

Article

Security Analysis of Image Encryption Based on Gyrator Transform by Searching the Rotation Angle with Improved PSO Algorithm

Jun Sang ^{1,2,*}, Jun Zhao ³, Zhili Xiang ^{1,2}, Bin Cai ^{1,2} and Hong Xiang ^{1,2}

¹ Key Laboratory of Dependable Service Computing in Cyber Physical Society of Ministry of Education, Chongqing University, Chongqing 400044, China; E-Mails: taizixzl@gmail.com (Z.X.); caibin@cqu.edu.cn (B.C.); xianghong@cqu.edu.cn (H.X.)

² School of Software Engineering, Chongqing University, Chongqing 401331, China

³ School of Automation, Huazhong University of Science and Technology, Wuhan 430074, China; E-Mail: zhaojunhust@gmail.com

* Author to whom correspondence should be addressed; E-Mail: jsang@cqu.edu.cn; Tel.: +86-23-6506-6007.

Academic Editor: Vittorio M.N. Passaro

Received: 12 July 2015 / Accepted: 31 July 2015 / Published: 5 August 2015

Abstract: Gyrator transform has been widely used for image encryption recently. For gyrator transform-based image encryption, the rotation angle used in the gyrator transform is one of the secret keys. In this paper, by analyzing the properties of the gyrator transform, an improved particle swarm optimization (PSO) algorithm was proposed to search the rotation angle in a single gyrator transform. Since the gyrator transform is continuous, it is time-consuming to exhaustedly search the rotation angle, even considering the data precision in a computer. Therefore, a computational intelligence-based search may be an alternative choice. Considering the properties of severe local convergence and obvious global fluctuations of the gyrator transform, an improved PSO algorithm was proposed to be suitable for such situations. The experimental results demonstrated that the proposed improved PSO algorithm can significantly improve the efficiency of searching the rotation angle in a single gyrator transform. Since gyrator transform is the foundation of image encryption in gyrator transform domains, the research on the method of searching the rotation angle in a single gyrator transform is useful for further study on the security of such image encryption algorithms.

Keywords: gyrator transform; image encryption; rotation angle; intelligent search; particle swarm optimization (PSO)

1. Introduction

Optical image encryption is one of the main research fields for image encryption. The basic idea is to apply random operations in optical transform domains to encrypt images. One of the typical optical image encryption techniques is the double-random phase-encoding (DRPE) technique [1]. By employing independent random phase encoding on both the input and the Fourier planes, it encodes an input image to a complex-amplitude encoded image, whose real and imaginary parts can be taken as independent stationary white noise. Following the basic idea, the image can also be encrypted in fractional Fourier transform domains [2–5]. In addition, Chen *et al.* proposed an optical image encryption method by using multilevel Arnold transform and noninterferometric imaging [6]. Reference [7] proposed ghost imaging using labyrinth-like phase modulation patterns for optical image encryption, which is highly efficient and highly secure, since only one phase-only mask should be pre-set and the labyrinth patterns occupy only a few spaces, while each labyrinth pattern possesses high randomness and flexibility. In [8], by employing a nonlinear optical correlation via a sparse phase, phase encryption with enhanced security was proposed.

Gyrator transform is a new optical transform which has been widely studied in recent years [9]. By employing the unique characteristics of gyrator transform, gyrator transform has been used for image encryption, including single image encryption [10–14], double image encryption [15–20], multi-image encryption [21], and color image encryption [22–28].

Image encryption in gyrator transform domains usually applies random operations in image gyrator transform domains to encrypt the secret image [10–28]. For example, random phase encoding may be applied in image gyrator transform domains [10–12]. In such a cryptosystem, since the rotation angle involved in gyrator transform is also one of the secret keys for image encryption, the security is higher than that of the traditional DRPE technique in the Fourier transform domain [1].

To analyze the security of image encryption in gyrator transform domains, the security of image encryption with single random phase encoding and a single gyrator transform was analyzed in [29]. For such a cryptosystem, the operation of random phase encoding only changes the phase angle of the original secret image instead of the amplitude of the image. Thus, the encryption security depends on the rotation angle used in a gyrator transform. Based on the periodicity of gyrator transform, [29] indicated that, by equally dividing the period interval $[0, 2\pi]$ of a gyrator transform with enough precision, and applying an exhaustive search, the rotation angle used in a gyrator transform can be obtained approximately with a known-plaintext attack. Then, the secret image can be decrypted with various qualities in terms of the dividing precision of the interval $[0, 2\pi]$. The analysis results may be used as a starting point for further security analysis of image encryption in gyrator transform domains.

