engineering proceedings

MDPI

Proceeding Paper

Phase-Image-Encryption-Based Elliptic Curve and Double-Random-Phase Encoding †

Arabind Kumar [1,*], Sanjay Yadav [2] and Tarul Garg [1]

[1] Department of Applied Sciences, The Northcap University, Gurugram 122017, Haryana, India; tarulgarg@ncuindia.edu
[2] PW-Institute of Innovation, Bengaluru 560049, Karnataka, India; sanjay.yadav1@pw.live
* Correspondence: arabind20asd003@ncuindia.edu
† Presented at the International Conference on Recent Advances in Science and Engineering, Dubai, United Arab Emirates, 4–5 October 2023.

Abstract: In this paper, we proposed an enhanced asymmetric cryptosystem scheme for image encryption using a combination of Elliptic Curve and Fourier transformations. Our proposed encryption and decryption process is highly secure with a smaller key size compared to other schemes due to the use of Elliptic Curve Cryptography. The experimental results prove that the image-encryption scheme proposed in this research is effective and has strong anti-attack and key sensitivity. Computer-based simulations have been performed for this scheme to complete the measurable examination utilizing histograms plots, and correlation distribution of adjacent pixels. Moreover, the security of this encryption scheme relies on Elliptic Curve Cryptography, which has high security. The validation of the scheme is shown using a grayscale image and all the computations are performed in MATLAB (R2021a). The security against several attacks like noise is also shown.

Keywords: Elliptic Curve Cryptography; image encryption; Fourier transformation; encoding; security

Citation: Kumar, A.; Yadav, S.; Garg, T. Phase-Image-Encryption-Based Elliptic Curve and Double-Random-Phase Encoding. *Eng. Proc.* **2023**, *59*, 155. https://doi.org/10.3390/engproc2023059155

Academic Editors: Nithesh Naik, Rajiv Selvam, Pavan Hiremath, Suhas Kowshik CS and Ritesh Ramakrishna Bhat

Published: 11 January 2024

1. Introduction

Computerized pictures are an appealing information type with a far reaching scope of utilization, and numerous clients are interested in executing content-security strategies on their pictures to keep them from being seen, for copyright or for control. In numerous applications like military-picture data sets, private video conferencing, clinical imaging framework, satellite television and online individual photo collection, security is fundamental. Likewise, the wide utilization of pictures of mechanical interactions transforms them into an asset and a resource. So, it is essential to shield confidential images and their information from unapproved access.

In 1995, Refregier and Javidi first proposed the double-random phase encoding (DPRE) [1] technique. Its properties, including a huge data limit, parallel processing and the fast speed of the optical cryptosystems, have attracted much notice in the research community.

Since then, optical encryption plans dependent on DRPE have been investigated by various specialists and improved upon using various methodologies, for example, a Fresnel domain, a partial Fourier domain [2], applying fractional Fourier change in digital holography [3], utilizing diffractive imaging [4], utilizing stage recovery calculation and intermodulation in a Fourier domain [5] and utilizing adequacy balance [6]. To further upgrade the security of optical encryption plans, distinctive cutting-edge innovations have been solidified in an unexpected way, with model-image-encoding dependent on multi-stage and multi-channel partial Fourier change [7]; arbitrary parallel stage regulation with combination recovery kind of Yang-Gu calculation; gyrator and Arnold transform [8]; advanced holography and joint correlators [9,10]; fractional Mellin change; Hartley change; Arnold change and solitary worth deterioration in fragmentary Hartley space; wavelet

domain [11]; gyrator wavelet change; stage-moving interferometry, phase recovery calculation [12]; photon-counting and polarimetric picture encryption [13,14]; pressure-based picture encryption; compression-imaging-based encryption with its weakness to ptychographic stage recovery [15]; and other methods [16].

The DRPE procedure proved to be defenseless as a direct result of its symmetric and linear nature [17], and it was furthermore discovered to be liable to known-plaintext [18], picked-ciphertext [19] and picked-plaintext assaults [20]. Therefore, the investigators were looking for asymmetric and nonlinear plans. Qin and Peng [21] planned phase-truncated Fouriertransforms (PTFT) in which amplitude and phase truncation nonlinear tasks acted twice. From there on, numerous specialists used PTFT tasks in their scheme [22]. Yet, the schemes dependent on PTFT were discovered to be powerless against unique assault and its variants [23]. Thus, agents were looking for explicit plans which should have nonlinear properties and oppose extraordinary assaults and have a secure channel to communicate the private key or to keep the decryption key secret; therefore, we need to utilize public key cryptography [24].

