Optica Applicata, Vol. L, No. 3, 2020
DOI: 10.37190/oa200312

Image encryption scheme based on a Gaussian apertured reality-preserving fractional Mellin transform

Mengmeng WANG[1, 2], Yannis POUSSET[1], Phillippe CARRÉ[1], Clency PERRINE[1], Nanrun ZHOU[2], Jianhua WU[2*]

[1] University of Poitiers, XLIM Institute,
86962 Futuroscope-Chasseneuil Cedex, France

[2] Department of Electronic Information Engineering, Nanchang University,
Nanchang, 330031, China

[*] Corresponding author: jhwu@ncu.edu.cn

An image encryption scheme based on a Gaussian apertured reality-preserving fractional Mellin transform (GARPFrMT) is proposed. The GARPFrMT was realized in the diffraction domain. The Gaussian aperture, like a soft aperture, improved the amount of light that passed through the lens compared to a hard aperture and reduced the light leakage at the edge of the lens, assisting to some extent in resisting direct attacks. In the proposed scheme, the reality-preserving transform was constructed in the diffraction domain to ensure that the cipher-text is real. The GARPFrMT is a nonlinear transformation used for eliminating potential insecurity existing in the linear image encryption system. In order to further enhance the security of the encryption system, an Arnold transform, and a bitwise XOR operation were employed for permutation and scrambling in the encryption process. Simulation results and theoretical analysis show that the proposed algorithm is feasible and capable of withstanding several common attacks.

Keywords: image encryption, Gaussian apertured reality-preserving FrMT, Collins diffraction, Arnold transform, bitwise XOR.

1. Introduction

With the development of modern information technology, information dissemination systems play a very vital role in people's daily lives. However, although people enjoy the convenience brought by the development of information technology, the issue of information security has become increasingly prominent. Besides, there is a growing concern about image encryption in the field of information security.

Refregier and Javidi [1], in 1995, first proposed a double random-phase encoding (DRPE) algorithm in the Fourier domain for optical image encryption. Based on the DRPE algorithm, optical image encryption technology has attracted a lot of attention, and many relevant researches have been published [2–5]. Lohmann pointed out that the fractional Fourier transform (FrFT) could be implemented with an optical system by changing the position of the lens [6, 7]. Unnikrishnan and Singh [5] applied the DRPE algorithm to the optical system of FrFT with the position of the lens and the incidence wavelength as the cipher keys, which enlarges the key space. Since then, several optical image encryption algorithms based on FrFT have been proposed [7–9]. Hennelly and Sheridan also indicated that FrFT is a linear transformation, which rotates the signal through any arbitrary angle into a mixed frequency-space domain [9]. However, to some extent, the linear FrFT-based encryption system has some potential security risks [10, 11]. To avoid the disadvantages stemming from the linearity of classical DRPE, Wang and Zhao [12] proposed an encryption algorithm based on nonlinear amplitude-truncation and phase-truncation in the Fourier domain. Joshi *et al.* [13] proposed a nonlinear image encryption scheme for color images, using natural logarithms and FrFT, which showed better anti-attack performance than linear image encryption methods.

Zhou *et al.* [14–17] proposed a series of nonlinear image encryption algorithms based on fractional Mellin transform (FrMT). FrMT itself is a nonlinear transform that makes the nonlinearity of the encryption system convenient and useful. FrMT can be realized by the fractional Fourier transform by changing the coordinates from the rectangular Cartesian coordinates to the polar coordinates, as described in [14]. An opto-electronic hybrid structure for FrMT has also been proposed in [14]. Because of those proposed nonlinear encryption systems, high robustness and sensitivity to the cipher keys are achieved. To simplify encryption process and enhance the sensitivity for fractional orders of FrMT, Zhou *et al.* [15] proposed an improved encryption algorithm based on a multi-order discrete fractional Mellin transform. However, the aforementioned encryption algorithms based on FrMT [14–16] finally obtained complex-valued cipher-text. In general, complex-values have some inconvenience in display, transmission and storage. Consequently, Zhou *et al.* [17] proposed an image encryption algorithm based on a reality-preserving fractional Mellin transform (RPFrMT), whose cipher-text is real-valued data.

Generally, there are no apertures in optical image encryption systems. However, in practice, apertures always exist in most optical systems, such as the finite size of lens [18]. The implementation of the aperture can facilitate the reduction and control of light leakage in optical systems. Therefore, it is necessary and practical to analyze the performance of optical encryption systems with aperture.

This paper proposes an image encryption scheme based on a Gaussian apertured reality-preserving FrMT. The apertured FrMT is realized through the log-polar transform and apertured FrFT [19, 20]. Since the lens with Gaussian apertures is variable and non-uniform, such as a soft aperture edge diaphragm, the intensity distributions of the output laser are improved, which facilitates the resistance to possible attacks for obtaining some useful information from the marginal leakage of light in the optical encryption systems. Thus, the Gaussian aperture is chosen to construct the apertured FrMT. Within the framework of paraxial approximation, the apertured FrFT can be implemented using the Collins diffraction integral formula. To obtain the real-valued encrypted data, the nonlinear Gaussian apertured reality-preserving FrMT (GARPFrMT) is constructed. The encryption process is mainly divided into three steps, namely a GARPFrMT transform, an Arnold permutation, and a bitwise XOR operation.

The rest of this paper is arranged as follows. In Section 2, the related background is reviewed, including the principles of apertured FrFT in an optical system. In Section 3, the encryption procedures based on GARPFrMT are presented in detail. In Section 4, simulations and analysis are given. Finally, conclusions are drawn in Section 5.

2. Background

2.1. Gaussian apertured FrFT optical system

FrFT can be performed in the diffraction domain in an optical system, as shown in Fig. 1. The lens is a Gaussian lens, f is the focal length with respect to the standard focal length f_s, and $d = f_s \tan(\varphi/2)$ is the transmission distance, where $\varphi = p \times \pi/2$, p is the fractional order of the FrFT.

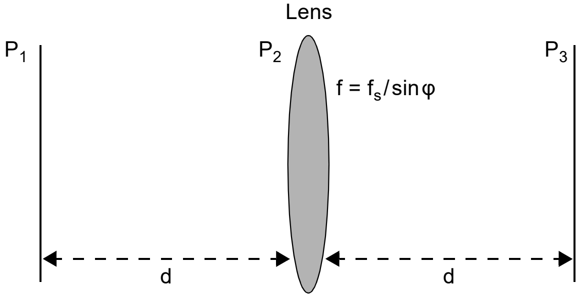

Fig. 1. An optical system for the Gaussian apertured FrFT.

Within the framework of the paraxial approximation, the field of light propagation across the optical system as shown in Fig. 1 is divided into two *ABCD* optical systems in accordance with the Collins diffraction integral formula [18]. $\{A_1, B_1, C_1, D_1\}$ and $\{A_2, B_2, C_2, D_2\}$ are respectively the elements of the transfer matrices of the two sections:

$$\begin{pmatrix} A_1 & B_1 \\ C_1 & D_1 \end{pmatrix} = \begin{pmatrix} 1 & d \\ 0 & 1 \end{pmatrix} \tag{1}$$

$$\begin{pmatrix} A_2 & B_2 \\ C_2 & D_2 \end{pmatrix} = \begin{pmatrix} A_1 & B_1 \\ C_1 & D_1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ -1/f & 1 \end{pmatrix} = \begin{pmatrix} 1 - d/f & d \\ -1/f & 1 \end{pmatrix} \tag{2}$$

For the optical field $E(x_1, y_1)$ at P_2, the following integral equation from P_1 to P_2 can be computed as:

$$E(x_1, y_1) = F_C\left[f(x_1, y_1)\right] = \frac{i}{\lambda B_1}\int_{-\infty}^{+\infty}\int_{-\infty}^{+\infty} f(x, y)$$
$$\times \exp\left\{-\frac{i2\pi}{2\lambda B_1}\left[A_1(x^2+y^2) - 2(xx_1+yy_1) + D_1(x_1^2+y_1^2)\right]\right\}\mathrm{d}x\,\mathrm{d}y \tag{3}$$

where F_C is the two-dimensional Collins diffraction transform with the incidence wavelength λ and $f(x, y)$ is the optical field at P_1.