Reference [29] focused on exhaustively searching the rotation angle used in a single gyrator transform. However, since a gyrator transform is continuous, it is time-consuming to exhaustively search for the rotation angle, even considering the periodicity of a gyrator transform and the data

precision in a computer. Thus, the computational intelligence method may be applied to speed up the searching.

In this paper, based on [29], by analyzing the properties of gyrator transform, an improved particle swarm optimization (PSO) algorithm was proposed to search for the rotation angle in a single gyrator transform. The research on the properties of a gyrator transform and the method of searching the rotation angle in a single gyrator transform is useful for further study on the security of the image encryption in gyrator transform domains.

This paper is organized as follows: in Section 2, gyrator transform is briefly introduced and analyzed. Section 3 proposes the improved PSO algorithm to search the rotation angle in single gyrator transform, while Section 4 performs the numerical simulation experiment. The final conclusions are presented in Section 5.

2. Brief Introduction and Analysis on Gyrator Transform

2.1. Gyrator Transform

Gyrator transform is a linear canonical integral transform, which introduces the rotation in position–spatial frequency planes of phase space. For a two-dimensional function $f_i(\vec{r}_i)$, the gyrator transform with rotation angle α is as Equations (1) and [9]:

$$\begin{aligned} f_o(\vec{r}_o) &= R^\alpha[f_i(\vec{r}_i)](\vec{r}_o) = \iint f_i(x_i, y_i) K_\alpha(x_i, y_i, x_o, y_o) dx_i dy_i \\ &= \frac{1}{|\sin \alpha|} \iint f_i(x_i, y_i) \left\{ \exp \left[i2\pi \frac{(x_o y_o + x_i y_i) \cos \alpha - (x_i y_o + x_o y_i)}{\sin \alpha} \right] \right\} dx_i dy_i \end{aligned} \quad (1)$$

where \vec{r}_i and \vec{r}_o are the input and output plane coordinates, respectively. α is the rotation angle.

For $\alpha = 0$ it corresponds to the identity transform, for $\alpha = \pi/2$, it reduces to the Fourier transform with a rotation of the coordinates at $\pi/2$. For $\alpha = \pi$, the reverse transform described by the kernel $\delta(r_o + r_i)$ is obtained. Meanwhile for $\alpha = 3\pi/2$, it corresponds to the inverse Fourier transform with a rotation of the coordinates at $\pi/2$ [9].

The gyrator transform is periodic with 2π . The gyrator transform can be implemented with numerical methods, according to the following three steps to transform $f_i(x, y)$ to $f_o(x, y)$:

Step 1:

$$B_\alpha(x_i, y_i) = f_i(x_i, y_i) \exp(j2\pi x_i y_i \cot \alpha) \quad (2)$$

Step 2:

$$t = \begin{cases} FFT2(B_\alpha(x_i, y_i)) & \text{if } \sin \alpha \geq 0 \\ IFFT2(B_\alpha(x_i, y_i)) & \text{if } \sin \alpha < 0 \end{cases} \quad (3)$$

where *FFT* and *IFFT* are fast Fourier transform and inverse Fourier transform, respectively.

Step 3:

$$f_o(x_i, y_i) = t \exp(j2\pi x_i y_i \cot \alpha) \quad (4)$$

2.2 Analysis on Gyrotator Transform

Suppose an image $f(x, y)$ is transformed to $g(x, y)$ with a gyrotator transform. The rotation angle used in the gyrotator transform is α . With known $f(x, y)$ and $g(x, y)$, we want to find the value of α .

Due to the continuity of the gyrotator transform, the number of the potential values of α used in the gyrotator transform is infinite. However, as [29] indicates, since the gyrotator transform is periodical with the period of 2π , the value of α may be obtained approximately by discretizing the interval $[0, 2\pi]$ with enough precision and applying an exhaustive search.

For example, apply a gyrotator transform on an image, using 2 as the value of the rotation angle. Then, equally divide the interval $[0, 2\pi]$ into 100,000 sub-intervals and use the obtained discrete values as the rotation angle in an inverse gyrotator transform to recover the image. The correlations between the recovered images and the original image were shown in Figure 1 [29].

