Optica Applicata, Vol. LV, No. 3, 2025
DOI: 10.37190/oa/207947

Optical image encryption in the Fresnel domain using the umbrella map and the Yang–Gu algorithm

ARABIND KUMAR[1,*], SANJAY YADAV[2,*]

[1] Department of Applied Sciences, The Northcap University Gurugram, India

[2] Alliance School of Applied Mathematics, Alliance University Bangalore, India

[*]Corresponding authors: arabind20asd003@ncuindia.edu (AK), sanjay.yadav@alliance.edu.in (SY)

We present a novel image encryption approach utilizing a unique combination of Yang–Gu mixing amplitude-phase retrieval and a nonlinear discrete chaotic umbrella map in the Fresnel domain. Our suggested method involves the algorithm of a deterministic phase mask prior to applying the Fresnel transform to the input image. To address the limitations and vulnerabilities of single chaotic map systems, we employ umbrella maps to scramble the modified image's pixels. This not only expands the range of available controls but also improves the key size. We first encode the scrambled picture, then apply a Fresnel transform, followed by a second application of the phase mask. The resulting image's phase-truncated component undergoes Yang–Gu mixture amplitude-phase retrieval algorithm in the Fresnel domain. The encryption process employs one-way binary modulation, ensuring easier storage and transmission of the image. Extensive statistical and attack analyses have been performed to evaluate the strength of proposed technique. Moreover, the sensitivity analysis of the scheme has been thoroughly investigated, confirming its effectiveness and reliability of encryption scheme.

Keyword: cryptography, image encryption, umbrella map, Fresnel transform, Yang–Gu algorithm.

1. Introduction

Multimedia information may now be conveniently saved and sent via the internet because to the widespread availability of digital technology and communication networks. This study is very sensitive, making data security a top priority. The effectiveness, security, and privacy of conventional digital cryptosystems have been the subject of extensive investigation. Many approaches have been offered over the last several decades to fulfil the demanding needs of image encryption [1-6]. A random phase mask (RPM) is used in both the input domain and the Fourier transform domain in the well-known technique of double random phase encoding (DRPE) [7]. DRPE-based optical encryption techniques, such as the Fourier transform [8,9], the discrete sine and cosine transform [9,10], the fractional Fourier transform [11], the gyrator transform [12,13], the fractional Hartley transform [14,15], the gyrator wavelet transform [16], and others,

have been implemented in a variety of settings [17-23]. Scrambling, which may be done using chaotic systems, is one of the finest methods for incorporating the encrypted image derived from the input image. Several properties of chaos, such as pseudo-randomness, ergodicity, and exponential sensitivity to beginning conditions, may be useful in cryptographic systems. As a result, a wide range of chaotic schemes have been constructed [24-39], including DNA-chaotic system hybrids [31,32], and 3D Lorentz chaotic systems [28-30]. A system's attributes and early conditions are critical in determining its chaotic nature and chaotic course. They improve the safety and dependability of encryption methods by prolonging the size of the key space in cryptographic systems.

Researchers have dedicated plethora of time and efforts on enhancing the efficiency of cipher schemes, and optical information encryption technology has been at the forefront of this because of the benefits of concurrent and fast processing capacity and the high efficiency of phase components. Refregier and Javidi's [22] double random phase encoding (DRPE) approach is one of the earliest and most extensively studied image-encrypting optical algorithms. This scheme encrypts the image amplitude using a 4-f imaging system and two independent random phase keys (RPKs). One is in the Fourier plane, the other is in the input plane. After more than 20 years of study and development, a wide range of optical information encryption techniques is now available. The optical signals may be encoded in a variety of ways, including amplitude, phase, wavelength, and polarization. Researchers' continued curiosity in optical security and encoding techniques have been seen in the abundance of recent publications [6-8]. The encryption technique's key space has been intended to be increased from the fractional Fourier transform (FrFT) domain to the Fresnel domain, the Hartley transform domain, and the wavelet domain. All the above techniques are based on the traditional DRPE configuration. The linear canonical integral gyrator transform (GT) depicts rotations in phase space's deformed position-spatial frequency planes. This technology is easily adaptable to a range of other optoelectronic systems and is simple to apply. This requirement has resulted in the development of several enhanced approaches for working with colour photographs, watermarking multiple images, and so on. Instead of a white-noised RPK, a structured phase key (SPK) could be utilized for encrypting data and decrypting it. There are quite a few different types of SPK, including toroidal zone masks, linear phase masks, spiral phase masks, and fractal zone masks. These SPKs have all been shown to be extremely flexible, safe, and user-friendly.