Since 1985, when elliptic curves were applied autonomously by Mill operator and Koblitz [25] to present another public key cryptosystem, numerous analysts have attempted to utilize this method on various information types and improve the productivity by proposing different strategies. Truth be told, the most alluring benefit of ECC that spurred cryptographers to utilize it was its more noteworthy security and all the more computationally effective properties it exhibits with identical key sizes in correlation with other public keys. This property changed ECC to a worthy choice for multimedia information types like pictures, video and sound, because of the enormous size and high information pace of these document types. So, a cryptosystem utilizing a short key size also with high security is required. ECC is a public key or asymmetric cryptography method, which means that the encryption key and decryption key are each unique. ECC is an asymmetric cryptosystem that gives security and quick execution as opposed to RSA. In contrast to private key cryptography, ECC is proper for applications in which a safe channelis not available for sendning a private key [26].

A large part of this exploration has been done in traditional change spaces like Fourier, fractional Fourier, Gyrator, wavelet, and other methods. B. Kekre et al. [27] proposed a hybrid wavelet-generation procedure utilizing existing orthogonal transforms. These wavelets can be created for various sizes and types by using segment changes and changing the number of components at each degree of goal. These remarkable wavelets have been utilized for picture examination and compression. This method can likewise be utilized for executing cryptosystems which can have broad key-space and security considering its intrinsic nature of versatility and adaptability. Pixel-scrambling techniques are used for reducing the correlation between the original and encrypted images. To serve this purpose, various chaotic systems like 2D logistic maps, the 3D Lorenz chaotic system [28], the 4D hyperchaotic system [29], and the chaotic Baker map have been utilized. They enhanced the security of optical schemes by extending the key-space and increasing randomness in the encrypted image [30].

In this paper, to enhance the security of the cryptosystem for image encryption, we mapped the pixel values to elliptic curve coordinates and performed point multiplication of pixel values with the generator ‘G’ to create affine coordinates on the elliptic curve. For such cases, while decrypting the cipher image, a corresponding pixel value was generated. In our algorithm, we worked on scrambling at the time of encryption and descrambling at the time of decryption and we ensured that the larger integer cannot be greater than the prime ‘P’, which was one of the parameters in finite filed equation of elliptic curve. Due to these mapping operations, we do not need to share the mapping table between the receiver and the sender.

2. Elliptic Curve Cryptography and Fourier Transformation

An elliptic curve is a non-singular cubic equation with an algebraic structure of elliptic form over a finite field. These structures are symmetric about the x-axis and this property plays an important role in operations.

$$y^2 = \{x^3 + ax + b\} \bmod p \quad (1)$$

where a and b are integers which satisfy $4a^3 + 27b^2 \neq 0 \pmod p$ and p is a large prime number. This approach uses six-tuples defined as {p, x, y, G, n, h}.

To encrypt an image, the sender and receiver decided to take an affine point G lies on an elliptic curve.

Step 1: Both users decide on a public number G and p
Step 2: Both users then select their private key a and b,
Step 3: The receiver's and sender's public key is calculated by the given rule

$$\text{Receivers public key } x = G^a \bmod p \quad (2)$$

$$\text{Senders public key } y = G^b \bmod p \quad (3)$$

Step 4: Both users then compute their symmetric keys

$$\text{receivers symmetric key} = x^a \bmod p \text{ and } y^b \bmod p = \text{Senders symmetric key} \quad (4)$$

In single variable, Fourier transform of a function f(x) is defined by [16]

$$F\{f(x)\} = \int_{-\infty}^{\infty} \mathbf{f(x)e^{-2\pi ixt}dx} \quad (5a)$$

In two variables, Fourier transform of a function f(x, y) is defined by

$$F\{f(x,y)\} = \int_{-\infty}^{\infty}\int_{-\infty}^{\infty} f(x,y)e^{-2\pi i(xu+yv)}dxdy \quad (5b)$$

3. Proposed Cryptosystems

The schematic flowchart of the proposed cryptosystem is represented in Figure 1. Here, two arbitrary decomposition cells are cascaded twice on ECC scrambled image.