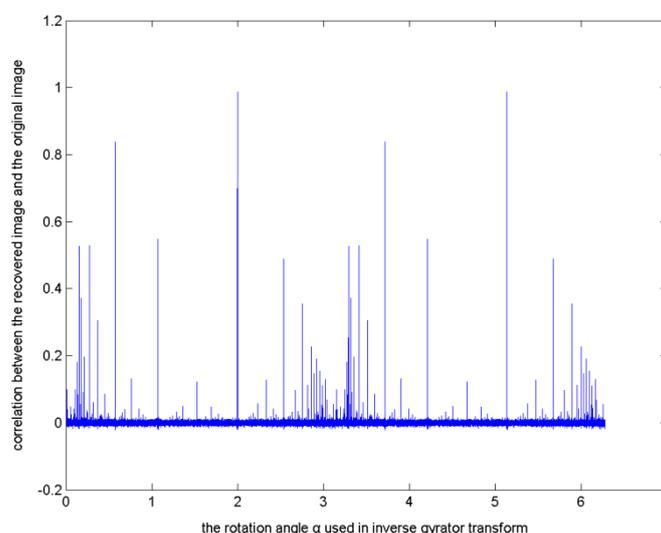


Figure 1. Correlations between the recovered images and the original image by equally dividing $[0, 2\pi]$ into 100,000 sub-intervals.

In Figure 1, the horizontal axis is the value of the rotation angle used in the inverse gyrotator transform, while the vertical axis is the correlation between the recovered image and the original image.

From Figure 1, it can be seen that, if the interval $[0, 2\pi]$ is equally divided into sub-intervals with great enough numbers, *i.e.*, discretized with enough precision, *e.g.*, 100,000, with an exhaustive search, the rotation angle used in a gyrotator transform can be obtained approximately and the original image can be recovered with high quality (the correlation being close to 1), even though the obtained rotation angle may not be the same as the original one.

In [29], it is also indicated that, the obtained approximate rotation angle can be used to recover other images transformed with the same rotation angle. It demonstrated that, taking a single gyrotator transform as a cryptosystem, by discretizing the interval $[0, 2\pi]$ with enough precision and applying an exhaustive search, the rotation angle can be obtained with a known-plaintext attack.

Obviously, due to the continuity of the gyrotator transform, to obtain the rotation angle used in a single gyrotator transform, the interval $[0, 2\pi]$ should be discretized with enough precision to apply an exhaustive search. It is time-consuming, even considering the data precision in a computer. To

accelerate the search speed, by analyzing the properties of the gyrator transform, we proposed an improved PSO algorithm to search the rotation angle used in a single gyrator transform, which will be described in the next section.

3. Improved PSO Algorithm

Particle Swarm Optimization (PSO) is a kind of evolution algorithm. It sets a swarm of particles, where each particle represents a potential solution. By evaluating each particle with the value of the fitness function, the velocity and the position of each particle are updated. The procedure of fitness-value evaluation and particle updating are repeated iteratively until an acceptable solution has been found or the maximum number of iterations is reached [30].

Since the gyrator transform has severe local convergence and obvious global fluctuations (Figure 1), it is easy to fall into a locally-optimal solution by applying the typical PSO algorithm to search for the rotation angle in a single gyrator transform. To solve such problem, an improved PSO algorithm to be suitable for such situation was proposed.

The search scope of the proposed improved PSO algorithm is dynamically changed, which is similar to using a microscope. Firstly, the rough position of the solution is observed in a large scope, usually, in the global scope. Then, by adjusting the lens, the solution is observed in a smaller scope, *i.e.*, in a local scope. This procedure may be repeated to gradually reduce the search scope until the final solution is either found or not. If the solution is not found after a certain number of iterations, amplify the observing scope for the next loop to try to search the solution again.

In the improved PSO algorithm, the basic idea of the PSO algorithm is kept, while the search stages corresponding to different search scopes are determined by the current best-fitness value.

Next, the specific procedure for searching the rotation angle in a single gyrator transform based on the improved PSO algorithm is described.

The definitions of the symbols used in the algorithm are listed in Table 1.

Table 1. The symbols used in the algorithm.