Earlier methods relied on traditional chaotic maps only jumble the pixels, resulting in valuability of data. Using the Fresnel domain, the umbrella map, and the Yang–Gu mixing algorithm, we propose a novel approach for image encryption. Scrambling the pixels using an umbrella map [40] and then using the Yang–Gu mixing method to make the scheme nonlinear and expand the space of the key and enhances the strength of the method while also generating an output with a real value that is easy to store and transfer. Here, we use the Fresnel domain to facilitate the development of higher-order structures. Results from statistical analysis, significant sensitivity analysis, and attack analysis are presented in Section 3 as part of the scheme validation process. Section 4

compares the proposed mechanism to recent scheme to understand its importance. Section 5 concludes the study.

2. Overview

2.1. Fresnel transform

The Fresnel transform is defined as an operation performed on the input image $I(x, y)$.

$$F(u, v) = \mathrm{FrT}_{\lambda, z}\{I(x, y)\} = \int_{-\infty}^{\infty}\int_{-\infty}^{\infty} I(x, y)\, h_{\lambda, z}(u, v, x, y)\, \mathrm{d}x\, \mathrm{d}y \tag{1}$$

In this case, the wave's wavelength and its propagation distance are represented by the Fresnel transform parameters z and λ and $h_{\lambda, z}(u, v, x, y)$ the kernel, which is represented by the following equation:

$$h_{\lambda, z}(u, v, x, y) = \frac{1}{\sqrt{i\lambda z}} \exp\left(i\frac{2\pi}{\lambda}\right) \exp\left[\frac{i\pi}{\lambda z}(u - x)^2 + (v - y)^2\right] \tag{2}$$

2.2. Yang–Gu mixture amplitude phase retrieval algorithm

In 2015, the idea of repeatedly recovering amplitudes and phases in the Fourier transform was proposed by Sui *et al*. [41], to strengthen the security of cryptosystems. The Yang–Gu mixed amplitude-phase retrieval technique in the discrete wavelet transform uses the input $r(x, y)$ and the public key (u, v). With this strategy, the hidden function $e_{k+1}(u, v)$ and phase function $\varphi(x, y)$ use criteria of convergence in their calculations.

At the beginning of each loop, a function is built. $e_1(u, v)$ when a random number between two values $[0, 1]$ is used. On the k-th iteration, $e_k(u, v)$ include with $R(u, v)$ as well as provide the result of an inverse Fresnel transform $F_k(x, y)$ as depicted in the below equation:

$$F_k(x, y) = \mathrm{IFrT}\{e_{k+1}(u, v)R(u, v)\} \tag{3}$$

where the inverse Fresnel transform's operators is denoted by IFrT. Let us examine the time amplitude by expression (3) be $h_k(x, y) = |F_k(x, y)|$ and phase part be $\varphi_k(x, y) = \arg F_k(x, y)$. Figure 1 showing the procedure of Yang–Gu mixture amplitude phase retrieval algorithm.

Next iteration's $e_k(u, v)$ may be determined by the following correlations:

$$E_k(u, v) = \mathrm{FrT}\{r(x, y)\exp[\varphi_k(x, y)]\} \tag{4}$$

$$e_k(u, v) = \mathrm{Re}\left|E_k(u, v)R^*(u, v)\right| \tag{5}$$

where $*$ denotes the conjugate operator, Re represents the real part operator and FrT denotes the Fresnel transformation operator.

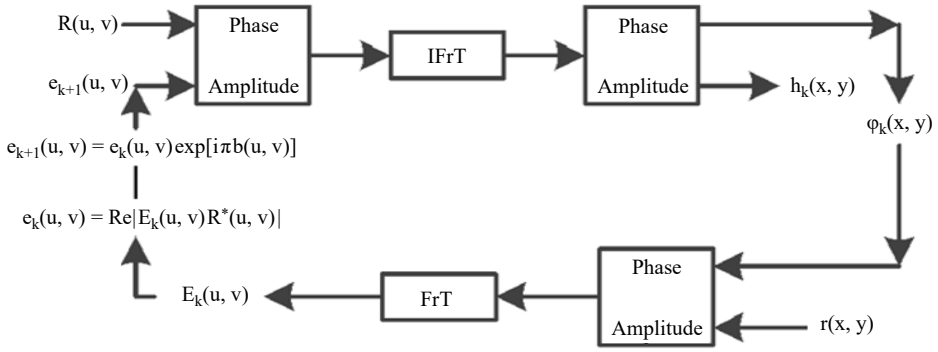

Fig. 1. Flowchart for Yang–Gu mixture amplitude phase retrieval algorithm.

