TELKOMNIKA Telecommunication Computing Electronics and Control
Vol. 24, No. 3, June 2026, pp. 1003~1013
ISSN: 1693-6930, DOI: 10.12928/TELKOMNIKA.v24i3.27650

Enhancing image security through nonlinear preprocessing and double random phase encoding using fractional fourier transform

Fayçal Radjah[1], Nacira Diffellah[2], Tewfik Bekkouche[3], Lahcene Ziet[1]
[1]LEPCI Laboratory, Department of Electronics, Faculty of Technology, University of Setif 1, Setif, Algeria
[2]LMSE Laboratory, Institute of Electronics and Telecommunications IET, University of Mohamed El Bachir El Ibrahimi, Bordj Bouarreridj, Algeria
[3]LMSE Laboratory, Department of Automatic and Intelligent Systems, Faculty of Technology, University of Setif 1, Setif, Algeria

Article Info

Article history:

Received Nov 1, 2025
Revised Feb 25, 2026
Accepted Mar 29, 2026

Keywords:

Confusion-diffusion
Double random phase encoding
Fractional fourier transform
Key sensitivity
Nonlinear preprocessing

ABSTRACT

Image encryption is crucial for secure data transmission in fields such as IoT, medical imaging, and biometrics. This paper proposes an enhanced encryption framework that combines nonlinear preprocessing with double random phase encoding (DRPE) using the fractional fourier transform (FrFT). The diffusion process replaces the conventional XOR operation with a nonlinear hyperbolic tangent (tanh) function, improving confusion diffusion complexity and resistance to cryptanalytic attacks. Experimental results show a reduction in peak signal-to-noise ratio (PSNR) from 9.03 dB to 7.25 dB and a mean squared error (MSE) increase to 10×10^3, indicating stronger encryption and lower correlation with the original image. The proposed method also enhances robustness against histogram and key-sensitivity attacks. Statistical analyses, including entropy and number of pixels change rate (NPCR) metrics, demonstrate that the approach outperforms conventional DRPE methods while maintaining computational efficiency. This hybrid nonlinear and FrFT-based framework provides a practical and scalable solution for secure image transmission in sensitive and real-time applications.

Corresponding Author:

Tewfik Bekkouche
LMSE Laboratory, Department of Automatic and Intelligent Systems, Faculty of Technology
University of Setif 1
Setif, Algeria
Email: toufik.bekkouche@univ-bba.dz

1. INTRODUCTION

With the rapid expansion of digital communication technologies, ensuring secure transmission of visual information has become a critical challenge in applications such as medical imaging, biometric authentication, internet of things (IoT), and secure multimedia systems. Due to their high redundancy and strong inter-pixel correlation, images are particularly vulnerable to unauthorized access, making robust image encryption techniques essential for protecting sensitive data [1], [2].

Image encryption methods are generally classified into spatial-domain and transform-domain approaches. Spatial-domain schemes mainly rely on confusion diffusion architectures, where pixel positions are permuted and pixel values are modified, typically using XOR operations combined with chaotic maps [3]-[5]. While these methods are computationally efficient, several studies have demonstrated that XOR-

based diffusion remains fundamentally linear, which limits resistance to statistical, differential, and chosen-plaintext attacks [6]-[11].

Transform-domain and optical encryption techniques have been extensively investigated as alternatives to spatial-domain schemes. Among them, double random phase encoding (DRPE) has emerged as a prominent optical encryption method due to its simplicity and compatibility with optical systems [12]. To enhance its security, DRPE has been extended using advanced transforms such as the fractional fourier transform (FrFT) and its variants, including multiple-parameter FrFT and discrete fractional transforms, which significantly enlarge the key space and improve encryption flexibility [13]-[16]. Moreover, chaos-based mechanisms have been widely integrated into DRPE frameworks to increase key sensitivity and strengthen resistance against brute-force and statistical attacks [17]-[24].

Despite these improvements, several cryptanalysis studies have revealed that DRPE and its FrFT-based extensions remain vulnerable to attacks exploiting their inherent linear structure, such as iterative phase-retrieval attacks and chosen-plaintext attacks [25], [26]. These vulnerabilities highlight that simply increasing key space or transform complexity is insufficient to guarantee strong security if the underlying encryption process remains linear.

Motivated by these findings, this paper proposes a novel nonlinear preprocessing scheme integrated with an FrFT-based DRPE framework. Unlike conventional approaches that rely on XOR-based diffusion, the proposed method replaces the XOR operator with a hyperbolic tangent (tanh) nonlinear diffusion function coupled with chaotic sequences. This design directly addresses the linear weakness of classical DRPE-based systems and spatial diffusion schemes. The main contribution of this work lies in demonstrating that the proposed tanh-based nonlinear diffusion significantly enhances encryption robustness, key sensitivity, and resistance to statistical and cryptanalytic attacks, while preserving computational efficiency and suitability for opto-digital image encryption systems.

2. METHOD

This section is organized into five relevant subsections that provide the necessary foundations for understanding the core contributions of the proposed encryption framework.

2.1. Logistic map

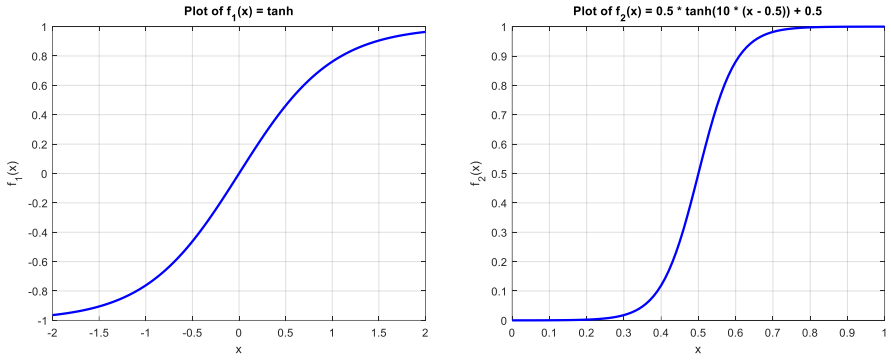
The iterative expression of the Logistic map sequence is given (1):

$$x_{i+1} = r \times x_i \times (1 - x_i) \tag{1}$$

where x_0 is the initial condition value $\in [0\ 1]$ and $r \in [3.9, 4]$ is the control parameter.