Symbol	Definition
NLoop	The maximum number of loop
NCLoop	The number of current loop
NGlobal	The maximum iterative number for global search
NCGlobal	The number of current global search
NLocal	The maximum iterative number for local search
NCLocal	The number of current local search
NParticle	The number of particle
Fitout	The fitness value when an acceptable solution is found
	The sizes of local scope for local search
SerX	X maybe 1, 2, 3, ..., n, which is corresponding to the different sizes of local scope, since the local searching scope maybe getting smaller during the search procedure
FitX	The threshold values of the fitness corresponding to different local search scopes SerX
Fitbest	Current best fitness value
Xbest	Current best particle corresponding to Fitbest

The flowchart of the algorithm is shown in Figure 2.

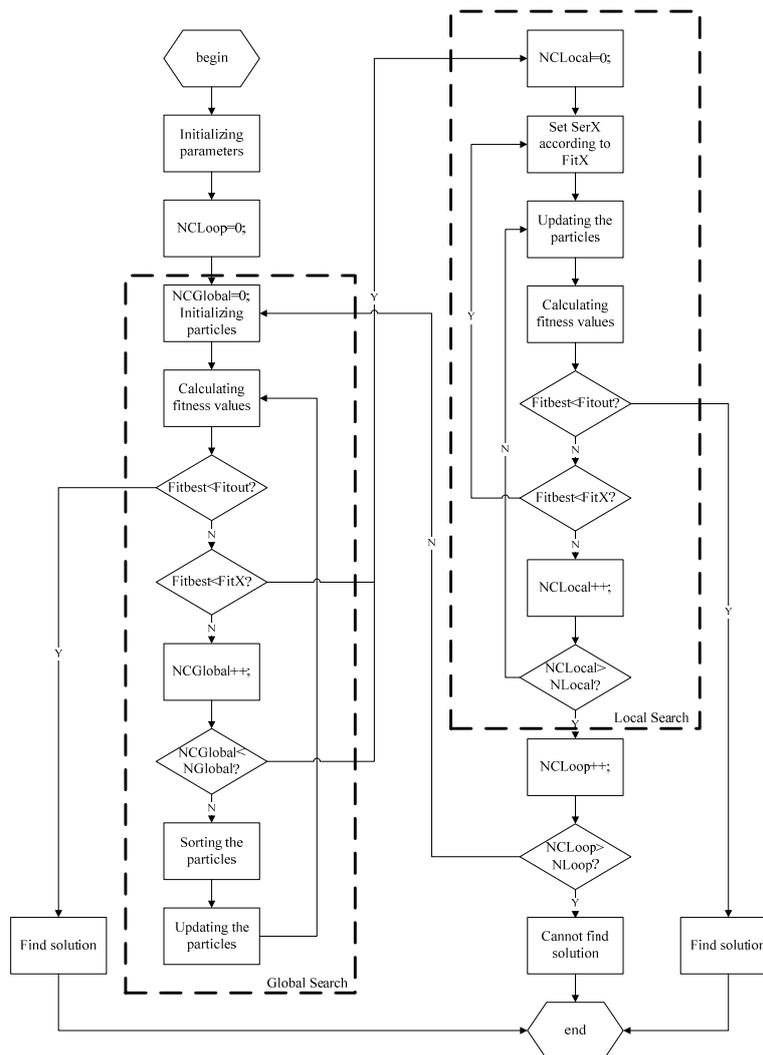


Figure 2. The flowchart of searching the rotation angle in a single gyrator transform with the improved PSO algorithm.

As Figure 2 illustrates, the procedure of the algorithm can be described as four major stages:

Stage 1: Initialize the parameters used in the algorithm, such as NLoop, NGlobal, NLocal, NParticle, Fitout, SerX, FitX, *etc.* Set NCLoop to be 0.

Stage 2: Global search.

In this stage, globally search the solution, *i.e.*, the rotation angle used in a single gyrator transform.

Firstly, the particles are initialized by being randomly generated among the interval $[0, 2\pi]$.

Secondly, the fitness values of the particles are calculated. The fitness function is the mean-square-error (MSE) between the recovered image $f'(x, y)$, by applying an inverse gyrator transform on the transformed image, $g(x, y)$ with the particle and the original image $f(x, y)$, which is defined as Equation (5):

$$MSE = \frac{1}{MN} \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} |g(x, y) - f(x, y)|^2 \quad (5)$$

If $\text{Fitbest} < \text{Fitout}$, the solution is found, output it and exit.