For the optical field $E(x_2, y_2)$ at P_3, the integral equation from the lens plane P_2 to the output plane P_3 is:

$$E(x_2, y_2) = F_C\left[E(x_1, y_1)\right] = \frac{i}{\lambda B_2}\int_{-\infty}^{+\infty}\int_{-\infty}^{+\infty} E(x_1, y_1)K(x_1, y_1)$$
$$\times \exp\left\{-\frac{ik}{2\lambda B_2}\left[A_2(x_1^2+y_1^2) - 2(x_1x_2+y_1y_2) + D_2(x_2^2+y_2^2)\right]\right\}\mathrm{d}x_1\,\mathrm{d}y_1 \tag{4}$$

where $K(x_1, y_1)$ represents the Gaussian aperture shown in Fig. 2, which can be rewritten as:

$$K(x_1, y_1) = \exp(-x_1^2/\sigma^2)\exp(-y_1^2/\sigma^2) \tag{5}$$

Then, the Gaussian apertured FrFT can be implemented through formulas (1)–(5) by changing the distance d and focal length of the lens f_s.

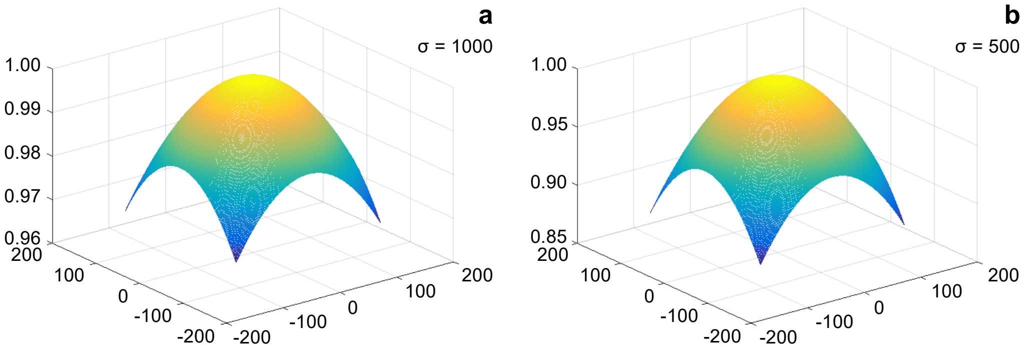

Fig. 2. Normalized intensity distributions of the Gaussian function for different standard deviations: $\sigma = 1000$ (**a**), $\sigma = 500$ (**b**), $\sigma = 200$ (**c**), and $\sigma = 50$ (**d**).

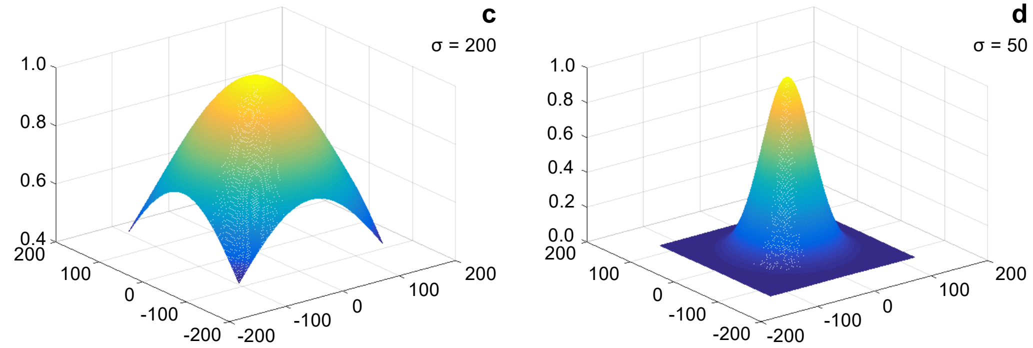

Fig. 2. Continued.

2.2. Chaotic system

The logistic map is a simple dynamic equation used to generate a numerical sequence with a complex behavior, which is defined as [21, 22]:

$$z_{l+1} = \mu z_l(1 - z_l) \tag{6}$$

where the iterative value z_l belongs to (0, 1), μ is a system parameter. The logistic map is a chaotic system when μ is within [3.57, 4].

2.3. Arnold transform

Arnold transform is a widely used scrambling transformation in image encryption systems and its general form is [23, 24]:

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 1 & b \\ a & ab+1 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \bmod N \tag{7}$$

where $[x, y]^T$ and $[x', y']^T$ are positions of an N-order matrix element before and after the Arnold transform, respectively, the operator "mod" represents the modulo operation. When $a = 1$, and $b = 1$, the transform is the common Arnold transform. The inverse Arnold transform is given as follows:

$$\begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} ab+1 & -a \\ -b & 1 \end{bmatrix} \begin{bmatrix} x' \\ y' \end{bmatrix} \bmod N \tag{8}$$

2.4. Reality preserving fractional transforms

Venturini and Duhamel [25] proposed a methodology to obtain reality-preserving forms of fractional transforms. Based on this methodology, Zhou *et al.* [17] gave a reality-preserving fractional Mellin transform. The reality-preserving fractional transform is reviewed briefly. If $x = \{x_1, x_2, ..., x_N\}^{\mathrm{T}}$ is a real one-dimensional signal, then the signal is constructed into a complex vector $\hat{\mathbf{x}}$ with length $N/2$, and N, which is even:

$$\hat{\mathbf{x}} = \{x_1 + ix_{N/2+1},\ \ x_2 + ix_{N/2+2},\ \ ...,\ \ x_{N/2} + ix_N\}^{\mathrm{T}} \tag{9}$$

where i is the imaginary unit. Then, the following calculation is performed:

$$\hat{\mathbf{Y}} = \begin{bmatrix} \mathrm{Re}(M_p) & -\mathrm{Im}(M_p) \\ \mathrm{Im}(M_p) & \mathrm{Re}(M_p) \end{bmatrix} \hat{\mathbf{x}} = B_p \hat{\mathbf{x}} \tag{10}$$

where Re(·) and Im(·) represent the real part and the imaginary part, respectively, M_p is the complex-valued discrete-fractional Mellin transform matrix with order p, size $(N/2) \times (N/2)$ [26]. The reality-preserving result of FrMT can be obtained:

$$Y = \left[\mathrm{Re}(\hat{\mathbf{Y}}),\ \ \mathrm{Im}(\hat{\mathbf{Y}})\right]^{\mathrm{T}} \tag{11}$$

3. Image encryption and decryption based on a Gaussian apertured reality-preserving FrMT

3.1. Gaussian apertured fractional Mellin transform

The Gaussian apertured fractional Mellin transform (GAFrMT) is a kind of the generalized nonlinear Mellin transform. Its nonlinearity ensures that the image encryption scheme is nonlinear and is capable of resisting a known-plaintext attack and chosen -plaintext attack. The Gaussian fractional Mellin transform is defined as follows:

$$\begin{aligned} M^{(p_1, p_2)}(u, v) = {} & C \int_{-\infty}^{+\infty} \int_{-\infty}^{+\infty} \mathrm{d}x\,\mathrm{d}y \frac{f(x, y)}{x^2 + y^2} K(x, y) \\ & \times \exp\left\{-2\pi i \left(\frac{u \ln\sqrt{x^2 + y^2}}{\sin\varphi_1} + \frac{v\,\mathrm{atan}(y/x)}{\sin\varphi_2}\right)\right. \\ & \left. + \pi i \left(\frac{u^2 + \ln^2\sqrt{x^2 + y^2}}{\tan\varphi_1} + \frac{v^2 + \mathrm{atan}^2(y/x)}{\tan\varphi_2}\right)\right\} \end{aligned} \tag{12}$$

where $K(x, y)$ is the Gaussian aperture, $\varphi_1 = p_1\pi/2$, $\varphi_2 = p_2\pi/2$, p_1, and p_2 are the fractional orders of the Gaussian apertured FrMT and C is a constant.

