; Vilardy, J.M.; Torres, C.O. Image processing operators based on the Gyrator transform: Generalized shift, convolution and correlation. *Photonics* **2019**, *6*, 120. [CrossRef]