2.2. Normalised hyperbolic tangent function

As illustrated in Figure 1(a), the hyperbolic tangent function exhibits strong nonlinear characteristics. To ensure that pixel values remain confined within the interval [0,1], the function is normalized, leading to the normalized hyperbolic tangent (Ntanh) function shown in Figure 1(b). This normalization preserves compatibility with image data while maintaining the desired nonlinear behavior. The introduction of the Ntanh function aims to increase diffusion nonlinearity, thereby improving resistance against statistical and differential cryptanalytic attacks.



(a) (b)

Figure 1. The plot: (a) hyperbolic tangent function $f_1(x)$ and (b) normalized hyperbolic tangent function $f_2(x)$

$$f_1(x) = tanh(x) \quad (2)$$

$$f_2(x) = 0.5 \times tanh(10 \times (x - 0.5)\ ) + 0.5 \quad (3)$$

2.3. Confusion diffusion architecture

The confusion-diffusion architecture, is a widely used image encryption technique operating in the spatial domain. It comprises two main stages: confusion and diffusion. The confusion stage rearranges the pixel positions of an image without altering their values, while the diffusion stage modifies the pixel values using an XOR operation. The detailed process of this architecture is outlined below, incorporating a chaotic function for enhanced security:

a. Let I_m represent the original image of size $m \times n$. Reshape I_m into a one-dimensional vector I of size $1 \times m \times n$.
b. Use the logistic chaotic map to generate a chaotic sequence $s(x_0, r_0)$ of the same size as I. Here, $x_0 \in [0\ 1]$ is the initial value, and $r_0 \in [3.9\ 4]$ is the control parameter.
c. Rearrange the pixels of I based on the ascending order of the values in the sequence $s(x_0, r_0)$, producing a new vector I'.
d. Generate another chaotic sequence $s'(x_1, r_1)$ using logistic map. Convert this sequence from the range [0,1] to [0,255] by: $s'' = round(s' \times 255)$.
e. Apply a recursive bitwise XOR operation between I' and s'' to produce an encrypted vector y as:
$$y_k = \begin{cases} s_k'' \oplus I_k', & k = 1 \\ s_k'' \oplus I_k' \oplus y_{k-1}, & k = 2,3,4, \dots\dots\dots, m \times n \end{cases}$$
Here, k represents the pixel index in the vector.
f. Reshape the encrypted vector y back into a two-dimensional matrix of size $m \times n$, yielding the final encrypted image E_m.

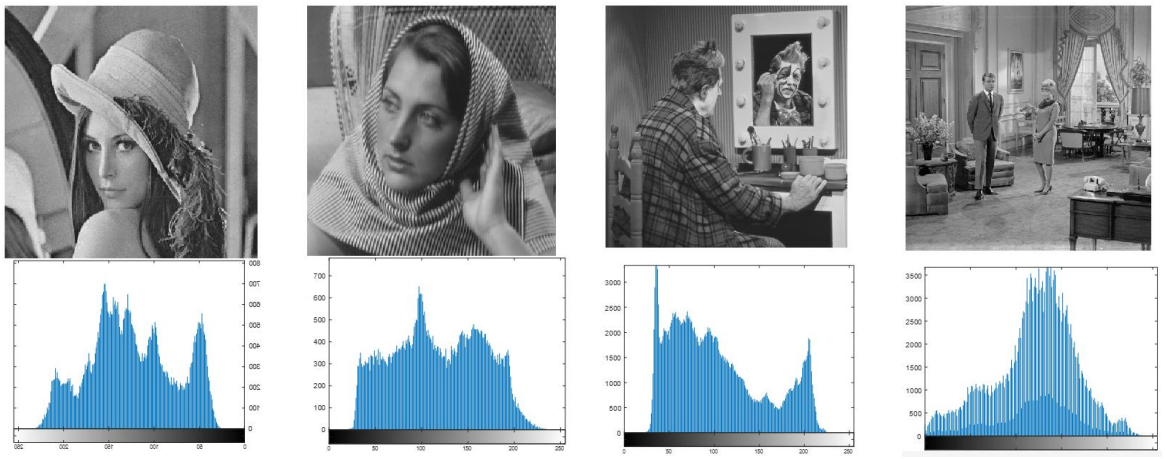
Once the nonlinear confusion–diffusion preprocessing is completed, the resulting encrypted image is not transmitted directly. Instead, it serves as the input to the transform-domain encryption stage. In this work, the output of the proposed tanh-based nonlinear diffusion is subsequently processed by a FrFT-based DRPE scheme, enabling a tight coupling between spatial-domain nonlinearity and frequency-domain encryption.

To assess the performance of the proposed nonlinear preprocessing technique Ntanh compared to the traditional XOR-based diffusion, four standard test images lena, barbara, clown, and livingroom were utilized, as illustrated in Figures 2(a) to (d), respectively. All simulations were conducted using MATLAB 2018, and the evaluation was based on three metrics:

a. Peak signal-to-noise ratio (PSNR): PSNR is a widely used metric in encryption schemes to measure the similarity between the original and encrypted images. A lower PSNR value indicates higher encryption strength and less resemblance to the original image.
b. Correlation coefficient: this metric evaluates the statistical dependence between the original and encrypted images, or between adjacent pixels in the encrypted image. A value close to zero or negative implies a better encryption quality as it indicates minimal correlation.
c. Entropy: entropy measures the randomness in the encrypted image. A value closer to the ideal value of 8 bits (for grayscale images) reflects better randomness and enhanced security against cryptographic attacks.

