Single image encryption based on phase mask in Fourier transform domain

S.M.Mukane[a], S.V.Sathe[b], J.D.Gujar[b], S.D.Aaher[b]

[a]Professor, Department of Electronics & Telecommunication, SVERI's, College of Engineering, Pandharpur.

[b] Final year students of UG programme, Department of Electronics & Telecommunication, SVERI's, College of Engineering, Pandharpur.

ABSTRACT:

A single image encryption based on phase mask in Fourier transform domain is employed. Firstly, the given input image is scaled out using three generated keys. Secondly, suitable numbers of phase iterations are applied and related FFT calculations are performed. In order to increase robustness of the algorithm, some FFT shift operations are applied. Finally, argument and phase functions are separated out. At receiver side, exact reverse process is performed. The proposed algorithm has faster convergent speed. Additionally, the algorithm enlarges the key space of the cryptosystem. Numerical simulations and security analysis verifies the robustness and effectiveness of the proposed method.

1. Introduction:

In this modern age of technology, information security plays a crucial role. Images are being the more effective means of information, so image security issues have become serious in current age. As optical encryption techniques are providing excellent properties such as parallel and high speed of multi-dimensional signal processing, so they have become an emerging field for information security. In recent years, the researchers have proposed various ways of image encryption and decryption techniques based on different domains such as Fast Fourier transform domain, Fresnel transform domain, Gyrator domain and Arnold transform domain. [1]

Now a days, color image encryption has become a grievous problem and has attracted a lot of attention. Optical encryption based on double phase encoding was first proposed by Refregier and Javidi [2]. Liansheng Sui et al. [3] proposed a single-channel color image encryption using phase retrieve algorithm in fractional Fourier domain. Singh and Sinha [4,5] proposed an image encryption based on fractional Fourier transform in which he has used logistic map, the tent map and the Kaplan-Yorke map to generate chaotic random phase masks. Zhang and Karim [6] proposed a method based on an indexed image and double phase random masks to encrypt a color image. Liansheng Sui and Bo Gao [7] proposed color image encryption based on gyrator transform and Arnold transform.

There are two categories of image encryption. First is symmetric cryptosystems, where the keys are same in the encryption and decryption process whereas in asymmetric cryptosystems keys are different at both the sides. In this paper, we are working with symmetric single image encryption based on phase mask in Fourier transform domain. Plaintext image of M*N size image is taken into consideration and is firstly scaled out. Strong keys α, β and γ are generated (in the order of 10^{20}) using mathematical computations. Then, desired number of phase iterations is applied and related FFT values are calculated. Also, we are applying some fftshift operations in order to generate strong ciphertext. The amplitude and phase functions are separated to enhance image security. At decryption side, we are doing exact reverse operation as that of encryption side. The expansive applications of phase iterations and fftshift operations tend to increase robustness of proposed encryption method. Based on the results of sensitivity analysis and noise attack analysis, the proposed method achieves better sort of security. In addition to this it also provides enlargement in key space. Overall the proposed encryption method demonstrates more efficient and better secure algorithm.

The given article is organized as follows. In section 2, the fundamentals of encryption and decryption process are discussed in detail. In section 3 sensitivity analysis and noise attack analysis are performed and related simulation results are given. At the end, the conclusion and future scope is discussed.

2. Encryption and Decryption Process:

2.1 Iterative fractional Fourier transform:

The fractional Fourier transform at order α of a two dimensional function f(Xi,Yi) can be expressed as

$$\begin{aligned} f_0(x_0,y_0) &= \mathcal{F}^{\alpha}\{f_i(x_i,y_i)\}(x_0,y_0) \\ &= \int\int_{-\infty}^{+\infty} \mathcal{K}(x_i,y_i;x_0,y_0) f(x_i,y_i)\, dx_i dy_i, \end{aligned}$$

Where (Xi, Yi) and (Xo, Yo) indicates the input and output coordinates respectively, and the transform kernel is denoted as

$$A_{\phi} = \frac{\exp[-i\pi \mathrm{sgn}(\sin\phi_{\alpha})/2 + i\phi_{\alpha}]}{|\sin\phi_{\alpha}|}$$

The AΦ is a trivial phase parameter and □α =α□/2 is the transform angle . The FrFT is linear and has the property that it is index additive.