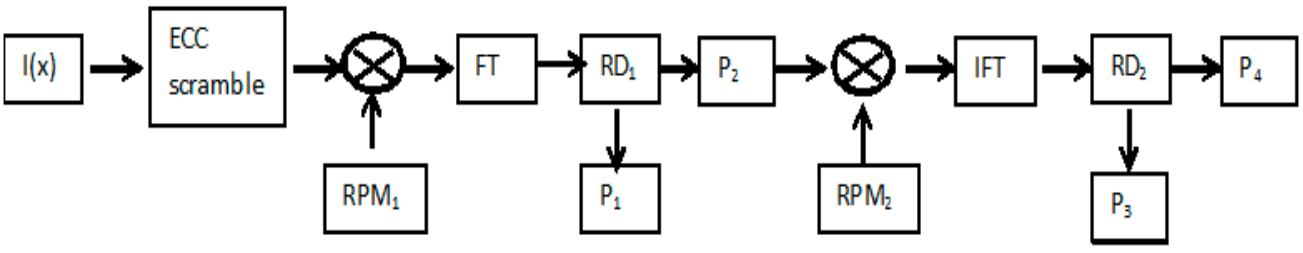

Figure 1. Flow chart of Encryption Scheme.

The encryption process can be performed by using the following steps:

Step 1: The intensity distribution I(x) of the input image is scrambled utilizing the permutation key stream accomplished through ECC to get ECC scramble.
Step 2: A random-phase mask RPM = exp (exp (iπ rand(x))) is applied on ECC scramble where rand(x) is a built-in function in MATLAB that generates pseudo-random numbers having values between [0, 1].
Step 3: The intensity distribution of ECC(x) in Fourier transformation domain ECC'(x) is obtained using the following equation:

$$ECC'(x) = FT\{\sqrt{}(ECC(x)).RPM_1\} \quad (6)$$

Here, FT represents Fourier transformation.

Step 4: Two masks $P_1(u)$ and $P_2(u)$ are generated using the random decomposition process:

$$P_1(u) = \frac{\frac{A(u)}{2}\sin\beta_2}{\sin(\beta_2+\beta_1)} \times \exp(i(\phi(u)-\beta_1)) \quad (7)$$

$$P_2(u) = \frac{\frac{A(u)}{2}\sin\beta_1}{\sin(\beta_2+\beta_1)} \times \exp(i(\phi(u)+\beta_2)) \quad (8)$$

where $A(u)$ and $\phi(u)$ represent the phase and amplitude components of $ECC'(u)$, β_1 and β_2 are uniformly generated random numbers of the same size as that of the image, with values of random numbers in the interval $[0, 2\pi]$.

Step 5: Then take inverse Fourier transform (IFT) of $P_2(u)$ to get $P_{itrans1}'(x)$

$$P_{itrans1}'(x) = IFT\{P_2(u)\} \quad (9)$$

Step 6: Two masks $P_3(x)$ and $P_4(x)$ are further obtained from $P_{itrans2}(x)$ using another random decomposition.

$$P_3(u) = \frac{\frac{A_1(x)}{2}\sin\beta_4}{\sin(\beta_4+\beta_3)} \times \exp(i(\phi_1(x)-\beta_3)) \quad (10)$$

$$P_4(u) = \frac{\frac{A_1(x)}{2}\sin\beta_3}{\sin(\beta_4+\beta_3)} \times \exp(i(\phi_1(x)+\beta_4)) \quad (11)$$

$\varphi_1(x)$ and $A_1(x)$ refer to the phase and amplitude part of $P_{itrans2}(x)$, respectively. Furthermore, β_3 and β_4 are uniformly generated random numbers of the similar size as that of image, with values of random numbers in the interval $[0, 2\pi]$.

The decryption process can be performed by using the following process Figure 2:

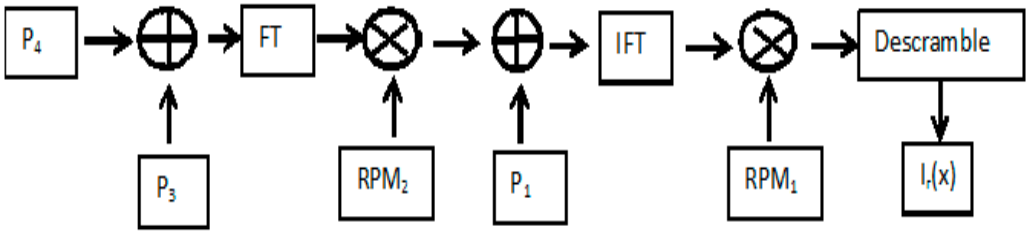

Figure 2. Flow Chart of Decryption Scheme.