If $\text{Fitbest} < \text{FitX}$, go to local search with search scope SerX , and the current best particle Xbest is set to be the particle $\text{X}(1)$ used for local search.

If $\text{NCGlobal} > \text{NGlobal}$, go to local search with search scope Ser1 , and the current best particle Xbest is set to be the particle $\text{X}(1)$ used for local search. This means that if the maximum iterative number for global search NGlobal is reached, even if the threshold value SerX for any local search is not reached, the algorithm will also go to local search.

Then, sort the particles according to their fitness values from least, and the particles are updated following Equation (6).

$$x_{i+1}(j) = \begin{cases} x_i(j) & 1 \leq j \leq 5 \\ x_i(1) + 0.001 \times \text{rand}(1) & 6 \leq j \leq 10 \\ x_i(2) + 0.01 \times \text{rand}(1) & 11 \leq j \leq 15 \\ x_i(3) + 0.1 \times \text{rand}(1) & 16 \leq j \leq 20 \\ 2 \times \pi \times \text{rand}(1) & 21 \leq j \leq \text{NParticle} \end{cases} \quad (6)$$

where $x_i(j)$ is the position of current particle, $x_{i+1}(j)$ is the position of the particle after updating, and NParticle is the number of particle.

As Equation (6) shows, the updating strategy for the global search can be described as keeping the five best particles, randomly generating five particles around each of the three best particles, and randomly generating the other particles globally.

Stage 3. Local search.

In this stage, locally search the solution in a reduced scope.

The local search scope is determined by SerX corresponding to FitX as the interval $[\text{X}(1) - \text{SerX}, \text{X}(1) + \text{SerX}]$.

Firstly, the particles are updated following Equation (7).

$$x_{i+1}(j) = \begin{cases} x_i(1) & j = 1 \\ x_i(1) + \text{SerX} \times \text{rand}(1) & 2 \leq j \leq 5 \\ x_i(1) - \text{SerX} + (2 \times \text{SerX}) / (\text{NParticle} - 5) \times (j - 6) & 6 \leq j \leq \text{NParticle} \end{cases} \quad (7)$$

where $x_i(j)$ is the position of current particle, $x_{i+1}(j)$ is the position of the particle after updating, NParticle is the number of particle.

As Equation (7) shows, the updating strategy for local search can be described as keeping the best particle, randomly generating four particles around the best particle, uniformly generating the other particles in the interval $[x_i(1) - \text{SerX}, x_i(1) + \text{SerX}]$.

Then, calculate the fitness values of the particles.

If $\text{Fitbest} < \text{Fitout}$, the solution is found, output it and exit.

If $\text{Fitbest} < \text{FitX}$, where the FitX is less than the threshold value used in the current local search, locally search again in a smaller scope, and the current best particle Xbest is set to be the particle $\text{X}(1)$ used for next search. Therefore, during the local search stage, the search scope may be getting smaller.

If $\text{NCLocal} \leq \text{NLocal}$, repeat local search with current search scope.

If $\text{NCLocal} > \text{NLocal}$, the solution is not found during the local search.

Stage 4. Loop again or exit.

If $NCLoop \leq NLoop$, go to global search to repeat search again.

If $NCLoop > NLoop$, cannot find the solution and exit.

The experiments by applying the proposed improved PSO algorithm to search the rotation angle in a single gyrator transform were conducted in the next section.

4. Experiments and Analysis

The experiments were conducted under the following environment:

Computer: HP G42 Notebook

CPU: Intel Core i3 M390 @2.67 GHz

OS: Windows 8 Professional

Matlab: R2013a

The values of the parameters used in the experiments are listed in Table 2.

Table 2. The values of the parameters used in the experiments.

Parameter	Value
NLoop	20
NGlobal	40
NLocal	10
NParticle	100
Fitout	0.05
SerX	0.001, 0.0001, 0.00001, 0.000001, 0.0000005
FitX	100, 80, 60, 40, 20

The image used in the experiments was image Cameraman shown in Figure 3. Different values of the rotation angle in the gyrator transform were used to conduct the experiments several times. The experimental results were listed in Table 3.



Figure 3. Cameraman.

Table 3. The experimental results for image Cameraman with different values of rotation angle.