Results presented in the Table 1 provide a comparative analysis between the proposed nonlinear preprocessing technique (Ntanh) and the traditional XOR-based diffusion method based on three metrics: PSNR, correlation, and entropy. The PSNR values for the nonlinear preprocessing (Ntanh) are consistently lower than those for XOR-based diffusion across all tested images. For example, for the lena image, the PSNR with Ntanh is 7.2577 dB, compared to 9.2632 dB for XOR. This trend is consistent for all other images as well. A lower PSNR indicates that the encrypted image is more dissimilar to the original, suggesting that Ntanh provides a higher level of security. The correlation values for Ntanh are significantly closer to zero or negative compared to the XOR-based method, indicating a better decorrelation of pixel values in the encrypted images. For instance, the correlation for the Lena image with Ntanh is -7.1129×10^{-4}, compared to 0.0072 for XOR. This improvement is observed in most cases, demonstrating the effectiveness of Ntanh in reducing statistical dependencies and enhancing encryption quality. The entropy values for Ntanh are slightly lower than those for XOR-based diffusion, suggesting a marginal reduction in randomness. For example, the entropy for the Lena image with Ntanh is 7.2345, while XOR achieves 7.9968. Although XOR achieves values closer to the ideal 8-bit randomness, the difference is minimal, and Ntanh still offers acceptable randomness levels for encryption purposes. The nonlinear preprocessing technique (Ntanh) shows superior performance in terms of reducing PSNR and correlation, which are critical metrics for encryption robustness. Although XOR-based diffusion achieves marginally higher entropy, Ntanh still ensures sufficient

randomness for secure encryption. These findings highlight the potential of the proposed Ntanh method in enhancing the overall security of image encryption systems.



(a) (b) (c) (d)

Figure 2. Standard tested images and their corresponding histograms: (a) lena, (b) barbara, (c) clown, and (d) livingroom

Table 1. Results of image encryption metrics for Ntanh and XOR-based diffusion techniques

Image	PSNR (dB)		Correlation		Entropy	
	Ntanh	XOR	Ntanh	XOR	Ntanh	XOR
Lena 256×256	7.2577	9.2632	-7.1129×10^{-4}	0.0072	7.2345	7.9968
Baebara 256×256	7.0353	9.1266	-0.0062	-0.0034	7.0934	7.9974
Livingroom 512×512	7.8946	9.3931	9.9606×10^{-4}	-4.9812×10^{-4}	7.5647	7.9992
Clown 512×512	6.9417	8.6731	2.3376×10^{-5}	2.3376×10^{-5}	6.3270	7.9993

2.4. Nonlinear preprocessing applied to FrFT based-DRPE

The nonlinear preprocessing stage modifies the statistical and structural characteristics of the input image by introducing strong nonlinearity in the diffusion process. The nonlinearly diffused image obtained from the previous stage is then embedded into the FrFT-based DRPE framework. Within the DRPE process, the preprocessed image is multiplied by a first random phase mask, transformed into the fractional fourier domain using randomly selected FrFT orders, and subsequently multiplied by a second random phase mask before applying the inverse FrFT [27]-[29]. The random phase masks and fractional orders constitute additional secret keys that significantly enlarge the key space. By introducing nonlinearity prior to the FrFT-based DRPE, the proposed framework effectively disrupts the linear relationship between plaintext and ciphertext that characterizes conventional DRPE systems. This integration enhances resistance to cryptanalytic attacks while preserving the flexibility and scalability of transform-domain encryption. Figure 3 illustrates the overall architecture of the proposed nonlinear preprocessing combined with FrFT-based DRPE.

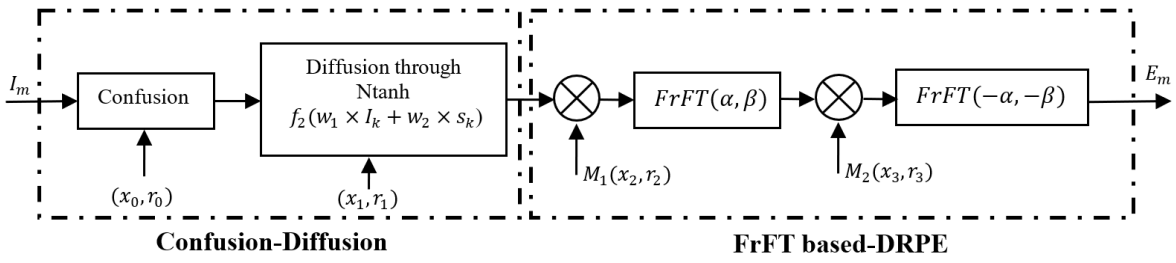


Figure 3. Nonlinear preprocessing applied to FrFT based-DRPE

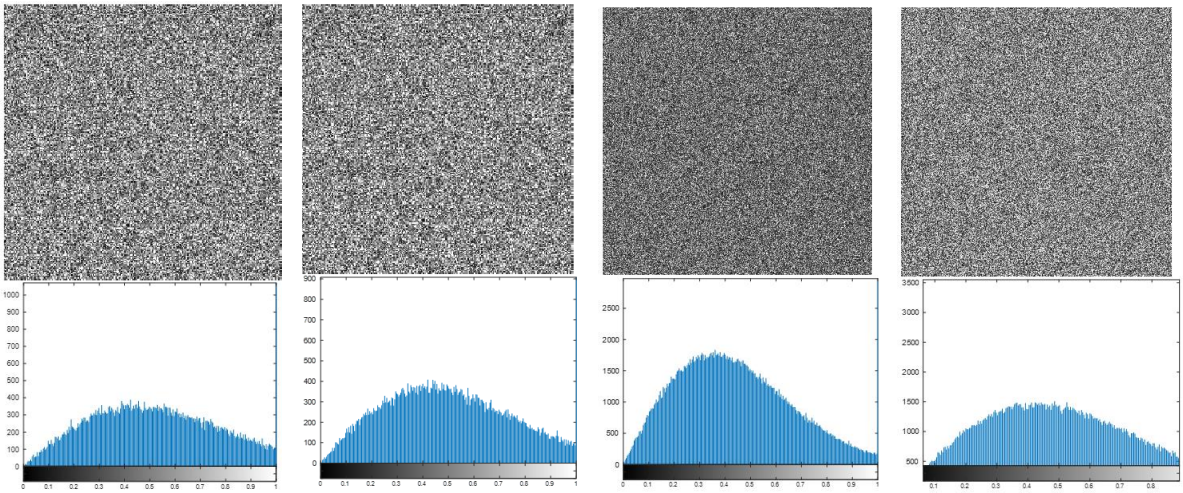
3. RESULTS AND DISCUSSION

To demonstrate the effectiveness and security of the proposed image encryption scheme, extensive simulations and analyses were performed. The results encompass histogram analysis, data loss impact, noise robustness, key sensitivity, and key space evaluation, as detailed below. All tests were conducted using standard images and metrics in MATLAB, following the methodology outlined in the previous sections for a fair comparison. For all experiments, the parameters of the chaotic maps and the FrFT were fixed unless otherwise stated. The logistic map was employed for chaotic sequence generation with control parameters $\mu = 3.999$ to ensure a fully chaotic regime, and initial conditions $x_0 \in (0,1)$ selected with a precision of 10^{-14}. Independent chaotic sequences were used for confusion, nonlinear diffusion, and random phase mask generation to avoid parameter reuse and correlation.