4. Validation of the Scheme

A grayscale image of Lena of size 256 × 256 was chosen as the input for MATLAB Implementation. The elliptic-curve scrambling was also obtained using the values on y^2 mod 123,457 = $\{x^3 + 5376x + 2438\}$mod 123,457. In this process, we obtained the mapping table, starting with first row point 0, and continued with the next points with next values. Once we completed the assignment of the first 256 points in the first column, and of a further 256 points in the second column, we carried on in the same sequence until the end. We obtained a total of 123,387 points on the curve and we filled 250 rows and 481 columns completely, with the remaining rows of the last column filled with zero. We have chosen some parameters to encrypt the image as: generator G = (2225, 75,856), receiver's private key y = 36,548, and the sender also had a chosen a random integer k = 23,412. Using the parameters defined above, the receiver's public key was P_B = (30,402, 35,513). We encrypted the image (Figure 3a) by this proposed encrypted scheme (Figure 3c) all processes were completed in MATLAB. (Figure 3d) is the recovered image by given decryption process.

We observed that the statistical metric correlation coefficient (CC) between the input and the recovered image was equal to one. Where CC is defined as,

$$CC = \frac{\mathrm{cov}(I_0(x,y), I_r(x,y))}{\sigma(I_0(x,y)), \sigma(I_r(x,y))} \quad (12)$$

where σ denotes the standard deviation and cov defines the covariance, and $I_0(x, y)$ and $I_r(x, y)$ are pixel values of input and output image, respectively.

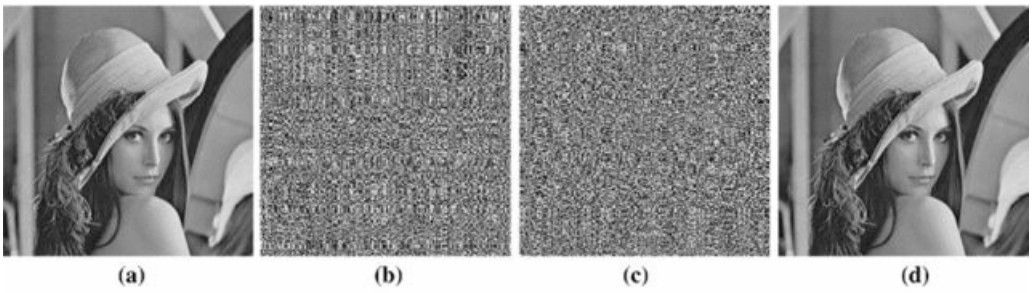

Figure 3. Validation of the Scheme (**a**) Original Inage, (**b**) Scrambled Image, (**c**) Encrypted Image, (**d**) Output Image.

5. Results and Discussion

5.1. Noise Attack

A robust cryptosystem is that which obtains the correct encrypted image even in a noisy environment. For the above encrypted scheme, we had shown the outcomes of noise attack in Figure 3c. We have presented result of the different noise strength n_k as per the formula

$$C_n = C\,(1 + n_k\,G) \quad (13)$$

where Gaussian noise is defined by G with Unity standard deviation zero mean and Cn is the noise-affected encrypted image. We have shown the result in Figure 4a–d with increasing noise strengths of 0.2, 0.5, 0.9 and 1.2, respectively. We obtained an easily recognizable image, even in the presence of high noise in an encrypted image. This shows that the proposed scheme is quite resistant to the noise attack. To strengthen our study, we also plotted the correlation coefficient versus noise strength, as shown in Figure 5. It is significant that we observed that the correlation coefficient between the recovered and input images was decreasing sharply up to noise strength one and after that the gradient of the curve was less sharp. This comparison gives strength to our conclusion that proposed scheme is robust enough.

Figure 4. Noise attack resistance with increasing noise strength (**a**) 0.2, (**b**) 0.5, (**c**) 0.9, (**d**) 1.2.