The Gaussian apertured FrMT can be obtained from the fractional Fourier transform with aperture by changing coordinates from rectangular Cartesian coordinates (x, y) to polar coordinates (ρ, θ). By letting $\rho = \ln\sqrt{x^2 + y^2}$ and $\theta = \mathrm{atan}(y/x)$, the relationship between the two-dimensional fractional Mellin transform and the fractional Fourier

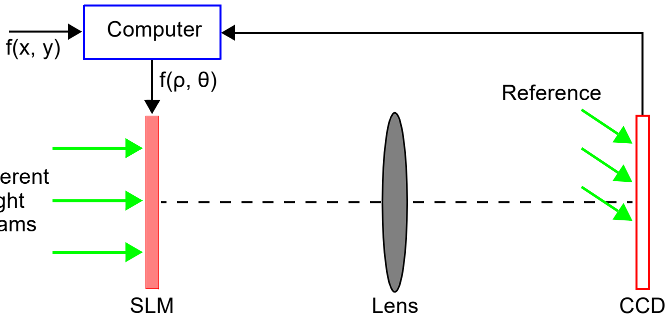

Fig. 3. Optoelectronic hybrid setup for apertured FrMT.

transform is that the Gaussian apertured FrMT can be represented by the log-polar transform and the Gaussian apertured FrFT, *i.e.*,

$$M_{\mathrm{G}}^{(p_1,\,p_2)}(u,\,v) \;=\; F_{\mathrm{G}}^{(p_1,\,p_2)}\Big(f(\rho,\,\theta)\Big) \tag{13}$$

where the operators $M_{\mathrm{G}}^{(p_1,\,p_2)}(\cdot)$ and $F_{\mathrm{G}}^{(p_1,\,p_2)}(\cdot)$ represent Gaussian apertured FrMT and Gaussian apertured FrFT having the same order $(p_1,\,p_2)$, respectively. Figure 3 shows an optoelectronic hybrid setup to transform coordinates from (x, y) to $(\rho,\,\theta)$ and to implement the Gaussian apertured FrFT.

The realization of FrMT has already been given in details by Zhou *et al.* [14]. Many parameters must be set in advance, including the geometric center of the original image (denoted as $(c_x,\,c_y)$), the outer radii of the annular domain (denoted as $r_{\max}$), and

$$r_{\max} \;=\; \max_{x,\,y}\left(\sqrt{(x-c_x)^2+(y-c_y)^2}\right) \tag{14}$$

In addition, the number of discrete sampling points along the distance axis and along the angle axis (denoted as $n_{\mathrm{r}},\, n_{\mathrm{w}}$). The GAFrMT-related parameters also should be set in advance, *i.e.*, the incidence wavelength λ, the standard focal length f_{s}, and the order p.

3.2. Gaussian apertured reality-preserving fractional Mellin transform

This paper proposes a reality-preserving transform suitable for Gaussian apertured FrMT in the diffraction domain. The details of the reality-preserving transform are as follows.

If A is a real square matrix with size $N \times N$, then it is used to construct a complex matrix B with size $N \times N/2$:

$$B(i,j) \;=\; A(i,j)+iA(i,\,N/2+j) \tag{15}$$

where $1 \le i \le N$, and $1 \le j \le N/2$.

Then the $\hat{\mathbf{Y}}$ can be obtained:

$$\begin{aligned}\hat{\mathbf{Y}} &= \left[\mathrm{Re}(M_{\mathrm{G},p}) + i\,\mathrm{Im}(M_{\mathrm{G},p})\right]\left[\mathrm{Re}(B) + i\,\mathrm{Im}(B)\right] \\ &= \left[\mathrm{Re}(M_{\mathrm{G},p})\mathrm{Re}(B) - \mathrm{Im}(M_{\mathrm{G},p})\mathrm{Im}(B)\right] + i\left[\mathrm{Im}(M_{\mathrm{G},p})\mathrm{Re}(B) + \mathrm{Re}(M_{\mathrm{G},p})\mathrm{Im}(B)\right] \\ &= \left[\mathrm{Re}(M_{\mathrm{G},p}\,\mathrm{Re}(B)) - \mathrm{Im}(M_{\mathrm{G},p}\,\mathrm{Im}(B))\right] + i\left[\mathrm{Im}(M_{\mathrm{G},p}\,\mathrm{Re}(B)) + \mathrm{Re}(M_{\mathrm{G},p}\,\mathrm{Im}(B))\right]\end{aligned} \tag{16}$$

where $M_{\mathrm{G},p}$ is the Gaussian apertured fractional Mellin transform with order p in the diffraction domain with size $N \times N/2$.

Finally, the reality-preserving result Y with size $N \times N$ is obtained:

$$Y = \left[\mathrm{Re}(\hat{\mathbf{Y}}),\ \mathrm{Im}(\hat{\mathbf{Y}})\right]^{\mathrm{T}} \tag{17}$$

3.3. Proposed image encryption and decryption scheme

The schematic of the proposed image encryption and decryption algorithm is shown in Fig. 4, and the encryption process is described as follows.

Step 1. Since the GARPFrMT is realized by the log-polar and the Gaussian apertured reality-preserving fractional Fourier transforms, the original image $f(x, y)$ is first log-polar transformed into $f(\rho, \theta)$ of size $n_{\mathrm{r}} \times n_{\mathrm{w}}$ from Cartesian coordinates (x, y) to polar coordinates (ρ, θ), as described in detail in [14].

Step 2. Then, $f(\rho, \theta)$ is regarded as the input of the Gaussian apertured reality-preserving FrFT with order p and parameter θ. Finally, the output $F(u, v)$ of the GARPFrMT can be obtained. The order p and incidence wavelength λ are regarded as cipher keys.

Step 3. The output $F(u, v)$ of the GARPFrMT is further permuted by the Arnold transform to generate a new encryption image named by $Y(u, v)$.