The FrFT-based DRPE stage utilized two independent fractional orders α_1 and α_2, randomly selected from the interval (0, 1). The random phase masks were generated using chaotic sequences uniformly mapped to the interval [0, 2 π]. All simulations were implemented in MATLAB 2018 on grayscale test images of sizes 256×256 and 512×512, ensuring a consistent and fair evaluation across all experiments.

3.1. Histogram analysis

The encrypted images produced by the proposed FrFT-based DRPE with nonlinear preprocessing exhibit nearly uniform histograms. In other words, the statistical distribution of pixel intensities in the cipher images is flat and bears no visible resemblance to the histograms of the original images, as illustrated in as illustrated for lena (Figure 4(a)), barbara (Figure 4(b)), clown (Figure 4(c)), and livingroom (Figure 4(d)). This uniformity indicates that an attacker cannot gain any meaningful information from the cipher by examining its histogram. The striking similarity among histograms of different encrypted images underscores the algorithm's robustness against histogram-based attacks. An adversary attempting statistical analysis on the encrypted data would find no characteristic peaks or patterns to exploit, confirming that the encryption effectively conceals the original image structure.



(a) (b) (c) (d)

Figure 4. Encrypted images and their corresponding histograms: (a) lena, (b) barbara, (c) clown, and (d) livingroom

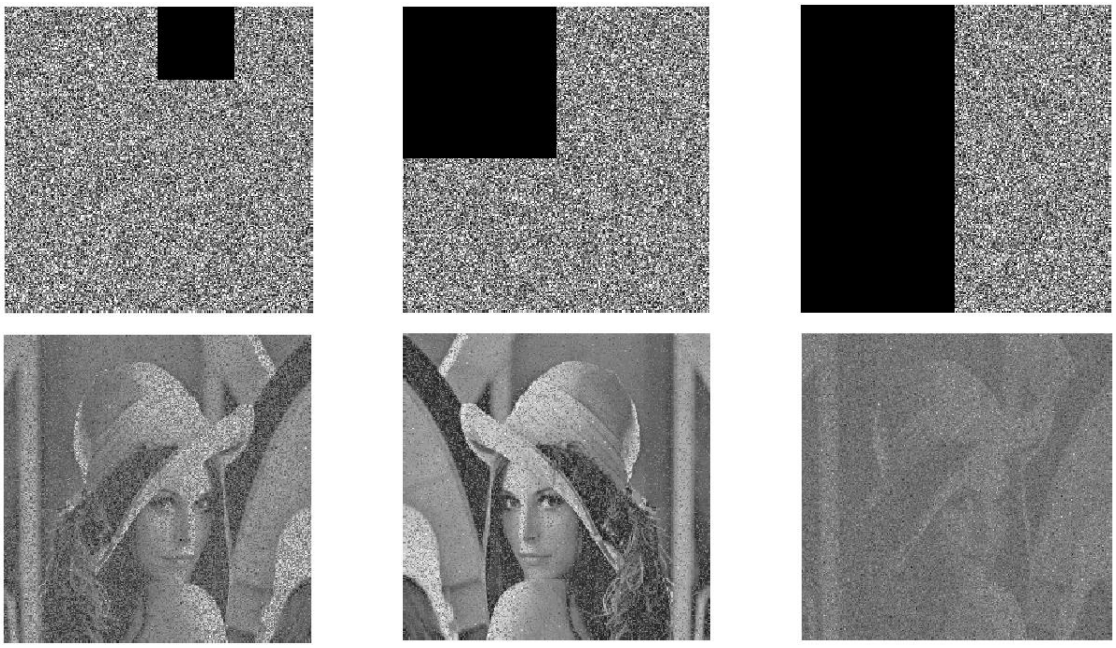
3.2. Data loss analysis

To evaluate the robustness of the proposed encryption scheme against partial data loss, controlled data-loss experiments were conducted on the encrypted images, as illustrated in Figure 5. This scenario simulates practical transmission impairments such as packet loss or intentional data removal attacks. Specifically, 12% (Figure 5(a)), 25% (Figure 5(b)), and 50% (Figure 5(c)) of the encrypted image data were randomly removed before the decryption process. Both qualitative and quantitative analyses were performed on the decrypted images. As the percentage of data loss increases, the visual quality of the decrypted images degrades rapidly, with the original image structure becoming unrecognizable even at moderate loss rates. This behavior indicates that the proposed encryption scheme does not tolerate partial ciphertext loss, which is a desirable property from a security perspective. To provide an objective evaluation, PSNR, number of pixel change rate (NPCR), and unified average changing intensity (UACI) were computed for each data-loss

scenario. The results demonstrate a sharp decline in PSNR values as data loss increases, while NPCR values consistently exceed 99% and UACI values remain close to the ideal value of 33%. These metrics confirm that even partial loss of encrypted data leads to widespread error propagation in the decrypted images, effectively preventing any meaningful information recovery. The quantitative results are summarized in Table 2.