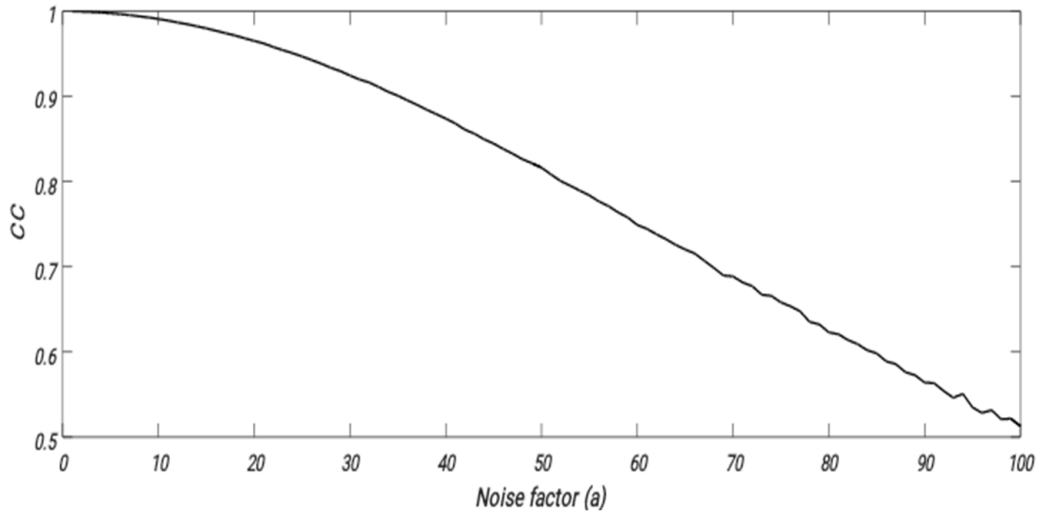

Figure 5. Plot of correlation coefficient versus noise strength.

5.2. Histogram Analysis

Any proposed encryption algorithm is worthy if the original and encrypted images give a different histogram. We have also confirmed the worthiness of our proposed scheme using histograms and the outcome is shown below. It is visible in Figure 6a,c that the plaintext and ciphertext had identical histograms and the encrypted image Figure 6b is totally different from the original one.

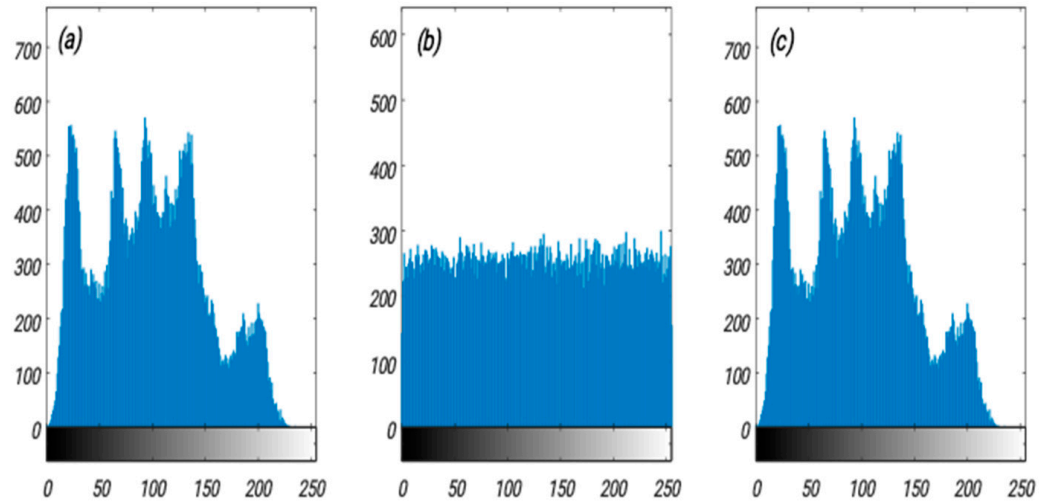

Figure 6. Histogram Analysis (**a**) Input Image, (**b**) Encrypted Image, (**c**) Decrypted Image.

5.3. Wrong Key Analysis

A minor change in one key with the remaining keys unchanged was to decrypt the image. The changes from these keys are as shown in Figure 7.