NGlobal	Original Rotation Angle	Obtained Rotation Angle	Fitness Value (MSE)	Number of Iteration	Used Time (s)
40	1.723456	0.868545572	0.00016785	63	156.425792
		2.427506487	0.0094	78	194.970638
		1.723456005	0	217	490.312829
		0.496425161	0.0090	77	198.694923
		2.905347971	0.0294	117	298.661654
		2.70692431	0.0285	117	291.795749
	2.523456	1.956698353	0	74	197.288178
		2.523456	0	38	98.478521
		1.035001755	0	78	198.249360

In order to compare, image Cameraman and the other three images Girl, Lena, and Testpat, shown in Figure 4, were used in the experiments and the results were list in Table 4.

**Figure 4.** (a) Image Girl; (b) Image Lena; (c) Image Testpat.**Table 4.** The experimental results for four images.

Image	Original Rotation Angle	Obtained Rotation Angle	Fitness Value (MSE)	Number of Iteration	Used Time (s)
Camerama	1.123456	0.594282984	0.000015259	38	103.03
Girl	1.123456	1.12345599	0	88	240.76
Lena	1.123456	2.050489581	0	50	119.18859
Testpat	1.123456	1.123456002	0	65	164.377708

In Tables 3 and 4, the number of iterations may be larger than NGlobal plus NLocal; because for each loop, the number of iterations is NGlobal plus NLocal. If the solution is not found, the algorithm will loop again. If the solution is found with several loops, the number of iterations is added together. On the other hand, when the maximum number of loops is reached and the solution is not found yet, it means that the solution cannot be found. According to a large number of experiments, by setting the maximum number of loops to 20, the ratio of not obtaining the solution is around 10%–15%.

To compare the time used for searching the rotation angle in a single gyrator transform, the experimental results for the above four images by using the improved PSO algorithm and the exhaustive search were listed in Table 5. Notice that for the improved PSO algorithm, the used time depends on the parameters and the original rotation angle. Here, we listed the used time for general situations following Tables 3 and 4. For the exhaustive search, according to [29], to obtain the rotation angle in a single gyrator transform, the interval $[0, 2\pi]$ should be divided into enough sub-intervals, e.g., the value of the rotation angle is accurate to six decimal places. Therefore, the time used for searching the rotation angle in a single gyrator transform was in terms of setting the value of the rotation angle to be accurate to six decimal places.

Table 5. The time used for searching the rotation angle in a single gyrator transform.

Image	Improved PSO Algorithm (s)	Exhaustive Searching (s)
Camorama	less than 500	around 71,200
Girl	less than 500	around 71,200
Lena	less than 500	around 71,200
Testpat	less than 500	around 71,200

From Tables 3–5, it can be seen that the time to obtain the rotation angle in a gyrator transform with the improved PSO algorithm is usually less than 500 s. On the contrary, if the value of the rotation angle is accurate to six decimal places, with an exhaustive search, the search time will be around 71,200 s. Obviously, with the improved PSO algorithm, the time used to search the rotation angle in a single gyrator transform decreases significantly.

More experiments were conducted on many different images with different rotation angles and different parameters, and similar results were yielded. In addition, our experiments demonstrated that, for different images transformed by a single gyrator transform with the same rotation angle, the rotation angle obtained with an image via the improved PSO algorithm can also be used to recover the other images. It indicates that, taking a single gyrator transform as a cryptosystem, the rotation angle which plays the role of secret key, can be efficiently obtained with a known-plaintext attack via the improved PSO algorithm.

It should be pointed out that the parameters used in the algorithm, such as NLoop, NGlobal, NLocal, NParticle, Fitout, SerX and FitX, *etc.* may be adjusted to be different values and the results may be different. However, in general, the search time with the proposed improved PSO algorithm is usually much less than that of exhaustive search.

From the above experimental results and discussion, it can be seen that encrypting an image with a single gyrator transform is insecure. Therefore, the image encryption methods in the gyrator transform domain usually apply iterative gyrator transforms [10–28]. With iterative gyrator transforms, the encryption security may be enhanced. However, following the existing security analysis methods for double-random-phase-encoding-based image encryption [31–36], especially the chosen-plaintext attack method [31], while combing the proposed improved PSO algorithm, the rotation angles used in iterative gyrator transforms may be obtained. This will be our future work.