Table 2. Quantitative results under data loss attacks

Data loss (%)	PSNR (dB)	NPCR (%)	UACI (%)
12	5.91	99.38	33.05
25	4.72	99.55	33.47
50	3.18	99.81	34.02



(a) (b) (c)

Figure 5. Loss data test: encrypted Lena and its corresponding decrypted image for lost: (a) 12%, (b) 25%, and (c) 50%

3.3. Noise addition

To quantitatively evaluate the robustness of the proposed encryption scheme against noise attacks, PSNR, NPCR, and UACI were computed for the decrypted images after noise injection. additive white Gaussian noise (AWGN) with variances of 0.005 and 0.01, as well as salt-and-pepper noise with densities of 5% and 10%, were applied to the encrypted images.

The results show that even low noise levels cause a severe degradation of the decrypted images, with PSNR values dropping below 5 dB in all tested cases. In addition, NPCR values remained above 99%, and UACI values exceeded 33%, indicating that noise perturbations propagate across the entire decrypted image. These quantitative results confirm that the proposed encryption scheme exhibits high sensitivity to noise, thereby preventing successful reconstruction under noise-based attacks. The corresponding quantitative results are summarized in Table 3.

Table 3. Quantitative results under noise attacks

Noise type	Level	PSNR (dB)	NPCR (%)	UACI (%)
AWGN	0.005	4.82	99.41	33.12
AWGN	0.01	3.97	99.56	33.48
Salt and pepper	5%	4.35	99.62	33.71
Salt and pepper	10%	3.21	99.78	34.05

3.4. Sensitivity test

A key feature of a secure chaotic encryption system is its extreme sensitivity to initial conditions and secret keys. We performed sensitivity tests to verify that tiny changes in the encryption key or parameters lead to drastic changes in the encryption and decryption outcome. The proposed scheme exhibits an excellent avalanche effect: as illustrated in detail through Figures 6(a) to (i), a minute alteration in the secret key (for example, a change in one of the logistic map initial seeds on the order of 10^{-14} results in a completely different encrypted image and a failure to correctly decrypt. In practical terms, if the decryption is attempted with a key that differs only slightly from the correct key, the output is an unintelligible image with no resemblance to the plain image. This superior sensitivity to decryption parameters was observed consistently any deviation in a FrFT order or a mask generation parameter yields a chaotic decryption result, confirming that an exact key match is required. Furthermore, we tested plaintext sensitivity by altering a single pixel in the original image and examining the change in the cipher. The NPCR in this case exceeded 99%, meaning almost every pixel in the encrypted image changed due to a one-pixel difference in the input. Likewise, the UACI was found to be around the ideal value of 33%, indicating significant intensity changes. Such high NPCR and UACI values imply that the encryption algorithm diffusely spreads the effect of even minor input changes across the entire image. This combination of key sensitivity and plaintext sensitivity ensures that the system can thwart differential attacksattackers cannot predict how small changes in key or plaintext affect the cipher, nor can they succeed with approximate keys.

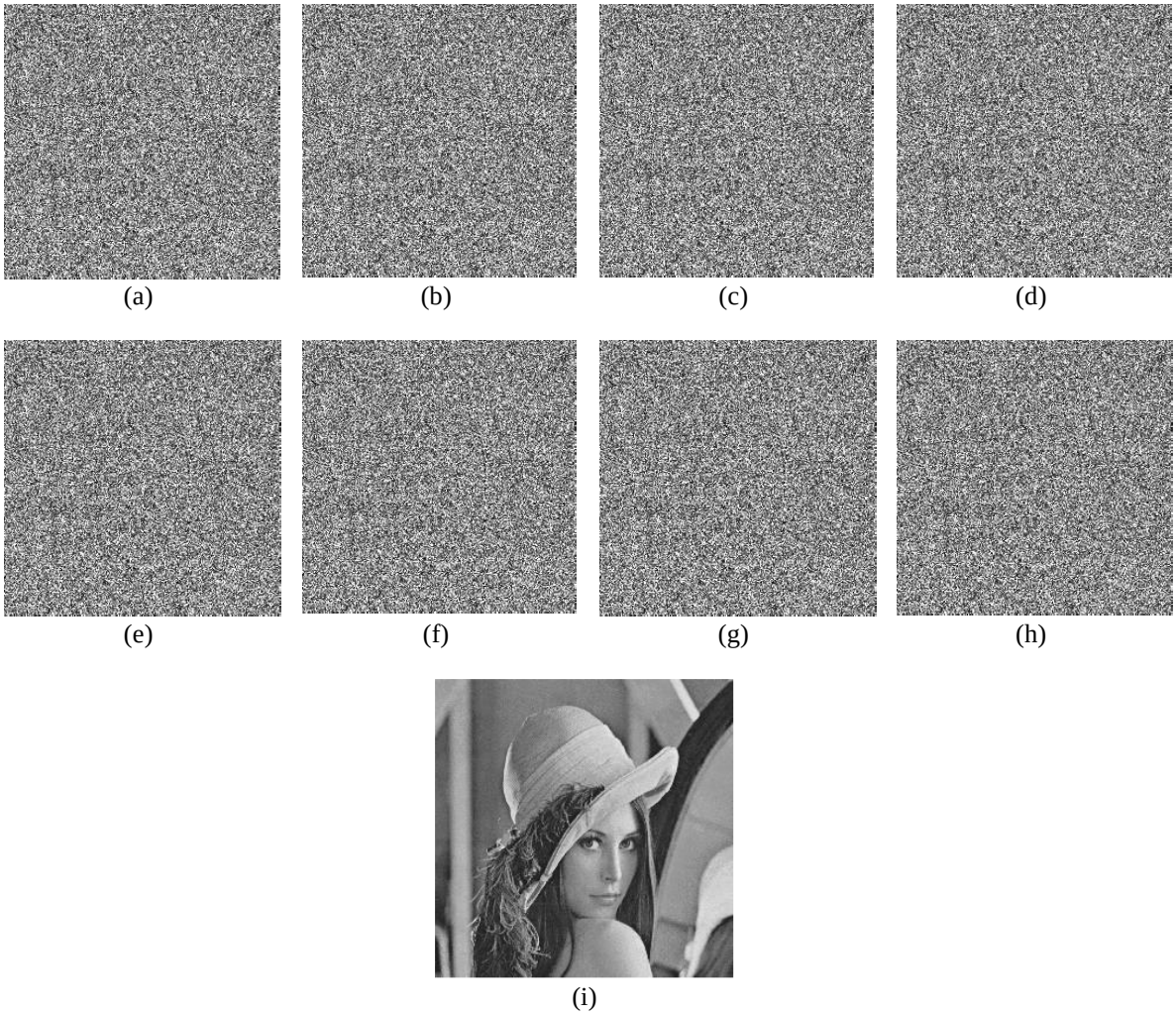


Figure 6. Sensitivity test: decrypted Lena with: (a) $x_0' = x_0 + 10^{-14}$, (b) $r_0' = r_0 + 10^{-14}$, (c) $x_1' = x_1 + 10^{-14}$, (d) $r_1' = r_1 + 10^{-14}$, (e) $x_2' = x_2 + 10^{-14}$, (f) $r_2' = r_2 + 10^{-14}$, (g) $x_3' = x_3 + 10^{-14}$, (h) $r_3' = r_3 + 10^{-14}$, and (i) correct key