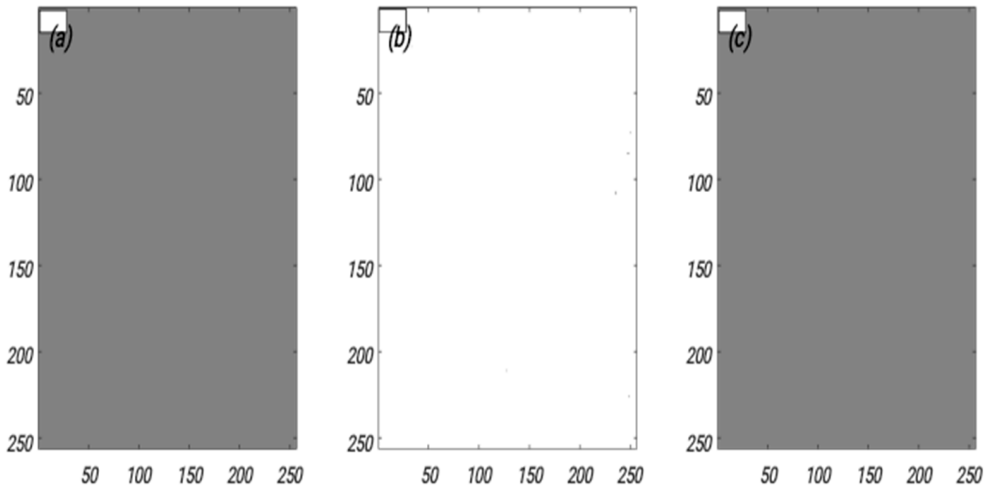

Figure 7. Decryption with wrong key: (**a**) plaintext, (**b**) ciphertext (**c**) and encrypted Image.

6. Conclusions

In this paper, we used two systems to encrypt an image. In order to generate a sequence using an elliptic curve point, the image was randomly scrambled by Fourier transformations. The elliptic curve points can increase the complexity of the algorithm and then serialize the matrix generated by it, and we encrypted the image information's with the key and the cipher text image. To prove the superiority of the algorithm, attack efficiency, wrong key analysis, noise attack, and histogram analysis were studied in this paper.

Author Contributions: S.Y.; Methodology, A.K.; original draft, writing work and all coding, T.G.; review. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not Applicable.

Data Availability Statement: Data are contained within the article.

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

References

1. Yadav, A.K.; Singh, P.; Singh, K. Cryptosystem based on devil's vortex Fresnel lens in the fractional Hartley domain. *J. Opt.* **2018**, *47*, 208–219. [CrossRef]
2. Kumar, J.; Singh, P.; Yadav, A.; Kumar, A. Asymmetric Cryptosystem for Phase Images in Fractional Fourier Domain Using LU-Decomposition and Arnold Transform. *Procedia Comput. Sci.* **2018**, *132*, 1570–1577. [CrossRef]
3. Singh, P.; Yadav, A.; Singh, K. Color image encryption using affine transform in fractional Hartley domain. *Opt. Appl.* **2017**, *47*, 421–433.
4. Vashisth, S.; Singh, H.; Yadav, A.K.; Singh, K. Image encryption using fractional Mellin transform, structured phase filters, and phase retrieval. *Opt.-Int. J. Light Electron Opt.* **2014**, *125*, 5309–5315. [CrossRef]
5. Gopinathan, U.; Monaghan, D.S.; Naughton, T.J.; Sheridan, J.T. A known-plaintext heuristic attack on the Fourier plane encryption algorithm. *Opt. Express* **2006**, *14*, 3181–3186. [CrossRef]
6. Mehra, I.; Nishchal, N.K. Optical asymmetric image encryption using gyrator wavelet transform. *Opt. Commun.* **2015**, *354*, 344–352. [CrossRef]
7. Rakheja, P.; Vig, R.; Singh, P. An asymmetric watermarking scheme based on random decomposition in hybrid multi-resolution wavelet domain using 3D Lorenz chaotic system. *Optik* **2019**, *198*, 163289. [CrossRef]
8. Joshi, M.; Chandrashakher; Singh, K. Color image encryption and decryption for twin images in fractional Fourier domain. *Opt. Commun.* **2008**, *281*, 5713–5720. [CrossRef]
9. Rakheja, P.; Vig, R.; Singh, P.; Kumar, R. An iris biometric protection scheme using 4D hyperchaotic system and modified equal modulus decomposition in hybrid multi resolution wavelet domain. *Opt. Quantum Electron.* **2019**, *51*, 204. [CrossRef]
10. Dou, S.; Shen, X.; Lin, C. Security-enhanced optical nonlinear cryptosystem based on double random phase encoding. *Opt. Laser Technol.* **2020**, *123*, 105897. [CrossRef]