Step 4. Logistic map with initial values μ and z_0 is iterated to obtain a random sequence $z' = [z'_1, z'_2, \ldots, z'_p]$, where $p = n_{\mathrm{r}} \times n_{\mathrm{w}}$. The sequence z' is used to perform the bitwise XOR operation to diffuse the encrypted image $Y(u, v)$ and finally obtain

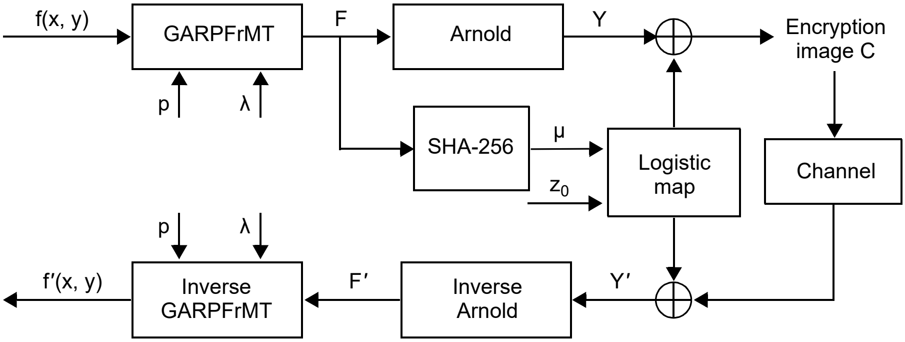

Fig. 4. Block diagram of the encryption and decryption process.

the cipher-text C. The cipher key μ used in the logistic map is generated using the SHA-256 algorithm, which is related to the output $F(u, v)$ of the GARPFrMT [27, 28]. The values μ and z_0 are used as cipher keys.

3.3.1. Decryption process

The decryption process is actually the inverse of the encryption shown in Fig. 4. First, the inverse bitwise XOR operation with cipher keys μ and z_0 is utilized to decrypt the cipher-text C. Secondly, the inverse Arnold transform is employed to recover the image $F'(u, v)$. Finally, the decrypted image $f'(x, y)$ can be recovered by performing an inverse GARPFrMT.

4. Simulation results and security analysis

A series of experiments were implemented on a computer with 3.60 GHz, GPU i7-4790 and RAM 8.00 GB using Matlab 2016(b) to analyze the proposed encryption algorithm based on GARPFrMT. The images of size 255 × 255 were considered as test plain images, since the GARPFrMT is good at processing images with odd lengths and widths.

4.1. Parameters setup

The grayscale image of *Elaine* as shown in Fig. 5, were selected as test plain images. The geometric center of the original image (c_x, c_y) is set as (128, 128), the outer radius of the annular domain is $r_{\max} = 181$. The rings and wedges were chosen as $n_r = 500$, and $n_w = 500$. The GARPFrMT-related parameters are set as: $\lambda = 632.8$ nm, $f_s = 4$ mm,

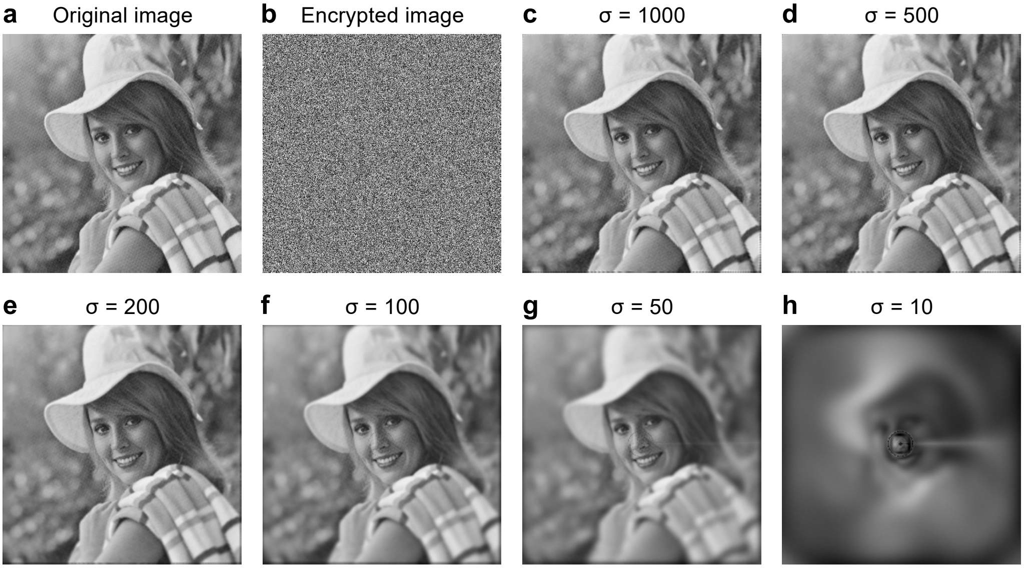

Fig. 5. Encrypted and decrypted results for different values σ: 1000, 500, 200, 100, 50 and 10; the original image *Elaine* (**a**), the encrypted image (**b**), and decrypted *Elaine* (**c**–**h**).

and the order p is set to 0.5. The initial value of the logistic map z_0 is equal to 0.32, and the parameter μ is obtained using the SHA-256 algorithm.

4.2. Encryption results and decrypted images

The simulation-encrypted results corresponding to the original image *Elaine* is shown in Fig. 5**b**, from which it can be seen that the cipher image is visually unrecognizable. There is a group of correctly decrypted images (Figs. 5**c**–5**h**) with six decryption images corresponding to six different values σ: 1000, 500, 200, 100, 50 and 10. As shown in Fig. 5, the decrypted images become blurred around the edges of the images as the value σ gradually decreases.

4.3. Histogram analysis

The histogram describes the number of pixels in the image with different gray levels and their frequency of occurrence. The histograms of cipher images should obey a fairly uniform distribution. Figure 6**a** shows the histograms of plain images. Figures 6**b**–6**d**

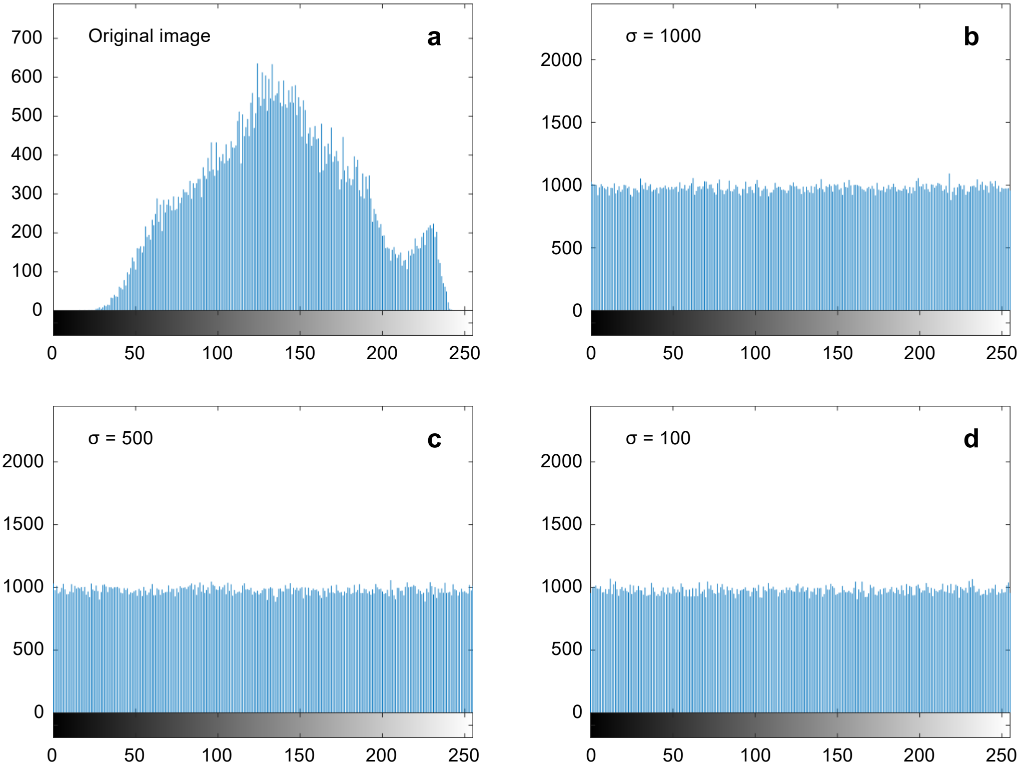

Fig. 6. Histograms of original image *Elaine* (**a**), and histograms of encrypted images for σ = 1000 (**b**), σ = 500 (**c**), and σ = 100 (**d**).

shows the histograms of cipher images for different values σ, such as 1000, 500, and 100. Obviously, the histograms of cipher images are nearly identical and almost uniformly distributed. Thus, there are reasons to believe that histograms of cipher images are no longer useful for attackers.