Once controls are in place, the iteration process stops. When the normalized mean squared error (NMSE) hits a certain threshold, the loop is terminated. The NMSE between the original and iterated picture may be determined by the given equation:

$$\mathrm{NMSE} = \frac{\sum_{xy}\left[r(x, y) - h_k(x, y)\right]^2}{\sum_{xy} r^2(x, y)} \tag{6}$$

A one-way binary phase modulation is used since the encrypted images contain both positive and negative elements. Application of the binomial phase modulation function results in $\exp(u, v)$, where each negative number has been changed into a positive number. Equation is used to get the value of b. The value of b is calculated using the following equation:

$$b(u, v) = \begin{cases} 1, & e_k < 0 \\ 0, & e_k > 0 \end{cases} \tag{7}$$

In this situation, $b(u, v)$ serves as a kind of secret key.

$$e_{k+1}(u, v) = e_k(u, v)\exp\left[i\pi b(u, v)\right] \tag{8}$$

The decoding key $D(u, v)$ is calculated using multiplying the binary phase modulation by the public random phase key $R(u, v)$ and $\exp[i\pi b(u, v)]$

$$D(u, v) = R(u, v)\exp\left[i\pi b(u, v)\right] \tag{9}$$

2.3. Deterministic phase mask

As part of their proposed encryption systems, scientists have investigated DRPE. There is plenty of bandwidth provided here for verified users to freely swap masks with one

another. To avoid this issue, a computational phase mask may be utilized in place of a randomly generated one. The low length of the shared key is an attractive feature since it requires less bandwidth and is easier to manage. In this study, chaotic maps are used to create deterministic phase masks. This method generates stochastic phase masks from both a cubic map and a chaotic logistic map. A nonlinear chaotic map in one dimension is as shown by the subsequent equation.

$$f(x) = t_1 x(1 - x) \tag{10}$$

and t_1, the bifurcation parameter, may be assumed to be $0 < t_1 < 4$. The following is the definition of the logistic map in its recursive form:

$$x_{n+1} = t_1 x_n(1 - x_n) \tag{11}$$

When n iterations are performed, the best estimate moves from x_0 to x_n, and $x_n \in [0, 1]$.

Once the bifurcation constraint is in the range [3.5699456, 4], shown in the following equation, chaotic behavior will occur. Let X_1 be a one-dimensional sequence generated by the nonlinear chaotic equation, with $M \times N$ elements, where N columns may be built by inserting components in the sequence in any order.

$$X_1 = \{x_1, x_2, x_3, ..., x_{M \times N}\} \tag{12}$$

Here $x_i \in [0, 1]$. If we take the sequence X_1 and arrange its M elements in a column, we may create the 2-dimensional matrix Y_1:

$$Y_1 = \{Y_{i,j} | i = 1, 2, ..., M;\ j = 1, 2, ..., N\} \tag{13}$$

Using this given equation (14), we can compute the deterministic phase mask:

$$\mathrm{DPM1}(x, y) = \exp\left[i 2\pi y_{i,j}(x, y)\right] \tag{14}$$

Wherein coded messages are sent using x_0 and t_1. A chaotic cubic map may similarly be used to produce the second DPM2. The cubic map's equation is as follows:

$$x_{n+1} = t_2 x_n(1 - x_n^2) \tag{15}$$

where the bifurcation parameter t_2 has a value within the interval $0 \le t_2 \le 4$.

2.4. Umbrella map

The sequence generated by various chaos functions may be modified to produce the desired attributes of pseudo-randomness, non-correlation, and ergodicity due to the chaotic system's sensitivity to initial conditions. As a result of its better chaotic behavior and characteristics, the chaotic system is well-suited for usage in image encryption methods. Every change to the chaotic system's initial circumstances will produce a fresh random value sequence that bears the characteristics of non-periodicity and non-convergence.

This study used a 2-dimensional chaotic umbrella map created by modifying the Tinkerbell map as its foundation. In 2020, SACHIN *et al*. [43] used the sine function in Tinkerbell's map to develop an umbrella map, which they discovered preserved the umbrella shapes of all the chaotic activity and the bifurcation diagrams that mimic them. The suggested map's fixed-point predictability was also investigated. We will now discuss the umbrella map, which we get by solving iterative equations:

$$x_{n+1} = \sin(x_n^2) - y_n^2 + a\sin(x_n) + by_n \tag{16}$$

$$y_{n+1} = \sin(2x_n)y_n + c\sin(x_n) + dy_n \tag{17}$$

The number of iterations and the map parameters are represented by n, a, b, c and d, respectively. The initial umbrella map key parameters are $a = 0.874$, $b \in (-0.6013, 0.5142)$, $c = 2$, and $d = 0.5$. The numerical simulation begins with the values 0.1787 and 0.178 for the initial parameters x_0 and y_0, respectively.

2.5. Proposed encryption algorithm

We used an umbrella map to boost DRPE's robustness and to randomly jumble its pixels. The decryption and encryption procedures for the suggested system are shown technically in Figs. 2 and 3, respectively.

An in-depth explanation of the intended cipher system is as follows.

2.5.1. Encryption process

Following is a technique for creating encrypted images $I_e(x)$ from the input image $I(x)$.