In addition, the FrFT satisfies the Parseval energy conservation theorem

$$\int\int_{-\infty}^{+\infty} |\mathcal{F}^{\alpha}[f(x_i,y_i)]|^2 dx_0 dy_0 = \int\int_{-\infty}^{+\infty} |f(x_i,y_i)|^2 dx_i dy_i.$$

These properties are very much important in color image encryption.

The Mean Square Error (MSE) is given by ,

$$MSE = \frac{\sum_{0}^{M-1}\sum_{0}^{N-1}[g-g^{k}]^2}{M \times N}$$

The Peak Signal-to-noise ratio can be calculated by,

$$\mathrm{PSNR} = 10\log_{10}\left(\frac{I_{\max}^2}{\mathrm{MSE}}\right)$$

2.2 Image encryption and decryption algorithm:

The proposed single image encryption based on phase mask in Fourier transform domain is shown in fig.1 and is described as follows

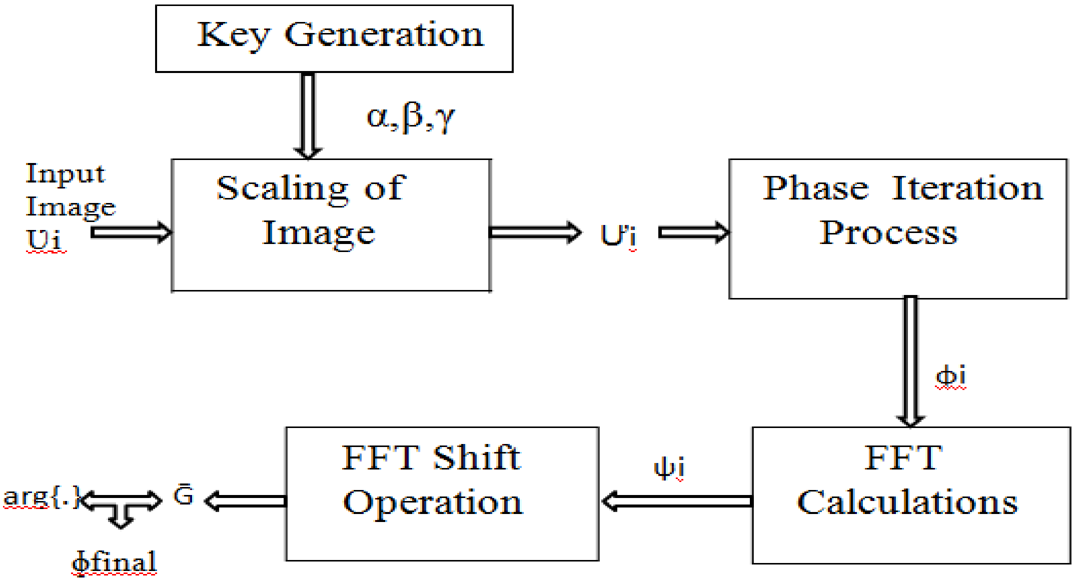

Fig. 1. Diagram of encryption process

1. The input image '□i' of size M*N is selected for encryption process. By using suitable mathematical computations three keys α, β and γ are generated. The scaling of the image is performed by using these generated keys which gives output as 'U̇i'.

2. The desired number of phase iterations are defined and related FFT calculations are performed which generates output as 'ψi'.

3. In order to increase robustness of the algorithm some FFT shift operations are applied

to generate complex interim matrix 'Ḡ'.

4. Finally, the argument and phase functions of cipher text image are separated.

Compared with the encryption, the decryption process is exactly reverse. Here, the argument and phase functions are collaborated and IFFT calculations are performed. At the end by using same keys as that of encryption side the original image can be reconstructed. The encrypted and reconstructed image is as shown in fig.3.