5. Conclusions

For gyrator transform-based image encryption, the rotation angle used in the gyrator transform is one of the secret keys. In this paper, considering the properties of the gyrator transform, an improved PSO algorithm was proposed and applied to search the rotation angle in a single gyrator transform. The experimental results demonstrate that the proposed improved PSO algorithm can significantly improve the efficiency of searching the rotation angle of a single gyrator transform. Since gyrator transform is the foundation of image encryption in gyrator transform domains, the research on the method of searching the rotation angle in a single gyrator transform is useful for further study on the security of the image encryption algorithms based on the gyrator transform.

The basic idea of the proposed improved PSO algorithm can also be used to search the optimization solutions for other problems with the similar characteristics of severe local convergence and obvious global fluctuations.

Acknowledgments

This work was supported by Specialized Research Fund for the Doctoral Program of Higher Education of China (SRFDP) (No. 20130191110027).

Author Contributions

Jun Sang supervised entire study. Jun Sang, Jun Zhao and Bin Cai contributed to theoretical study. Jun Zhao and Zhili Xiang contributed to literature research. Jun Zhao and Jun Sang conceived and designed the experiments. Jun Zhao and Zhili Xiang performed the experiments. Zhili Xiang and Hong Xiang analyzed the data. Jun Sang, Jun Zhao and Bin Cai wrote the draft manuscript. Bin Cai and Hong Xiang contributed to manuscript definition of important intellectual content and manuscript revision. Jun Sang approved the final version of the manuscript.

Conflicts of Interest

The authors declare no conflict of interest.

References

1. Refregier, P.; Javidi, B. Optical image encryption based on input plane and Fourier plane random encoding. *Opt. Lett.* **1995**, *20*, 767–769.
2. Tao, R.; Meng, X.; Wang, Y. Image encryption with multiorders of fractional Fourier transforms. *IEEE Trans. Inf. Forensics Secur.* **2010**, *5*, 734–738.
3. Lang, J. Image encryption based on the reality-preserving multiple-parameter fractional Fourier transform. *Opt. Commun.* **2012**, *285*, 2584–2590.
4. Liu, Z.; Li, S.; Yang, M.; Liu, W.; Liu, S. Image encryption based on the random rotation operation in the fractional Fourier transform domains. *Opt. Lasers Eng.* **2012**, *50*, 1352–1358.
5. Liu, S.; Sheridan, J.T. Optical encryption by combining image scrambling techniques in fractional Fourier domains. *Opt. Commun.* **2013**, *287*, 73–80.