4.4. Correlation of adjacent pixels

As shown in Table 1, there exist strong neighborhood correlations between adjacent pixels for the original images. However, to be secured and efficient, those neighborhood correlations should not exist for encrypted images. Therefore, it is necessary to perform a correlation analysis on adjacent image pixels in cipher and plain images. The correlation coefficient between each pair is defined as

$$C = \frac{\sum_{i=1}^{N_1}(x_i - \bar{x})(y_i - \bar{y})}{\sqrt{\sum_{i=1}^{N_1}(x_i - \bar{x})^2 \sum_{i=1}^{N_1}(y_i - \bar{y})^2}} \tag{18}$$

where $\bar{x} = \dfrac{1}{N_1}\sum_{i=1}^{N_1} x_i$ and $\bar{y} = \dfrac{1}{N_1}\sum_{i=1}^{N_1} y_i$, N_1 denotes the number of adjacent pixel pairs chosen in the horizontal, vertical, and diagonal directions. Table 1 shows that the adjacent pixels of the original images have a very strong correlation, whereas those in the ciphered images for different values σ are very weak. Therefore, the proposed image encryption algorithm based on GARPFrMT is secured against correlation analysis attack.

Table 1. Correlation between two adjacent pixels.

Image	σ	Horizontal direction	Vertical direction	Diagonal direction
Plain *Elaine*		0.9589	0.9526	0.9276
Encrypted *Elaine*	1000	–0.0085	0.0055	0.0071
	500	0.0013	0.0117	0.0098
	200	0.0071	–0.0080	0.0066
	100	0.0012	0.0156	0.0015
	50	0.0051	–0.0004	0.0028
Plain *Peppers*		0.9600	0.9394	0.9083
Encrypted *Peppers*	1000	–0.0060	–0.0065	0.0046
	500	0.0071	0.0087	0.0092
	200	–0.0027	–0.0028	–0.0115
	100	–0.0034	–0.0007	0.0088
	50	0.00003	–0.0038	0.0035

4.5. Key sensitivity and key space analyses

4.5.1. Key sensitivity

In the experiments, three different control parameters $\sigma = 1000, 500, 100$ of Gaussian aperture were used to analyze the cipher key sensitivity. Figure 7 shows the decrypted results of *Elaine* with incorrect keys. Figures 7**a**–7**c** illustrates the decrypted images with an incorrect GAPRFrMT order $p = 0.6$. Figures 7**d**–7**f** presents the decrypted images with a wrong initial value for logistic map $z_0 + 10^{-15}$. The decrypted results with

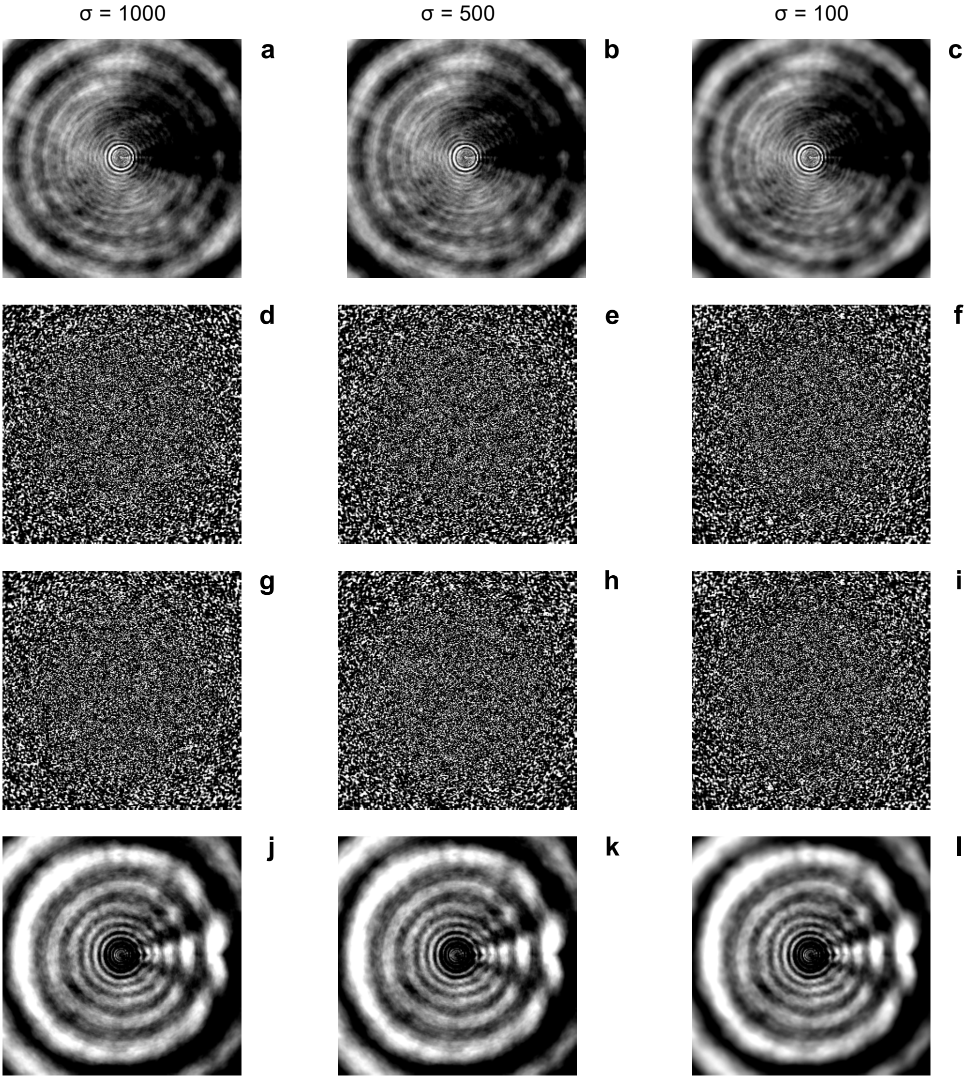

Fig. 7. Decrypted *Elaine* using incorrect cipher keys with different values σ: 1000, 500, 100. Incorrect GARPFrMT order of 0.6 (**a**–**c**), wrong initial value for logistic map $z_0' = z_0 + 10^{-15}$ (**d**–**f**), wrong parameter for logistic map parameter $\mu' = \mu + 10^{-15}$ (**g**–**i**), wrong incidence wavelength $\lambda' = \lambda + 10^{-7}$ (**j**–**l**).

a wrong parameter for logistic map $\mu + 10^{-15}$ are given in Figs. 7**g**–7**i**. The incorrect incidence wavelength $\lambda' = \lambda + 10^{-7}$ is used for the decryption process, the decrypted images are shown in Figs. 7**j**–7**l**.

4.5.2. Key space analysis

To measure the similarity between the original image and the decrypted image, the mean square error (MSE) and logarithm of mean square error (LMSE) are introduced to evaluate the quality of the decrypted images. MSE is defined as:

$$\mathrm{MSE} = \frac{1}{M_1 M_2} \sum_{i=1}^{M_1} \sum_{j=1}^{M_2} \left[f(i,j) - f'(i,j) \right]^2 \tag{19}$$

where $f(i,j)$ denotes the original image pixel, $f'(i,j)$ is the pixel of the decrypted image, M_1 and M_2 are the sizes of original and decrypted images, respectively.