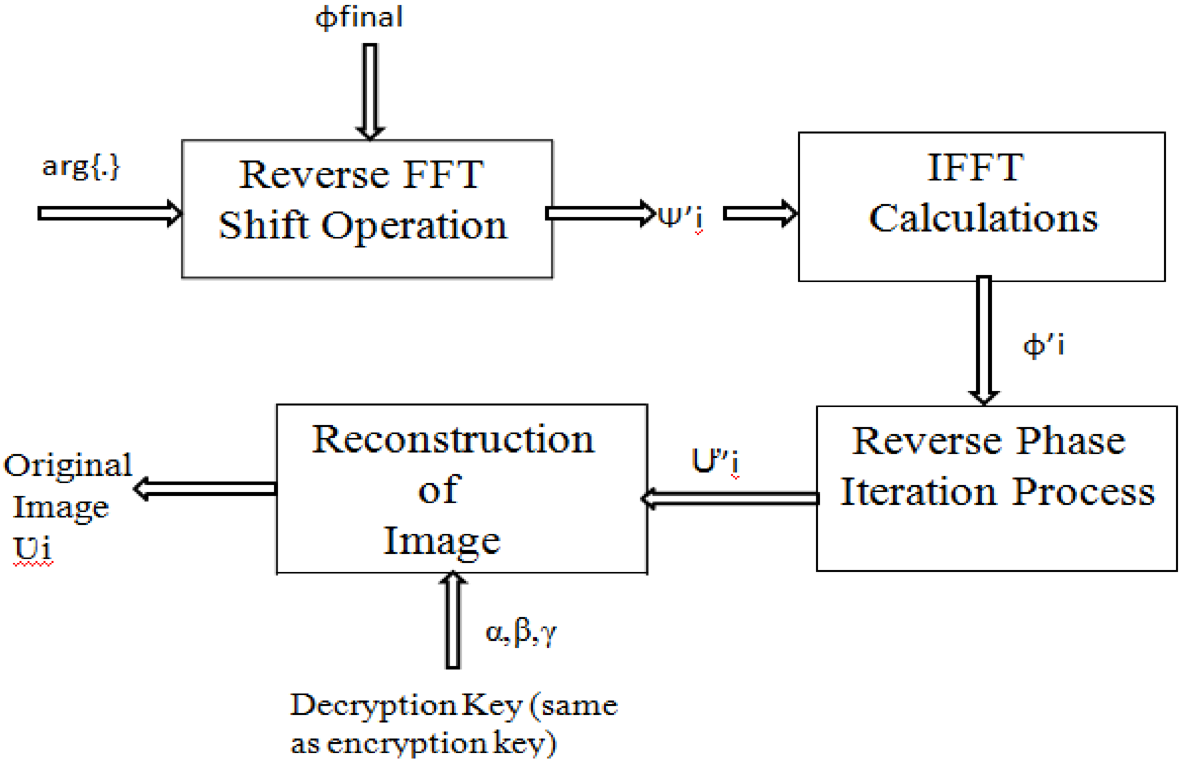
ϕfinal
arg{.}
Reverse FFT Shift Operation
ψ′i
IFFT Calculations
ϕ′i
Reverse Phase Iteration Process
U″i
Reconstruction of Image
Original Image Ui
α,β,γ
Decryption Key (same as encryption key)

Fig. 2. Diagram of decryption process

3. Numerical simulation and security analysis:

We carry out proposed algorithm on the image "cameraman.jpg" with 256 x 256 pixels.

3.1 Sensitivity analysis

Fig. 4 shows the RMSE versus number of iterations plot which signifies that after 30 iterations we are getting significant low value of the RMSE.