11. Anjana, S.; Saini, I.; Singh, P.; Yadav, A.K. Asymmetric Cryptosystem Using Affine Transform in Fourier Domain. In *Advanced Computational and Communication Paradigms*; Bhattacharyya, S., Gandhi, T., Sharma, K., Dutta, P., Eds.; Springer: Singapore, 2018; pp. 29–37.
12. Cai, J.; Shen, X. Modified optical asymmetric image cryptosystem based on coherent superposition and equal modulus decomposition. *Opt. Laser Technol.* **2017**, *95*, 105–112. [CrossRef]
13. Liu, X.; Wu, J.; He, W.; Liao, M.; Zhang, C.; Peng, X. Vulnerability to ciphertext-only attack of optical encryption scheme based on double random phase encoding. *Opt. Express* **2015**, *23*, 18955–18968. [CrossRef] [PubMed]
14. Singh, P.; Yadav, A.K.; Singh, K.; Saini, I. Optical image encryption in the fractional Hartley domain, using Arnold transform and singular value decomposition. *AIP Conf. Proc.* **2017**, *1802*, 020017.
15. Rakheja, P.; Vig, R.; Singh, P. Asymmetric hybrid encryption scheme based on modified equal modulus decomposition in hybrid multi-resolution wavelet domain. *J. Mod. Opt.* **2019**, *66*, 799–811. [CrossRef]
16. Rakheja, P.; Vig, R.; Singh, P. An asymmetric hybrid cryptosystem using equal modulus and random decomposition in hybrid transform domain. *Opt. Quantum Electron.* **2019**, *51*, 54. [CrossRef]
17. Refregier, P.; Javidi, B. Optical image encryption based on input plane and Fourier plane random encoding. *Opt. Lett.* **1995**, *20*, 767–769. [CrossRef] [PubMed]
18. 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]
19. Unnikrishnan, G.; Singh, K. Double random fractional Fourier-domain encoding for optical security. *Opt. Eng.* **2000**, *39*, 2853–2859. [CrossRef]
20. Peng, X.; Wei, H.; Zhang, P. Chosen-plaintext attack on lensless double-random phase encoding in the Fresnel domain. *Opt. Lett.* **2006**, *31*, 3261–3263. [CrossRef]
21. Vilardy, J.M.; Torres, C.O.; Jimenez, C.J. Double image encryption method using the Arnold transform in the fractional Hartley domain. In Proceedings of the 8th Iberoamerican Optics Meeting and 11th Latin American Meeting on Optics, Lasers, and Applications, Porto, Portugal, 22–26 July 2013; SPIE Proceedings; Volume 8785, p. 87851R.
22. Qin, W.; Peng, X. Asymmetric cryptosystem based on phase-truncated Fourier transforms. *Opt. Lett.* **2010**, *35*, 118–120. [CrossRef]
23. Liu, Y.; Du, J.; Fan, J.; Gong, L. Single-channel color image encryption algorithm based on fractional Hartley transform and vector operation. *Multimed. Tools Appl.* **2015**, *74*, 3171–3182. [CrossRef]
24. Singh, P.; Yadav, A.K.; Singh, K. Phase image encryption in the fractional Hartley domain using Arnold transform and singular value decomposition. *Opt. Lasers Eng.* **2017**, *91*, 187–195. [CrossRef]
25. Nishchal, N.K. *Optical Cryptosystems*; IOP Publishing: Bristol, UK, 2019.
26. Abdelfattah, M.; Hegazy, S.F.; Areed, N.F.; Obayya, S.S. Compact optical asymmetric cryptosystem based on unequal modulus decomposition of multiple color images. *Opt. Lasers Eng.* **2020**, *129*, 106063. [CrossRef]
27. Yadav, A.K.; Singh, P.; Saini, I.; Singh, K. Asymmetric encryption algorithm for colour images based on fractional Hartley transform. *J. Mod. Opt.* **2019**, *66*, 629–642. [CrossRef]
28. Zhang, Y.; Xiao, D.; Wen, W.; Liu, H. Vulnerability to chosen-plaintext attack of a general optical encryption model with the architecture of scrambling-then-double random phase encoding. *Opt. Lett.* **2013**, *38*, 4506–4509. [CrossRef] [PubMed]
29. Kumar, J.; Singh, P.; Yadav, A.K.; Kumar, A. Asymmetric Image Encryption Using Gyrator Transform with Singular Value Decomposition. In *Engineering Vibration, Communication and Information Processing*; Ray, K., Sharan, S.N., Rawat, S., Jain, S.K., Srivastava, S., Bandyopadhyay, A., Eds.; Springer: Singapore, 2019; pp. 375–383.
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]