Step 1: The input image $I(x)$ is masked after being subjected to a first deterministic phase mask DPM1.

$$I_m(x) = I(x) \times \text{DPM1} \tag{18}$$

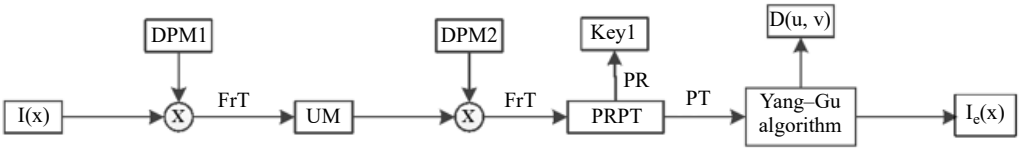

Fig. 2. The schematic diagram of the encryption process.

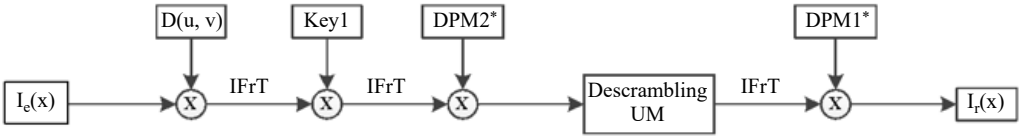

Fig. 3. The schematic diagram of the decryption process.

Step 2: The Fresnel transform (FrT) of $I_{\mathrm{m}}(x)$ is obtained.

$$I_{\mathrm{sc}}(x) = UM\{\mathrm{FrT}[I_m(x)]\} \tag{19}$$

Step 3: When used with another deterministic phase mask, DPM2 $I_{\mathrm{sc}}(x)$

$$I_{\mathrm{scm}}(x) = I_{\mathrm{sc}}(x) \times \mathrm{DPM2} \tag{20}$$

Step 4: Another use of the Fresnel transform (FrT) operation; in this case, the phase reserve (PR) operation is used to establish a private key (Key1), and the phase truncated (PT) component is used for further processing.

$$I_{\mathrm{trans\_scm}}(x) = \mathrm{FrT}[I_{\mathrm{scm}}(x)] \tag{21}$$

$$\mathrm{Key1} = \mathrm{PR}[I_{\mathrm{trans\_scm}}(x)] \tag{22}$$

$$I_{\mathrm{mag}}(x) = \mathrm{PT}[I_{\mathrm{trans\_scm}}(x)] \tag{23}$$

Step 5: To cipher a picture, we use the real-valued Yang–Gu (YG) mixing approach detailed in Section 2.2.

$$I_{\mathrm{e}}(x) = \mathrm{YG}[I_{\mathrm{mag}}(x)] \tag{24}$$

2.5.2. Decryption process

The steps for decryption procedure.

Step 1: $I_{\mathrm{e}}(x)$ image is combined with $D(u, v)$ to get $I_{\mathrm{ret}}(x)$

$$I_{\mathrm{ret}}(x) = I_{\mathrm{e}}(x) \times D(u, v) \tag{25}$$

Step 2: Try it in the reverse direction inverse Fresnel transform (IFrT) of $I_{\mathrm{ret}}(x)$ Fresnel function ($I_{\mathrm{ret}}(x)$)

$$I_{\mathrm{inter}}(x) = \mathrm{IFrT}[I_{\mathrm{ret}}(x)] \tag{26}$$

Step 3: Key1 is a private key that may be used to $I_{\mathrm{rec\_trans\_scm}}(x)$

$$I_{\mathrm{rec\_trans\_scm}}(x) = I_{\mathrm{inter}}(x) \times \exp(i\mathrm{Key1}) \tag{27}$$

Step 4: Take inverse Fresnel transform IFrT of $I_{\mathrm{rec\_trans\_scm}}(x)$ to get $I_{\mathrm{rec\_sm}}(x)$

$$I_{\mathrm{rec\_sm}}(x) = \mathrm{IFrT}[I_{\mathrm{rec\_trans\_scm}}(x)] \tag{28}$$

Step 5: Use DPM2* the conjugate of DPM to decode the received information.

$$I_{\mathrm{rec\_sc}}(x) = I_{\mathrm{rec\_sm}}(x) \times \mathrm{DPM2}^* \tag{29}$$

Step 6: Descramble $I_{\text{rec\_sc}}(x)$ applying umbrella map and using IFrT to obtain

$$I_{\text{rec\_m}}(x) = \text{IFrT}\{\text{UM}[I_{\text{rec\_sc}}(x)]\} \tag{30}$$

Step 7: Applying DPM1 conjugate that is DPM1* to $I_{\text{rec\_m}}(x)$ to obtain decrypted image.

$$I_{\text{r}}(x) = I_{\text{rec\_m}}(x) \times \text{DPM1}^* \tag{31}$$

The proposed encryption method uses double deterministic phase masks, an auxiliary key, and a private key (Key1). Binary phase modulation $b(u, v)$ and a random phase key $R(u, v)$ are brought together in $D(u, v)$. Fresnel parameters are crucial because they expand the range of valid pivot points in the scheme. The parameters a, b, c and d, as well as the initial seed values, are all retained in the umbrella map. DPM2, Key1, α_1, α_2, and x_0 and y_0 correspond to the public keys $D(u, v)$ and DPM1, and the digits a, b, c, and d that they share. This is why the technique employs the usage of both private and public keys.