3.5. Key space analysis

Finally, the key space of the proposed encryption scheme was analyzed to confirm its sufficiency against brute-force attacks. The algorithm introduces multiple secret parameters at different stages, resulting in a high-dimensional key vector. In the FrFT-based DRPE system with nonlinear preprocessing, secret keys include the fractional orders used in the FrFT, the two chaotic mask generation parameters (e.g., the initial seeds and control parameters x_2, r_2 and x_3, r_3 for the logistic maps producing masks $M_1(x_2, r_2)$ and $M_2(x_3, r_3)$, and the weighting factors w_1, w_2 in the nonlinear diffusion function. Each continuous parameter can be represented with a high precision; for example, if one considers a precision of 10^{-14} for chaotic map seeds, each such parameter has about 10^{+14} possible values. The combined key space, which is the product of all possibilities for each independent key parameter, is astronomically large. In aggregate, the key space size is well above 2^{128}, far exceeding the typical security requirement for resisting brute-force attacks. An adversary would therefore face an infeasible task when attempting exhaustive search: even if one could test billions of keys per second, the time required to search such a vast space would be prohibitively large (about 10^{30} years or more). This analysis confirms that the scheme's security is not limited by key space size. In comparison to many classical encryption systems, this method offers a significantly larger key domain, which strengthens its defense against brute force and dictionary attacks. Each encryption instance can use a unique set of keys drawn from this huge space, making the probability of guessing the correct key virtually zero.

In addition to its digital implementation, as shown in Figure 7, the proposed encryption scheme offers a compelling pathway toward opto-digital realization, particularly due to the inherent compatibility of DRPE and the FrFT with optical systems. By leveraging spatial light modulators (SLMs), diffractive optical elements (DOEs), and photodetectors, the nonlinear preprocessing and DRPE framework could be partially or fully implemented in the optical domain. This hybrid opto-digital architecture would significantly accelerate encryption and decryption processes through parallel light processing, while also reducing power consumption making it suitable for real-time applications in secure optical communications, biomedical imaging, and defense. Future work will investigate the feasibility of mapping the nonlinear preprocessing stage onto optical components, either through programmable optics or optoelectronic circuits, to enable compact and high-speed optical encryption systems.

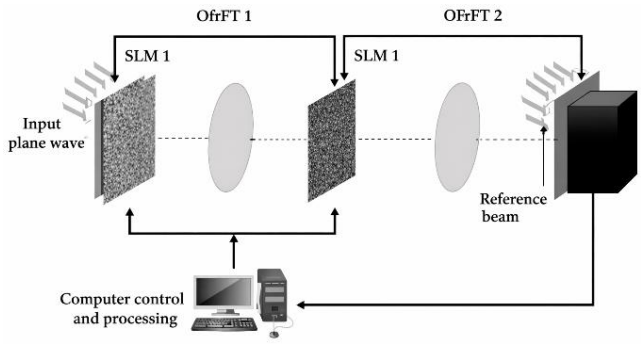


Figure 7. Opto-digital FrFT-DRPE implementation

3.6. Comparative analysis with state-of-the-art methods

To objectively assess the performance of our proposed nonlinear preprocessing scheme combined with FrFT-based DRPE, we present a comparative analysis with selected state-of-the-art image encryption techniques in Table 4. These methods include both chaos-based and transform-domain schemes that are widely cited in the literature. We use the following encryption performance metrics for comparison:

a. PSNR (dB): lower is better for encryption strength
b. Entropy (bits): closer to 8 indicates higher randomness
c. NPCR (%): higher values show better sensitivity to plaintext changes
d. UACI (%): reflects average intensity change; higher is better
e. Encryption time (s): efficiency of algorithm

According to Table 4 Our proposed scheme achieves:

a. Lower PSNR (indicating stronger encryption)
b. Higher NPCR and UACI (indicating better diffusion and confusion)
c. Comparable or better entropy
d. Competitive runtime with FrFT-based methods

Compared to other FrFT- or chaos-enhanced DRPE techniques, the Ntanh preprocessing significantly improves the sensitivity and robustness of the encryption system while preserving computational feasibility. These results support the suitability of our method for high-security applications such as biometric and medical image encryption.

Table 4. Quantitative results comparison

Method	PSNR (dB)	Entropy	NPCR	UACI	Time(s)
XOR + DRPE (baseline)	9.26	7.99	99.13	32.2	0.18
XOR + DRPE + FrFT [17]	8.45	7.96	99.23	32.5	0.29
DRPE + compressive + chaos [22]	8.71	7.98	99.31	33.1	0.34
Preprocessing + DRPE + MpFrFT [27]	9.22	7.89	99.44	33.36	0.33
Preprocessing + DRPE + FrFT [28]	8.92	7.82	99.52	33.39	0.26
Ntanh + DRPE (ours)	7.25	7.56	99.62	33.4	0.27

4. CONCLUSION

This paper presented a robust image encryption framework that integrates nonlinear preprocessing with a DRPE scheme operating in the FrFT domain. By replacing the conventional XOR-based diffusion with a tanh nonlinear diffusion mechanism, the proposed approach effectively addresses the intrinsic linearity weakness of classical spatial and DRPE-based encryption schemes. Beyond quantitative improvements in traditional security metrics such as PSNR, entropy, NPCR, and UACI, the proposed framework demonstrates a substantial enhancement in cryptographic robustness. The introduction of nonlinearity significantly strengthens key sensitivity, diffusion efficiency, and resistance to statistical, differential, and brute-force attacks. These properties are essential for modern encryption systems that must operate in adversarial environments where advanced cryptanalysis techniques are increasingly accessible. From a practical perspective, the combination of nonlinear preprocessing and FrFT-based DRPE offers a flexible and scalable solution suitable for high-security applications, including optical image encryption, biometric data protection, medical image confidentiality, and secure IoT-based imaging systems. The compatibility of the proposed method with opto-digital architectures further broadens its applicability, enabling potential deployment in high-speed and parallel optical encryption platforms.