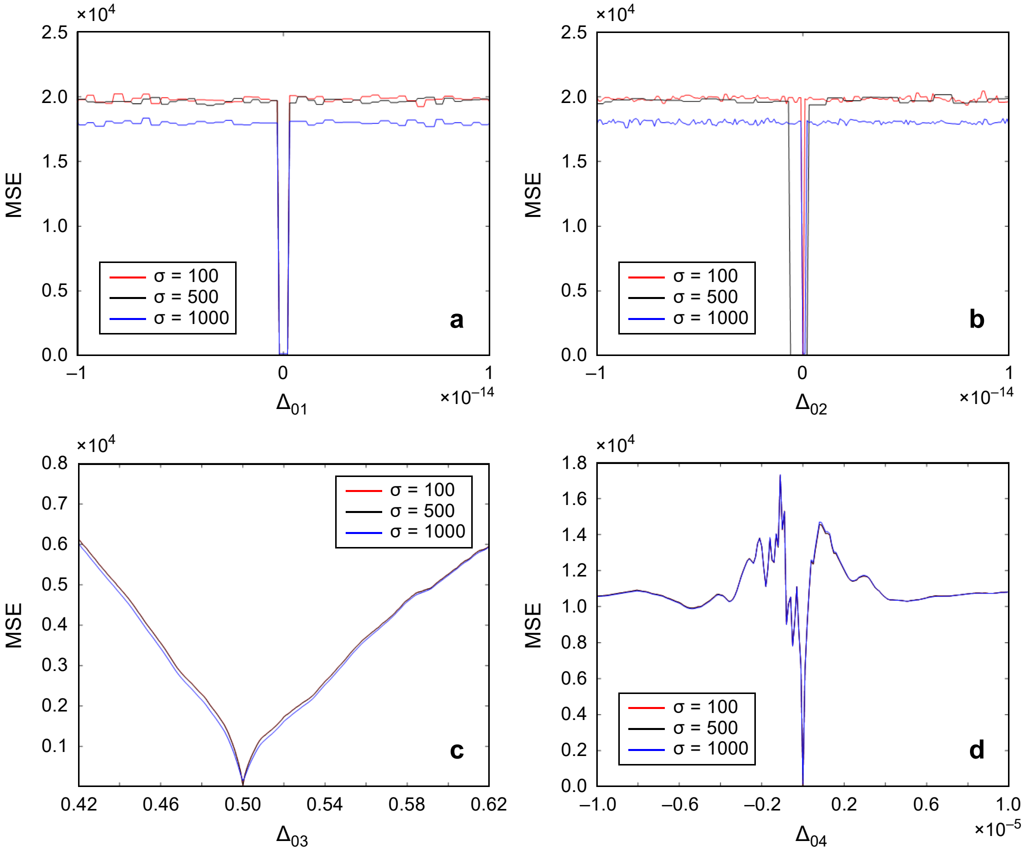

Fig. 8. MSE curves for parameter $\mu + \Delta_{01}$ (**a**), initial value $z_0 + \Delta_{02}$ (**b**), GARPFrMT order $p + \Delta_{03}$ (**c**), and incidence wavelength $\lambda + \Delta_{04}$ (**d**).

ALVAREZ and LI [29] indicated that the encryption scheme is secure when its cipher key space is at least up to 2^{100}. As can be seen from Figs. 7 and 8, the double-precision of the parameters z_0, μ of the logistic map is approximately 10^{-15}, then the value of those cipher key spaces is 10^{30}. The cipher key space for the incidence wavelength λ is 10^7. The period of the Arnold transform is 751 when the output size of GARPFrMT is 500 × 500. Therefore, the total key space is at least 10^{39}, which is greater than 2^{100}. This means that the key space is large enough to resist brute-force attacks.

In addition to a sufficiently large key space, the order p of GARPFrMT further expands the cipher key space.

4.6. Information entropy analysis

Information entropy is used to describe the randomness of image textures. The entropy H is defined as

$$H = \sum_{i=1}^{n} P(x_i) \log_2 P(x_i) \tag{20}$$

where $P(x_i)$ represents the probability of the occurrence of the pixels x_i for an n-gray level image. The results shown in Table 2 indicate that the entropies of the encrypted images for different values σ are very close to 8 [30]. Therefore, the proposed scheme has the ability to resist information entropy attacks.

Table 2. Comparison of entropies of original and encrypted images for different values σ.

Original images		Encryption image				
		$\sigma = 1000$	$\sigma = 500$	$\sigma = 200$	$\sigma = 100$	$\sigma = 50$
Elaine	7.5036	7.9993	7.9993	7.9992	7.9993	7.9993
Cameraman	7.0030	7.9992	7.9992	7.9993	7.9994	7.9993
Peppers	7.3656	7.9992	7.9993	7.9992	7.9994	7.9992

4.7. Differential attacks

The number of pixels change rate (NPCR) and the unified average changing intensity (UACI) are two commonly used quantities to test the ability of an encryption algorithm to resist differential attacks. The NPCR and UACI are represented as follows:

$$\text{NPCR} = \sum_{i=1}^{M_1} \sum_{j=1}^{M_2} D(i,j) \frac{1}{M_1 M_2} \times 100\% \tag{21}$$

$$\text{UACI} = \left[\sum_{i=1}^{M_1} \sum_{j=1}^{M_2} \frac{|C_1(i,j) - C_2(i,j)|}{255} \right] \frac{1}{M_1 M_2} \times 100\% \tag{22}$$

$$D(i,j) = \begin{cases} 0, & C_1(i,j) = C_2(i,j) \\ 1, & C_1(i,j) \neq C_2(i,j) \end{cases} \tag{23}$$

where $D(i,j)$ is a bipolar; $C_1(i,j)$ and $C_2(i,j)$ are pixel values of encrypted images of size $M_1 \times M_2$, whose original images have a 1-bit pixel difference.

The experimental NPCR and UACI are shown in Tables 3 and 4, respectively, from which it can be known that all the NPCRs and UACIs are very close to the expected values of 99.6054% and 33.4635%, respectively [30]. The results indicate that the proposed scheme is sensitive to plain-text changes.

Table 3. NPCR (%) values of encrypted images for different values σ.

Image	$\sigma = 1000$	$\sigma = 500$	$\sigma = 200$	$\sigma = 100$	$\sigma = 50$
Elaine	99.6136	99.6396	99.6056	99.6192	99.6156
Cameraman	99.5832	99.5832	99.5816	99.5956	99.6112
Peppers	99.5952	99.6176	99.5912	99.6168	99.6272

Table 4. UACI (%) values of encrypted images for different values σ.