The suggested approach is adaptable to both digital and optical implementations, as seen in the bottom of Fig. 4, which depicts a hybrid configuration that may be utilized to integrate both the digital and optical elements of the decryption process. The optical system and the computer use charged-coupled devices (CCDs) and spatial light modulators (SLM) for data transfer. Each decryption key has its own unique SLM that must be protected at all costs. $D(u, v)$, Key1, DPM1* and DPM2*. The computer helps the descrambling process that makes usage of the umbrella map go more smoothly. Finally, the CCD is utilized to save the decoded image to the computer.

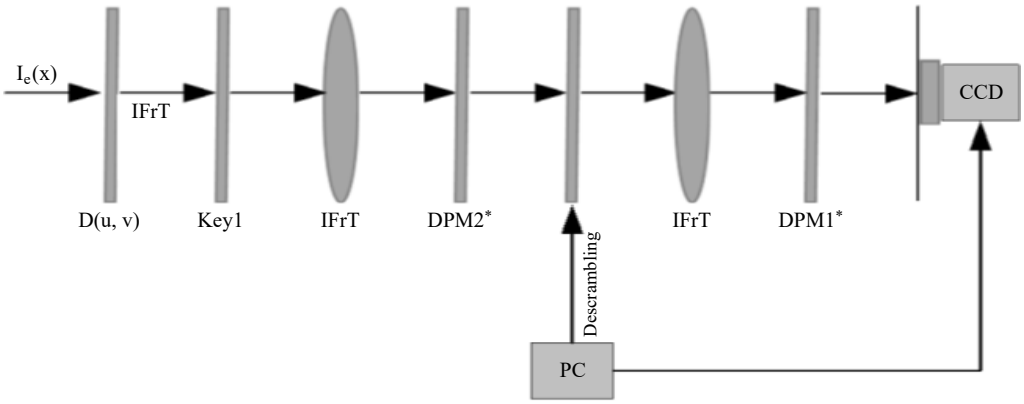

Fig. 4. Optical setup of the proposed mechanism.

3. Results and analysis

Numerical simulation is employed in this part to verify and confirm the study's conclusions. There are grayscale pictures of *Barbara* and *Peppers*, as well as a 256-by-256 bi-

nary image. Using logistic and cubic maps with initial values and control parameters, $x_0 = 0.4$ and, $x_0 = 0.564$, respectively, and $t_1 = 3.99995$ and $t_2 = 3$, respectively, deterministic phase masks are produced. The NMSE threshold is 0.0001 for a high-quality image when utilizing the Yang–Gu strategy's. The umbrella map's parameters a, b, c and d are 0.874, 0.4532, 2, and 0.5. The initial values of x_0 and y_0 are given as 5.1787, and 0.178, respectively.

Figure 5 demonstrates the strategy's verification. Figures 5(a)–(c) shows the *Peppers* and *Barbara* input images as well as a binary picture. Figures 5(d)–(e) and Figs. 5(g)–(i) depict two different private keys, Key1 and $D(u, v)$, respectively. The encrypted images that were obtained are shown in Figs. 5(j)–(i). Figure 5(m)–(o) depicts, nevertheless, the corresponding decoded images. Decoded pictures of *Peppers* and