Future work will focus on implementing the proposed framework in real-time and embedded environments, as well as exploring its integration into hybrid optical digital systems to further accelerate encryption and decryption processes. Additionally, extensive validation on large-scale and multimodal datasets, particularly in biometric and medical imaging contexts, will be conducted to assess scalability, robustness, and practical deployment feasibility.

ACKNOWLEDGMENTS

The authors would like to thank their home institutions for support.

FUNDING INFORMATION

This research received no external funding.

AUTHOR CONTRIBUTIONS STATEMENT

This journal uses the Contributor Roles Taxonomy (CRediT) to recognize individual author contributions, reduce authorship disputes, and facilitate collaboration.

Name of Author	C	M	So	Va	Fo	I	R	D	O	E	Vi	Su	P	Fu
Fayçal Radjah	✓	✓	✓		✓	✓		✓	✓	✓				
Nacira Diffellah	✓	✓		✓	✓	✓			✓	✓				
Lahcene Ziet	✓	✓			✓	✓	✓		✓	✓		✓		
Tewfik Bekkouche	✓	✓		✓	✓	✓			✓	✓		✓		

C : **C**onceptualization
M : **M**ethodology
So : **So**ftware
Va : **Va**lidation
Fo : **Fo**rmal analysis
I : **I**nvestigation
R : **R**esources
D : **D**ata Curation
O : Writing - **O**riginal Draft
E : Writing - Review & **E**diting
Vi : **Vi**sualization
Su : **Su**pervision
P : **P**roject administration
Fu : **Fu**nding acquisition

CONFLICT OF INTEREST STATEMENT

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

DATA AVAILABILITY

Data availability is not applicable to this paper as no new data were created or analyzed in this study.

REFERENCES

[1] Q. Zhang, L. Guo, and X. Wei, "Image encryption using DNA addition combining with chaotic maps," *Mathematical and Computer Modelling*, vol. 52, no. 11–12, pp. 2028–2035, Dec. 2010, doi: 10.1016/j.mcm.2010.06.005.

[2] P. Refregier and B. Javidi, "Optical image encryption based on input plane and Fourier plane random encoding," *Optics Letters*, vol. 20, no. 7, p. 767, Apr. 1995, doi: 10.1364/ol.20.000767.

[3] X. Tong and M. Cui, "Image encryption with compound chaotic sequence cipher shifting dynamically," *Image and Vision Computing*, vol. 26, no. 6, pp. 843–850, Jun. 2008, doi: 10.1016/j.imavis.2007.09.005.

[4] N. K. Pareek, V. Patidar, and K. K. Sud, "Image encryption using chaotic logistic map," *Image and Vision Computing*, vol. 24, no. 9, pp. 926–934, Sep. 2006, doi: 10.1016/j.imavis.2006.02.021.

[5] G. Zhou, D. Zhang, Y. Liu, Y. Yuan, and Q. Liu, "A novel image encryption algorithm based on chaos and Line map," *Neurocomputing*, vol. 169, pp. 150–157, Dec. 2015, doi: 10.1016/j.neucom.2014.11.095.

[6] J. Liang, D. Xiao, Y. Xiang, and R. Doss, "A Compressed Sensing Based Image Compression-Encryption Coding Scheme without Auxiliary Information Transmission," *ICC 2022 - IEEE International Conference on Communications. IEEE*, pp. 5573–5578, May 16, 2022. doi: 10.1109/icc45855.2022.9839131.

[7] S. Behnia, A. Akhshani, H. Mahmodi, and A. Akhavan, "A novel algorithm for image encryption based on mixture of chaotic maps," *Chaos, Solitons & Fractals*, vol. 35, no. 2, pp. 408–419, Jan. 2008, doi: 10.1016/j.chaos.2006.05.011.

[8] N. Zhou, Y. Wang, and L. Gong, "Image encryption algorithm based on fractional Fourier transform and chaos," *Optics Communications*, vol. 285, no. 11, pp. 3024–3029, 2012, doi: 10.1016/j.optcom.2012.01.065.

[9] X. Shi and D. Zhao, "Color image hiding based on the phase retrieval technique and Arnold transform," *Applied Optics*, vol. 50, no. 14, p. 2134, May 2011, doi: 10.1364/ao.50.002134.

[10] X. Wang, L. Teng, and X. Qin, "A novel colour image encryption algorithm based on chaos," *Signal Processing*, vol. 92, no. 4, pp. 1101–1108, Apr. 2012, doi: 10.1016/j.sigpro.2011.10.023.

[11] G. Alvarez and S. Li, "Some basic cryptographic requirements for chaos-based cryptosystems," *International Journal of Bifurcation and Chaos*, vol. 16, no. 08, pp. 2129–2151, Aug. 2006, doi: 10.1142/S0218127406015970.

[12] Y. Frauel, A. Castro, T. J. Naughton, and B. Javidi, "Resistance of the double random phase encryption against various attacks," *Optics Express*, vol. 15, no. 16, p. 10253, 2007, doi: 10.1364/oe.15.010253.

[13] X. Chai, Z. Gan, K. Yuan, Y. Chen, and X. Liu, "A novel image encryption scheme based on DNA sequence operations and chaotic systems," Advances in Optics and Photonics, vol. 31, no. 1, pp. 219–237, Apr. 2017, doi: 10.1007/s00521-017-2993-9.