6. Chen, W.; Chen, X. Optical image encryption using multilevel Arnold transform and noninterferometric imaging. *Opt. Eng.* **2011**, *50*, 117001.
7. Chen, W.; Chen, X. Ghost imaging using labyrinth-like phase modulation patterns for high-efficiency and high-security optical encryption. *Europhys. Lett.* **2015**, *109*, 14001.
8. Chen, W.; Wang, X.; Chen, X. Security-enhanced phase encryption assisted by nonlinear optical correlation via sparse phase. *J. Opt.* **2015**, *17*, 035702.
9. Rodrigo, J.A.; Alieva, T.; Calvo, M.L. Gyrator transform: Properties and applications. *Opt. Express* **2007**, *15*, 2190–2230.
10. Singh, N.; Sinha, A. Gyrator transform-based optical image encryption, using chaos. *Opt. Lasers Eng.* **2009**, *47*, 539–546.
11. Liu, Z.; Xu, L.; Lin, C.; Dai, J.; Liu, S. Image encryption scheme by using iterative random phase encoding in gyrator transform domains. *Opt. Lasers Eng.* **2011**, *49*, 542–546.
12. Liu, Z.; Yang, M.; Liu, W.; Li, S.; Gong, M.; Liu, W.; Liu, S. Image encryption algorithm based on the random local phase encoding in gyrator transform domains. *Opt. Commun.* **2012**, *285*, 3921–3925.
13. Daza, S.M.; Vega, F.; Matos, L.; Moreno, C.T.; Diaz, M.L.; Daza, Y.M. Image encryption based on convolution operation in the gyrator transform domain. In Proceedings of the IECON 2012 38th Annual Conference on IEEE Industrial Electronics Society, Montreal, QC, Canada, 25–28 October 2012; pp. 1527–1529.
14. Liu, Z.; Chen, H.; Liu, T.; Li, P.; Xu, L.; Dai, J.; Liu, S. Image encryption by using gyrator transform and Arnold transform. *J. Electron. Imaging* **2011**, *20*, 013020.
15. Li, H.; Wang, Y. Double-image encryption based on iterative gyrator transform. *Opt. Commun.* **2008**, *281*, 5745–5749.
16. Liu, Z.; Guo, Q.; Xu, L.; Ahmad, M.A.; Liu, S. Double image encryption by using iterative random binary encoding in gyrator domains. *Opt. Express* **2010**, *18*, 12033–12043.
17. Liu, Z.; Zhang, Y.; Li, S.; Liu, W.; Liu, W.; Wang, Y.; Liu, S. Double image encryption scheme by using random phase encoding and pixel exchanging in the gyrator transform domains. *Opt. Lasers Technol.* **2013**, *47*, 152–158.
18. Li, H.; Wang, Y.; Yan, H.; Li, L.; Li, Q.; Zhao, X. Double-image encryption by using chaos-based local pixel scrambling technique and gyrator transform. *Opt. Lasers Eng.* **2013**, *51*, 1327–1331.
19. Wang, Q.; Guo, Q.; Lei, L. Double image encryption based on phase-amplitude mixed encoding and multistage phase encoding in gyrator transform domains. *Opt. Lasers Technol.* **2013**, *48*, 267–279.
20. Shao, Z.; Shu, H.; Wu, J.; Dong, Z.; Coatrieux, G.; Coatrieux, J.L. Double color image encryption using iterative phase retrieval algorithm in quaternion gyrator domain. *Opt. Express* **2014**, *22*, 4932–4942.
21. Wang, Q.; Guo, Q.; Lei, L. Multiple-image encryption system using cascaded phase mask encoding and a modified Gerchberg-Saxton algorithm in gyrator domain. *Opt. Commun.* **2014**, *320*, 12–21.
22. Abuturab, M.R. Color image security system using double random-structured phase encoding in gyrator transform domain. *Appl. Opt.* **2012**, *51*, 3006–3016.

23. Abuturab, M.R. Color information security system using discrete cosine transform in gyrator transform domain radial-Hilbert phase encoding. *Opt. Lasers Eng.* **2012**, *50*, 1209–1216.
24. Abuturab, M.R. Color information cryptosystem based on optical superposition principle and phase-truncated gyrator transform. *Appl. Opt.* **2012**, *51*, 7994–8002.
25. Sui, L.; Gao, B. Color image encryption based on gyrator transform and Arnold transform. *Opt. Lasers Technol.* **2013**, *48*, 530–538.
26. Chen, H.; Du, X.; Liu, Z.; Yang, C. Color image encryption based on the affine transform and gyrator transform. *Opt. Lasers Eng.* **2013**, *51*, 768–775.
27. Abuturab, M.R. Single-channel color information security system using LU decomposition in gyrator transform domains. *Opt. Commun.* **2014**, *323*, 100–109.
28. Abuturab, M.R. An asymmetric color image cryptosystem based on Schur decomposition in gyrator transform domain. *Opt. Lasers Eng.* **2014**, *58*, 39–47.
29. Sang, J.; Cai, B.; Zhang, B.; Hong, D.; Hu, H. Security analysis of random phase encoding based image encryption in gyrator transform domains. In Proceedings of the 9th International Conference on Computational Intelligence and Security, Leshan, China, 14–15 December 2013; pp. 579–582.
30. Engelbrecht, A.P. *Fundamentals of Computational Swarm Intelligence*; John Wiley & Sons: New York, NY, USA, 2005.
31. Wei, H.; Peng, X.; Zhang, P.; Liu, H.; Feng, S. Chosen-plaintext attack on double phase encoding encryption technique. *Acta Opt. Sin.* **2007**, *27*, 824–829. (In Chinese)
32. 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.
33. 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.
34. 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.
35. Qin, W.; He, W.; Meng, X.; Peng, X. Optical cryptanalysis of DRPE-based encryption systems. *Proc. SPIE* **2009**, *7512*, doi:10.1117/12.839999.
36. Nakano, K.; Suzuki, H.; Yamaguchi, M.; Obi, T.; Ohshima, N. Quantitative analysis on key estimation by known-plaintext attacks to DRPE. *Proc. SPIE* **2011**, *8011*, doi:10.1117/12.903356.