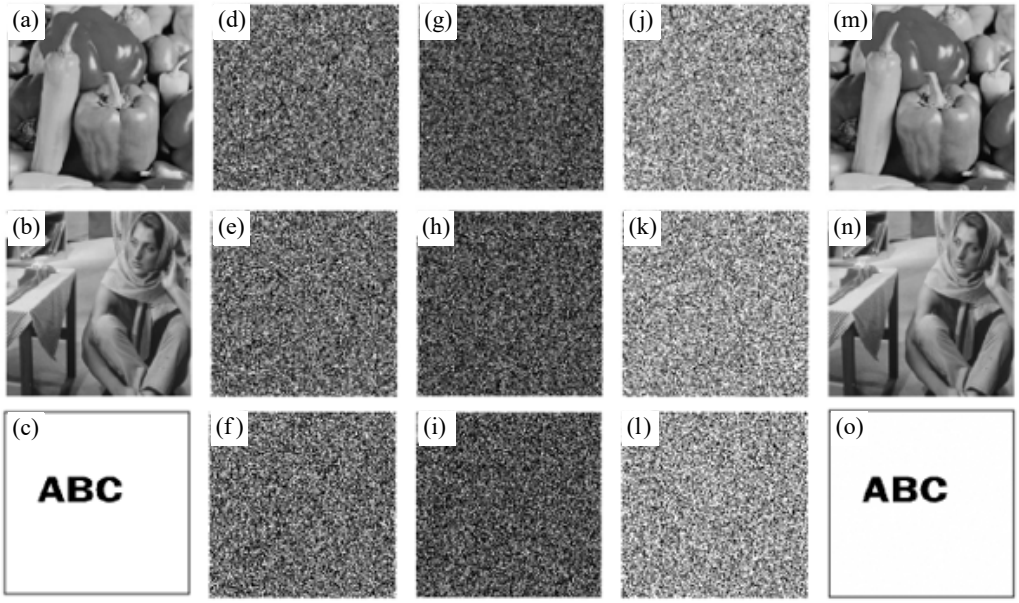

Fig. 5. Scheme validation results. (a)–(c) The input images of *Peppers*, *Barbara* and binary image; (d)–(e) and (g)–(i) the private Key1 and another key $D(u, v)$ for each image taken individually; (j)–(l) their corresponding ciper images obtained; (m)–(o) the corresponding decrypted images.

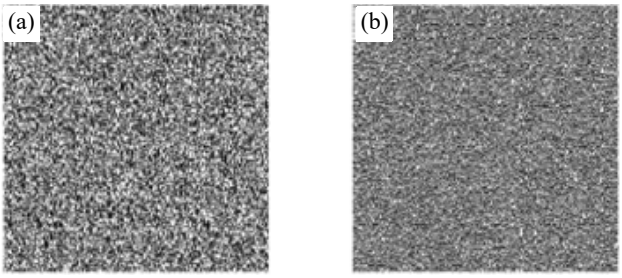

Fig. 6. Deterministic masks (a) DPM1 and (b) DPM2.

T a b l e 1. Evaluation results of MSE and PSNR.

Algorithm	Parameters		
	Input image	MSE	PSNR [dB]
DRPE [7]	Gray image	4.13×10^{-23}	291.9
	Binary image	2.83×10^{-23}	304.1
JIAO *et al*. [14]	Gray image	4.13×10^{-27}	292.8
	Binary image	7.33×10^{-27}	301.2
PENG *et al*. [19]	Gray image	7.04×10^{-16}	178.4
	Binary image	3.59×10^{-16}	190.25
Proposed cryptosystem	Gray image	8.58×10^{-25}	240.18
	Binary image	7.29×10^{-25}	241.30

Barbara as well as a binary image are shown in Table 1 along with their matching MSE and PSNR values. These numbers indicate the potential success of the suggested method. Figure 6 (a) and (b) displays two deterministic masks DPM1 and DPM2.

The effectiveness of the proposed approach has been shown by extensive statistical analysis, attack analyses, and crucial sensitivity assessments.

3.1. Statistical analysis

The system's validity and reliability have been verified using histogram and 3D plot analysis, correlation distribution testing, and entropy data display. The correlation coefficient (CC), mean squared error (MSE), and peak signal-to-noise ratio (PSNR) are obtained by

$$\mathrm{CC} = \frac{\sum_{i=1}^{H_1}\sum_{j=1}^{W_1}\left|\left[I(i,j)-\overline{I(i,j)}\right]\left[I_{\mathrm{r}}(i,j)-\overline{I_{\mathrm{r}}(i,j)}\right]\right|}{\sqrt{\sum_{i=1}^{H_1}\sum_{j=1}^{W_1}\left[I(i,j)-\overline{I(i,j)}\right]^2}\sqrt{\sum_{i=1}^{H_1}\sum_{j=1}^{W_1}\left[I_{\mathrm{r}}(i,j)-\overline{I_{\mathrm{r}}(i,j)}\right]^2}} \tag{32}$$

In this context, images of size $H_1 \times W_1$ are expressed by $I(i,j)$ and $I_{\mathrm{r}}(i,j)$ individually. The calculation of average is done by given equation:

$$\overline{I(i,j)} = \frac{1}{H_1 \times W_1}\sum_{i=1}^{M}\sum_{n=1}^{N} I(i,j) \tag{33}$$

The median extracted image $I_{\mathrm{r}}(i,j)$ may be obtained in a similar fashion. The following formula may be used to get the mean squared error (MSE):

$$\mathrm{MSE}(I(i,j), I_{\mathrm{r}}(i,j)) = \frac{1}{H_1 \times W_1}\sum_{i=1}^{H}\sum_{n=1}^{W}\left[I(i,j)-I_{\mathrm{r}}(i,j)\right]^2 \tag{34}$$