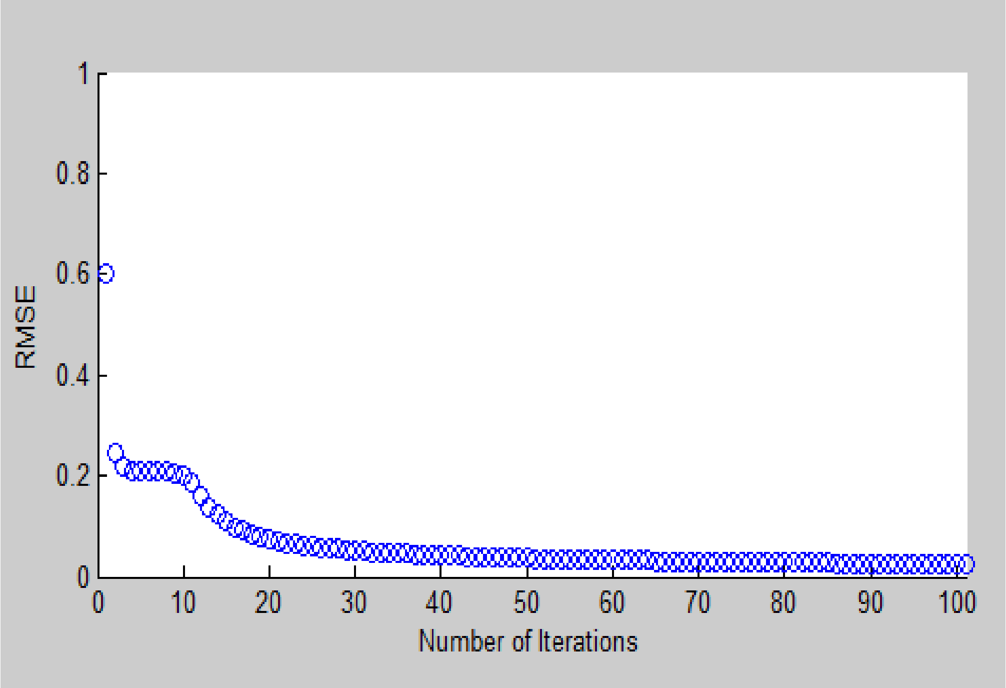

Fig. 3. Encrypted and Reconstructed Image

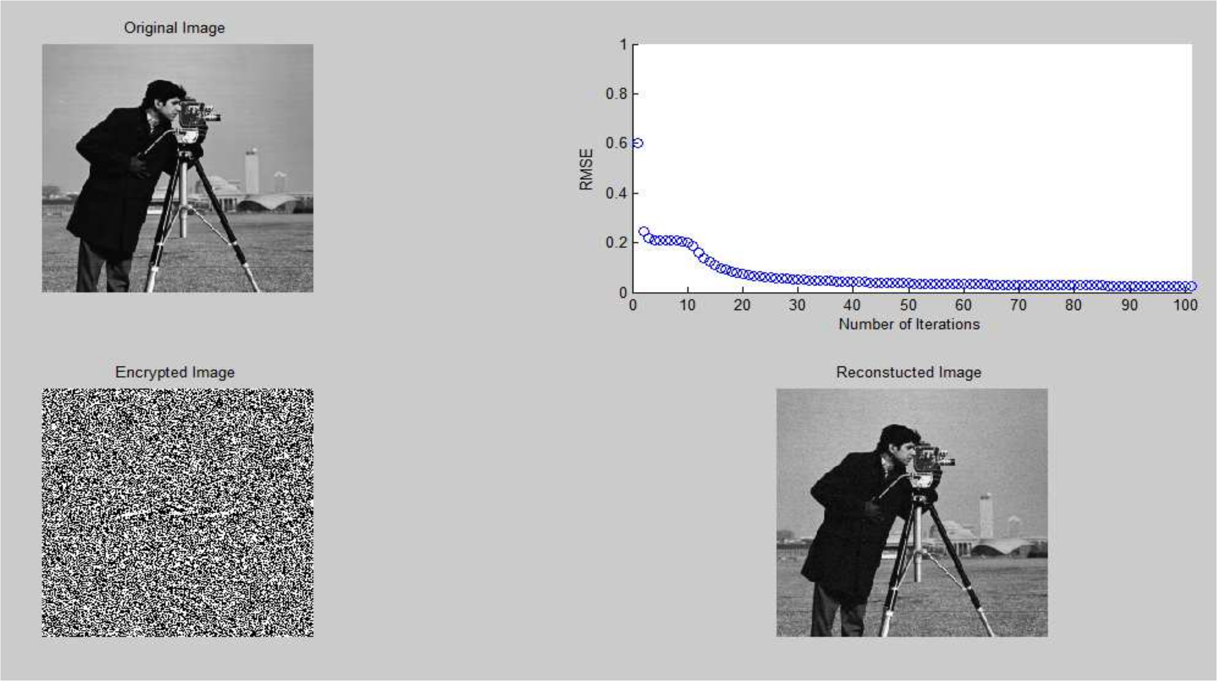

Fig. 4 RMSE versus Number of Iterations

3.2 Key space analysis

From the description of the image encryption and decryption algorithm, we realized that key space is going to play an important role at decryption side. So, we have generated key space of the cryptosystem almost equals to 10^{20}, which is enormous to resist brute-force attack.

Table 1 shows values of corresponding RMSE and PSNR with respect to number of iterations.

Number of Iteration	PSNR value	MSE value
10	-12.2923	0.1035
20	5.4853	0.0071
30	16.2866	0.0028
40	16.4956	0.0020
50	17.5812	0.0016
60	25.0132	0.0012
70	31.1059	9.2874e-04
80	32.5460	8.2855e-04
90	32.7677	7.3564e-04
100	34.0635	6.6100e-04

Table 1:- Results of Numerical Simulations

4. Conclusion:

In summary, we have proposed a single image encryption based on phase mask in Fourier transform domain. Fourier transform is the transform between spatial domain and frequency domain, and the cryptosystems based on pure encryption operation of Fourier transform suffer from some disadvantages resulted from its linearity. In order to strengthen security, we have used more number of phase iterations along with some FFT shift operations. The original image will not be recovered unless the correct keys are known. The proposed algorithm provides high convergent speed in the process of image decryption. From illustration of various numerical simulations and based on security analysis we jumps to the verdict that the proposed method is more feasible and effective against various attacks such as brute-force attack and noise attack.