[14] A. Alfalou and C. Brosseau, "Optical image compression and encryption methods," *Advances in Optics and Photonics*, vol. 1, no. 3, p. 589, Oct. 2009, doi: 10.1364/aop.1.000589.

[15] B. Javidi and T. Nomura, "Securing information by use of digital holography," *Optics Letters*, vol. 25, no. 1, p. 28, Jan. 2000, doi: 10.1364/ol.25.000028.

[16] N. Singh and A. Sinha, "Optical image encryption using fractional Fourier transform and chaos," *Optics and Lasers in Engineering*, vol. 46, no. 2, pp. 117–123, Feb. 2008, doi: 10.1016/j.optlaseng.2007.09.001.

[17] X. Wang, L. Liu, and Y. Zhang, "A novel chaotic block image encryption algorithm based on dynamic random growth technique," *Optics and Lasers in Engineering*, vol. 66, pp. 10–18, Mar. 2015, doi: 10.1016/j.optlaseng.2014.08.005.

[18] H. Liu and X. Wang, "Color image encryption based on one-time keys and robust chaotic maps," *Computers & Mathematics with Applications*, vol. 59, no. 10, pp. 3320–3327, May 2010, doi: 10.1016/j.camwa.2010.03.017.

[19] H. Zhu, C. Zhao, and X. Zhang, "A novel image encryption–compression scheme using hyper-chaos and Chinese remainder theorem," *Signal Processing: Image Communication*, vol. 28, no. 6, pp. 670–680, Jul. 2013, doi: 10.1016/j.image.2013.02.004.

[20] Y. Zhou, L. Bao, and C. L. P. Chen, "Image encryption using a new parametric switching chaotic system," *Signal Processing*, vol. 93, no. 11, pp. 3039–3052, Nov. 2013, doi: 10.1016/j.sigpro.2013.04.021.

[21] Y. Wu, "Image encryption using the two-dimensional logistic chaotic map," *Journal of Electronic Imaging*, vol. 21, no. 1, p. 013014, Mar. 2012, doi: 10.1117/1.jei.21.1.013014.

[22] H. L. Ndassi, R. Kengne, A. G. G. Tegue, M. T. Motchongom, R. Tchitnga, and M. Tchoffo, "A robust image encryption scheme based on compressed sensing and novel 7D oscillato with complex dynamics.," *Heliyon*, vol. 9, no. 6, p. e16514, Jun. 2023, doi: 10.1016/j.heliyon.2023.e16514.

[23] G. Kaur, R. Agarwal, and V. Patidar, "Color image encryption scheme based on fractional Hartley transform and chaotic substitution–permutation," *The Visual Computer*, vol. 38, no. 3, pp. 1027–1050, Jan. 2021, doi: 10.1007/s00371-021-02066-w.

[24] Y. Zhou, L. Bao, and C. L. P. Chen, "A new 1D chaotic system for image encryption," *Signal Processing*, vol. 97, pp. 172–182, Apr. 2014, doi: 10.1016/j.sigpro.2013.10.034.

[25] G. Unnikrishnan, J. Joseph, and K. Singh, "Optical encryption by double-random phase encoding in the fractional Fourier domain," *Optics Letters*, vol. 25, no. 12, p. 887, Jun. 2000, doi: 10.1364/ol.25.000887.

[26] C. Guo, S. Liu, and J. T. Sheridan, "Iterative phase retrieval algorithms Part II: Attacking optical encryption systems," *Applied Optics*, vol. 54, no. 15, p. 4709, May 2015, doi: 10.1364/ao.54.004709.

[27] S. E. Azoug and S. Bouguezel, "A non-linear preprocessing for opto-digital image encryption using multiple-parameter discrete fractional Fourier transform," *Optics Communications*, vol. 359, pp. 85–94, Jan. 2016, doi: 10.1016/j.optcom.2015.09.054.

[28] T. Bekkouche and S. Bouguezel, "A recursive non-linear pre-encryption for opto-digital double random phase encoding," *Optik*, vol. 158, pp. 940–950, Apr. 2018, doi: 10.1016/j.ijleo.2017.12.142.

[29] T. Bekkouche, N. Diffellah, and L. Ziet, "Hybrid image encryption based on digital pre-encryption and optical single random phase encoding," *Optica Applicata*, vol. 49, no. 4, 2019, doi: 10.37190/oa190403.

BIOGRAPHIES OF AUTHORS

Fayçal Radjah is a researcher at the Faculty of Technology, University of Ferhat Abbas, Setif. He obtained his Engineering degree in 1989 and a Master Degree in 1993. He is actually a member of the Power Electronics and Industrial Control research laboratory since 2012. In 2022, he obtained his Ph.D. Degree. Currently, he works on the development of signal processing algorithms and implementing them on FPGA. He can be contacted at email: radjah.faycal@yahoo.fr.

Nacira Diffellah is a researcher and lecturer at the Institute of Electronics and Telecommunications, Mohamed El Bachir El Ibrahimi University of Bordj Bou Arreridj, Algeria. She obtained her engineering degree after working on the analysis and synthesis of digital filters. She then completed a Magister degree focused on the modeling and fuzzy logic control of biotechnological systems, before pursuing a Ph.D. dedicated to image denoising using proximal methods. Her research interests mainly revolve around signal processing and image processing, and she also supervises master's students in these areas. She can be contacted at email: nacira.diffellah@univ-bba.dz.

Tewfik Bekkouche received the Engineering and Ph.D. degrees in Electronics in 1990 and 2018, respectively. He is currently a Professor at the University of Bordj Bou Arreridj, Algeria. With a solid academic background and extensive expertise in the field, he is committed to developing secure and innovative solutions in information technology. His research interests include image encryption, biometrics, and information security. He can be contacted at email: toufik.bekkouche@univ-bba.dz.

Lahcene Ziet is an Assistant Professor at the Department of Electronics at the University of Ferhat Abbas, Setif. In 1990, he obtained his Engineering degree in Electronic Engineering followed by a Master degree in Electronics in 1994 from the previous university. He taught at the same university until 2004. In 2007, he obtained his Ph.D. in Information Security and Signature Analysis. Currently, his research focuses on topics related to security. He can be contacted at email: lahcene.ziet@univ-setif.dz.