Margin of error mean squared relating the source image $r(x, y)$ and the iterated image, the NMSE (normalized mean squared error) is calculated

$$\mathrm{NMSE} = \frac{\sum_{x,y}\left[r(x,y) - h_{\mathrm{k}}(x,y)\right]^2}{\sum_{x,y} r^2(x,y)} \tag{35}$$

The peak signal-to-noise ratio (PSNR) can be determined as

$$\mathrm{PSNR} = 10\log\left|\frac{255^2}{\mathrm{MSE}}\right| \tag{36}$$

3.1.1. Histogram analysis

The dissemination of the grayscale quantities in a photograph is depicted by a histogram, which is a bar graph. It demonstrates how many pixels are needed to produce a specific shade of grey. A key component of any effective picture encryption method is that the original and encrypted image's histogram must deviate significantly. This illustrates how much randomness or uncertainty the encryption technique introduced into the image. Figure 7 shows the suggested method's histogram graphs using the *Barbara* input image. Figure 7 displays histograms for image input, encryption, and decryption. The figure indicates that although the encrypted image's histogram plot is practically flat, appearing like white stationary noise, the decrypted image's histogram plot is comparable to the input image. The robustness and longevity of the proposed mechanism are so clearly shown.

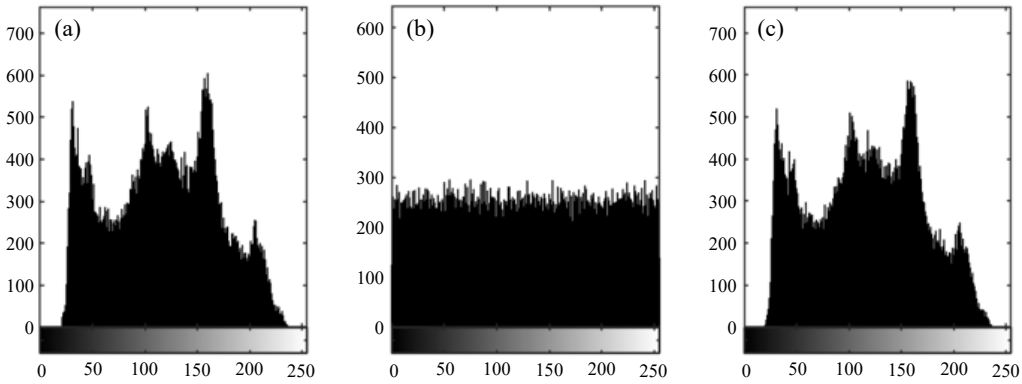

Fig. 7. The histogram plot for (a) the input image of *Barbara*, (b) encrypted image, and (c) decrypted image.

3.1.2. 3D plot analysis

The *Barbara* image, the encrypted *Barbara*, and the decoded *Barbara* are all displayed in Fig. 8. The encrypted image's pixels are not physically connected, as shown by

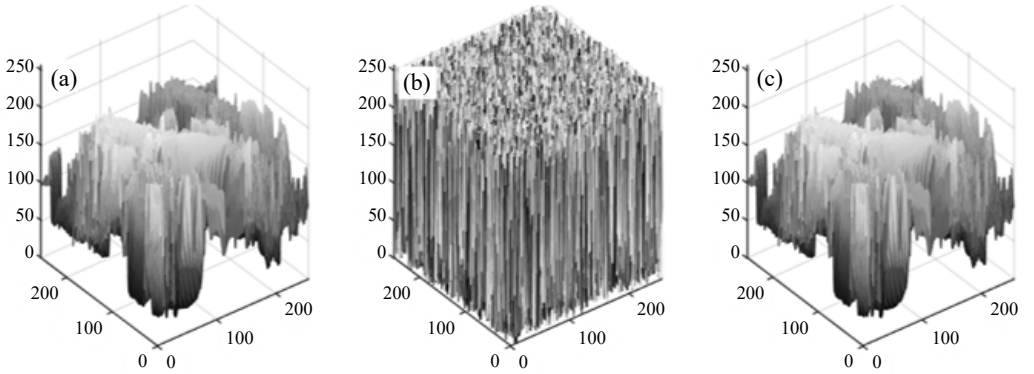

Fig. 8. The image pixel intensity distribution of the (a) input image of *Barbara*, (b) corresponding encrypted image, and (c) decrypted image individually.

Fig. 8(b). The CC parameter, which indicates how closely an encrypted image matches its original input version, is determined to have the value of –0.0042. In contrast, the input and decrypted images share a lot of similarities in terms of the pixel distribution and correlation between their individual pixels (CC = 0.9998). It effectively demonstrates the efficiency and dependability of the proposed method.