Image	$\sigma = 1000$	$\sigma = 500$	$\sigma = 200$	$\sigma = 100$	$\sigma = 50$
Elaine	33.5040	33.5050	33.5107	33.4867	33.5570
Cameraman	33.5654	33.5294	33.4850	33.5044	33.4988
Peppers	33.4638	33.4272	33.5354	33.5366	33.5836

4.8. Robustness analysis

Since the cipher images are easily affected by noise and data loss during transmission and processing, it is necessary to measure the robustness of the proposed image encryption algorithm, noting that noise attack and occlusion attack are two effective assessment methods. Salt and pepper noise with different intensities is used to alter the decrypted images generated at different values of σ. Figure 9 shows the decrypted im-

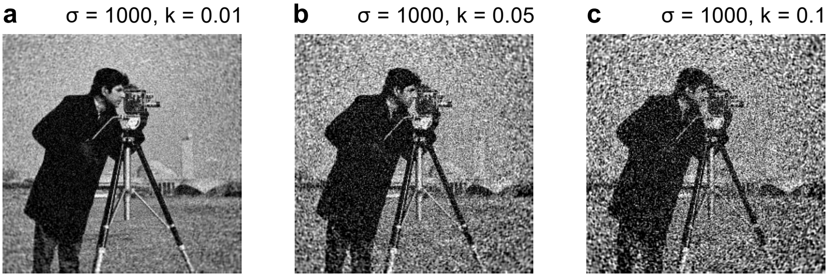

Fig. 9. Decrypted *Cameraman* with various intensities of salt and pepper noises. At different values σ, decrypted images with $k = 0.01$ (**a**, **d**, **g**), decrypted images with $k = 0.05$ (**b**, **e**, **h**), and decrypted images with $k = 0.1$ (**c**, **f**, **i**).

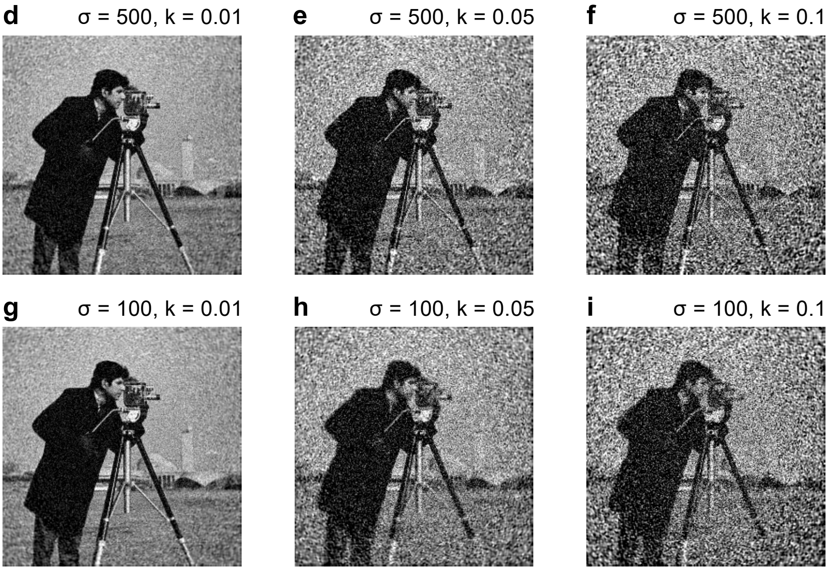

Fig. 9. Continued.

ages of *Cameraman* when k is equal to 0.01, 0.05, and 0.1, respectively. It can be seen that the major information of the original image is still visually perceptible even with a certain amount of noise added to the encrypted images.

The robustness on resisting occlusion attack was analyzed with an occlusion ratio of 1/16, 1/8, 1/4, as shown in Figs. 10**a**, 10**e**, and 10**i**, respectively. The corresponding

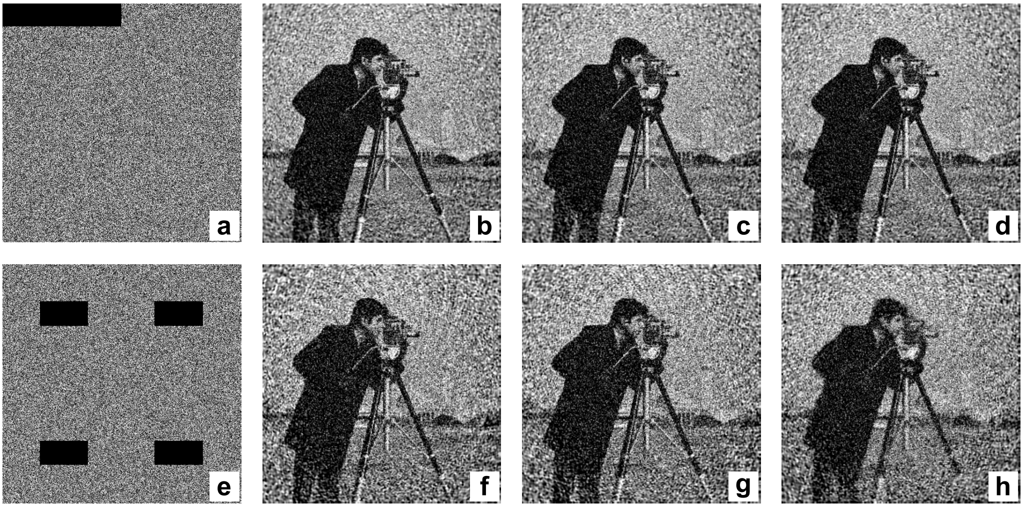

Fig. 10. Decrypted *Cameraman* with various occlusion ratios. Encrypted images with 1/16 (**a**), 1/8 (**e**), and 1/4 (**i**) occlusion. At different values σ, decrypted images with 1/16 occlusion (**b**–**d**), decrypted images with 1/8 occlusion (**f**–**h**), and decrypted images with 1/16 occlusion (**j**–**l**).

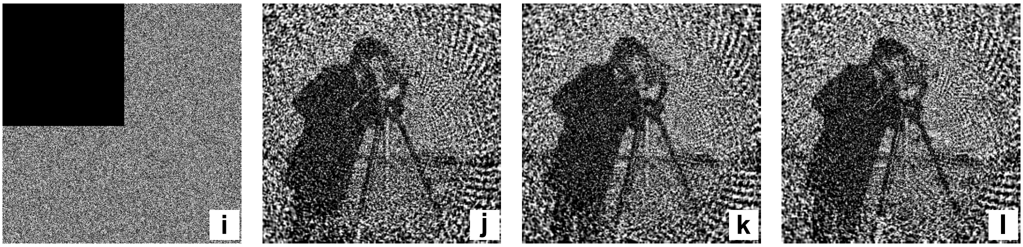

Fig. 10. Continued.

decrypted results at different values σ are presented in Figs. 10**b**–10**d**, 10**f**–10**h** and 10**j**–10**l**, respectively. As shown in Fig. 10, it is observed that the decrypted images remain visible, although the degree of data loss is different. It can be seen that the proposed scheme has a certain degree of robustness against noise and occlusion attacks.

5. Conclusion

An image encryption scheme based on the nonlinear Gaussian apertured reality-preserving fractional Mellin transform is presented. The Gaussian aperture is variable and non-uniform, and as a soft aperture edge diaphragm, the intensity distributions of the output laser are improved. The reality-preserving transform in the diffraction domain ensures that the cipher-text is real, which is convenient for display, transmission and storage. The nonlinearity of GARPFrMT can reduce the potential insecurity in an image encryption system caused by linear encryption algorithms. To further enhance the security of the encryption system, the Arnold transform and the bitwise XOR operation are adopted to encrypt the output of GARPFrMT. The simulation results demonstrate that the Gaussian aperture parameter σ influences the performance of the optical encryption system. In addition, the encryption algorithm is sensitive enough to the cipher keys, and the key space is large enough against brute-force attacks. Furthermore, the simulation results have shown that the encryption system is capable of resisting different attacks, such as known-plaintext attack, chosen-plaintext attack, and statistical analysis attacks. Besides its high security, the proposed scheme is robust with noise and occlusion attacks.

Acknowledgements – This work was partially financed by the National Natural Science Foundation of China (grant numbers 61662047, 61861029).

References

[1] Refregier P., Javidi B., *Optical image encryption based on input plane and Fourier plane random encoding*, Optics Letters **20**(7), 1995, pp. 767–769, DOI: 10.1364/OL.20.000767.