Acknowledgements

This work was supported by SVERI's college of engineering, Pandharpur.

References

1. Liansheng Sui, Kuaikuai Duan, Junli Liang, Zhiqiang Zhang, Haining Meng. Asymmetric multiple-image encryption based on coupled logistic maps in fractional Fourier transform domain. Opt Lett 2014;62:139-52.
2. Refregier P, Javidi B. Optical image encryption based on input plane and Fourier plane random encoding. OptLett1995;20:767–9.
3. Liansheng Sui, Meiting Xin, Ailing Tian, Haiyan Jin. Single-channel color image encryption using phase retrieve algorithm in fractional Fourier domain. Opt Lett 2013;51:1297-1309.
4. Singh N, Sinha A. Optical image encryption using fractional Fourier transform and chaos. Optics and Lasers in Engineering 2008;46:117-23.

5. Singh N, Sinha A. Gyrator transform-based optical image encryption, using chaos. Optics and Lasers in Engineering 2008;47:539-46.
6. Zhang SQ, Karim MA. Color image encryption using double random phase encoding. Microwave and Optical Technology Letters 1999;21:318-23.
7. Liansheng Sui and Bo Gao. Color image encryption based on gyrator transform and Arnold transform. Optics and Laser Technology 2013;48:530-38.
8. Liansheng Sui, Haiwei Lu, Xiaojuan Ning, Yinghui Wang. Asymmetric double-image encryption method by using iterative phase retrieval algorithm in fractional Fourier transform domain. Optical Engineering 2014;53(2),026108.
9. Liansheng Sui and Bo Gao. Single-channel color image encryption based on iterative fractional Fourier transform and chos. Optics and Laser Technology 2013;48:117-127
10. Zhanybai T. Zhusubaliyev, ErikM. Multilayered tori in a system of two coupled logistic maps. Phys Lett A2009;373:946–51.