[2] Situ G.H., Zhang J.J., *Double random-phase encoding in the Fresnel domain*, Optics Letters **29**(14), 2004, pp. 1584–1586, DOI: 10.1364/OL.29.001584.

[3] He W.Q., Peng X., Meng X.F., *A hybrid strategy for cryptanalysis of optical encryption based on double-random phase–amplitude encoding*, Optics & Laser Technology **44**(5), 2012, pp. 1203–1206, DOI: 10.1016/j.optlastec.2012.01.021.

[4] Wang Y., Quan C., Tay C.J., *Asymmetric optical image encryption based on an improved amplitude–phase retrieval algorithm*, Optics and Lasers in Engineering **78**, 2016, pp. 8–16, DOI: 10.1016/j.optlaseng.2015.09.008.

[5] Unnikrishnan G., Singh K., *Double random fractional Fourier-domain encoding for optical security*, Optical Engineering **39**(11), 2000, pp. 2853–2859, DOI: 10.1117/1.1313498.

[6] Dorsch R.G., Lohmann A.W., *Fractional Fourier transform used for a lens-design problem*, Applied Optics **34**(20), 1995, pp. 4111–4112, DOI: 10.1364/AO.34.004111.

[7] Lohmann A.W., *Image rotation, Wigner rotation, and the fractional Fourier transform*, Journal of the Optical Society of America A **10**(10), 1993, pp. 2181–2186, DOI: 10.1364/JOSAA.10.002181.

[8] Chen L.F., Chang G.J., He B.Y., Mao H.D., Zhao D.M., *Optical image conversion and encryption by diffraction, phase retrieval algorithm and incoherent superposition*, Optics and Lasers in Engineering **88**, 2017, pp. 221–232, DOI: 10.1016/j.optlaseng.2016.08.013.

[9] Hennelly B.M., Sheridan J.T., *Image encryption and the fractional Fourier transform*, Optik **114**(6), 2003, pp. 251–265, DOI: 10.1078/0030-4026-00257.

[10] Peng X., Zhang P., Wei H., Yu B., *Known-plaintext attack on optical encryption based on double random phase keys*, Optics Letters **31**(8), 2006, pp. 1044–1046, DOI: 10.1364/OL.31.001044.

[11] Frauel Y., Castro A., Naughton T.J., Javidi B., *Resistance of the double random phase encryption against various attacks*, Optics Express **15**(16), 2007, pp. 10253–10265, DOI: 10.1364/OE.15.010253.

[12] Wang X.G., Zhao D.M., *Multiple-image encryption based on nonlinear amplitude-truncation and phase-truncation in Fourier domain*, Optics Communications **284**(1), 2011, pp. 148–152, DOI: 10.1016/j.optcom.2010.09.034.

[13] Joshi M., Shakher C., Singh K., *Logarithms-based RGB image encryption in the fractional Fourier domain: a non-linear approach*, Optics and Lasers in Engineering **47**(6), 2009, pp. 721–727, DOI: 10.1016/j.optlaseng.2008.11.003.

[14] Zhou N.R., Wang Y.X., Gong L., *Novel optical image encryption scheme based on fractional Mellin transform*, Optics Communications **284**(13), 2011, pp. 3234–3242, DOI: 10.1016/j.optcom.2011.02.065.

[15] Zhou N.R., Wang Y.X., Wu J.H., *Image encryption algorithm based on the multi-order discrete fractional Mellin transform*, Optics Communications **284**(24), 2011, pp. 5588–5597, DOI: 10.1016/j.optcom.2011.08.034.

[16] Zhou N.R., Li H., Wang D., Pan S., Zhou Z., *Image compression and encryption scheme based on 2D compressive sensing and fractional Mellin transform*, Optics Communications **343**, 2015, pp. 10–21, DOI: 10.1016/j.optcom.2014.12.084.

[17] Zhou N.R., Wang Y.X., Gong L., Chen X., Yang Y., *Novel color image encryption algorithm based on the reality preserving fractional Mellin transform*, Optics & Laser Technology **44**(7), 2012, pp. 2270–2281, DOI: 10.1016/j.optlastec.2012.02.027.

[18] Wang K.L., Zhao C., *Analytical solution for an anomalous hollow beam in a fractional Fourier transforming optical system with a hard aperture*, Optics & Laser Technology **44**(5), 2012, pp. 1232–1239, DOI: 10.1016/j.optlastec.2012.01.005.

[19] Sazbon D., Rivlin E., Zalesky Z., Mendlovic D., *Optical transformations in visual navigation*, Proceedings 15th International Conference on Pattern Recognition. ICPR-2000, IEEE Computer Society, Barcelona, Spain, 2000, DOI: 10.1109/ICPR.2000.902881.

[20] Sazbon D., Zalevsky Z., Rivlin E., Mendlovic D., *Using Fourier/Mellin-based correlators and their fractional versions in navigational tasks*, Pattern Recognition **35**(12), 2002, pp. 2993–2999, DOI: 10.1016/S0031-3203(02)00018-3.

[21] Zhou N.R., Jiang H., Guo L.H., Xie X.W., *Double-image compression and encryption algorithm based on co-sparse representation and random pixel exchanging*, Optics and Lasers in Engineering **110**, 2018, pp. 72–79, DOI: 10.1016/j.optlaseng.2018.05.014.

[22] Sui L., Liu B., Wang Q., Li Y., Liang J., *Color image encryption by using Yang–Gu mixture amplitude-phase retrieval algorithm in gyrator transform domain and two-dimensional Sine logistic modulation map*, Optics and Lasers in Engineering **75**, 2015, pp. 17–26, DOI: 10.1016/j.optlaseng.2015.06.005.

[23] Ding W., Qi D.X., *Digital image transformation and information hiding and disguising technology*, Chinese Journal of Computers **21**, 1998, pp. 838–843.

[24] Liu Z.J., Gong M., Dou Y.K., Liu F., Lin S., Ahmad M.A., Dai J.M., Liu S.T., *Double image encryption by using Arnold transform and discrete fractional angular transform*, Optics and Lasers in Engineering **50**(2), 2012, pp. 248–255, DOI: 10.1016/j.optlaseng.2011.08.006.

[25] Venturini I., Duhamel P., *Reality preserving fractional transforms [signal processing applications]*, 2004 IEEE International Conference on Acoustics, Speech, and Signal Processing, 2004, DOI: 10.1109/ICASSP.2004.1327083.

[26] Xin Y., Tao R., Wang Y., *Real-value encryption of digital image utilizing fractional Fourier transform*, Optical Technology **34**, 2008, pp. 498–508.

[27] Zhang Y., Tang Y.J., *A plaintext-related image encryption algorithm based on chaos*, Multimedia Tools and Applications **77**, 2018, pp. 6647–6669, DOI: 10.1007/s11042-017-4577-1.

[28] Chai X.L., Gan Z.H., Chen Y., Zhang Y.S., *A visually secure image encryption scheme based on compressive sensing*, Signal Processing **134**, 2017, pp. 35–51, DOI: 10.1016/j.sigpro.2016.11.016.

[29] Alvarez G., Li S.J., *Some basic cryptographic requirements for chaos-based cryptosystems*, International Journal of Bifurcation and Chaos, **16**(8), 2006, pp. 2129–2151.

[30] Zahmoul R., Ejbali R., Zaied M., *Image encryption based on new Beta chaotic maps*, Optics and Lasers in Engineering **96**, 2017, pp. 39–49, DOI: 10.1016/j.optlaseng.2017.04.009.

Received August 26, 2019