3.1.3. Correlation distribution analysis

1000 randomly selected horizontal, diagonal, and vertical pixels from the source picture and the encrypted image were used to conduct a correlation distribution analysis, the results of x which are shown in Fig. 9. The pixels in the input picture $I(x)$ are shown to be substantially associated with one another in the diagonal, horizontal, and vertical planes in Figs. 9(a), (c), and (e), while in Figs. 9(b), (d), and (f), they are not. This is evidence that pixels have been distributed randomly as anticipated by the idea and demonstrates the reliability of the suggested method.

3.1.4. Entropy analysis

Entropy of an image may be a good indicator of how uncertain or unpredictable it is. Eight bits is the maximum amount of entropy that may be used to represent a picture. The pixel distribution of an image is consistent with white stationary noise. Ideally, the entropy of the encrypted image would be as close to maximum as possible, and this is something that any good photo encryption system should strive for. As a result, we may use the equation to determine the encrypted image's entropy after utilizing the suggested technique to create it.

$$H(m) = -\sum_{i=1}^{M} p(m_i)\log_2 p(m_i) \tag{37}$$

where $p(m_i)$, stands for the probability of symbol m_i. To what extent the method described in the encrypted image causes unpredictability and uncertainty is shown by the result of 7.9955. This demonstrates the scheme's robustness and stability.

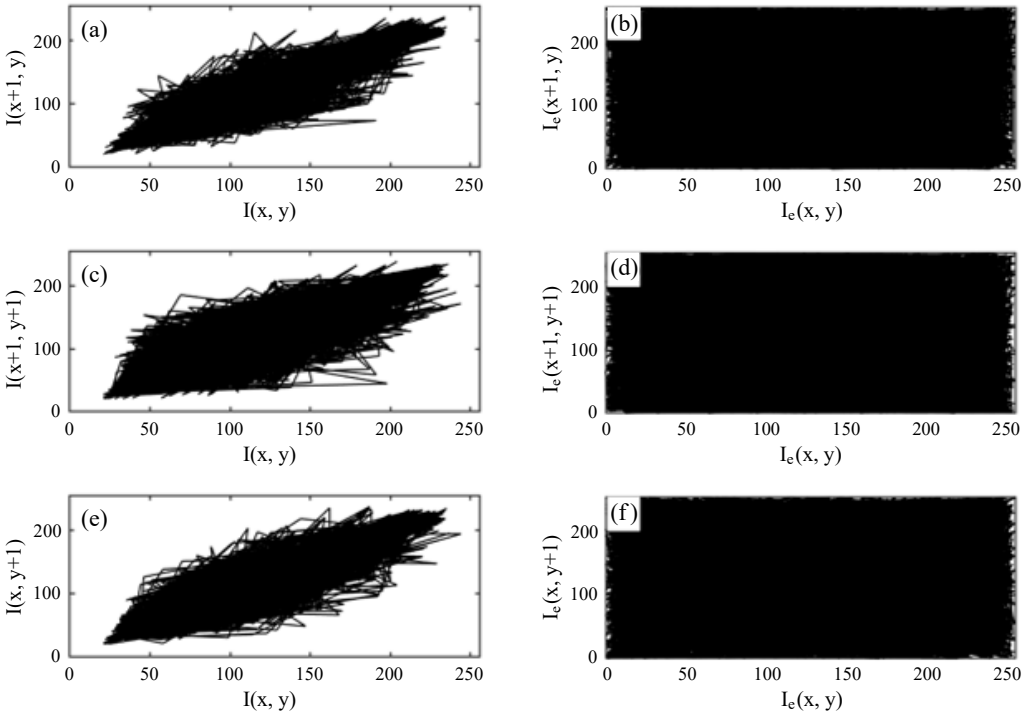

Fig. 9. The correlation distribution analysis of randomly selected 1000 pixels of the (a, c, e) input image $I(x)$ and (b, d, f) encrypted image $I_e(x)$ in horizontal, diagonal and vertical direction.

The PSNR results indicate that while there is a slight loss in image quality, it is within acceptable limits for secure image transmission. This indicates that the proposed cryptosystem achieves the desired level of randomness.

3.2. Attack analysis

Several types of threats have been investigated, and the suggested strategy's resilience has been determined. Occlusion attacks, noise attacks, and other common forms of cryptographic assault were all subjected to the method's scrutiny.

3.2.1. Occlusion attack analysis

There is always the possibility that part or all a communication may be corrupted or deleted due to network problems or outages. An adversary may try to decrypt the image by removing data, so any security approach must take this possibility into account. It has been determined whether the proposed strategy is effective against certain attacks or environmental circumstances. Three versions of the encrypted picture are displayed in Figs. 10(a–c), each with a different amount of occlusion (25%, 50%, and 75%) to illustrate how successful and resilient the suggested technique is against occlusion attacks. Figure 10(d, g, j) displays *Peppers*' and *Barbara*'s original, unencrypted pictures, as well

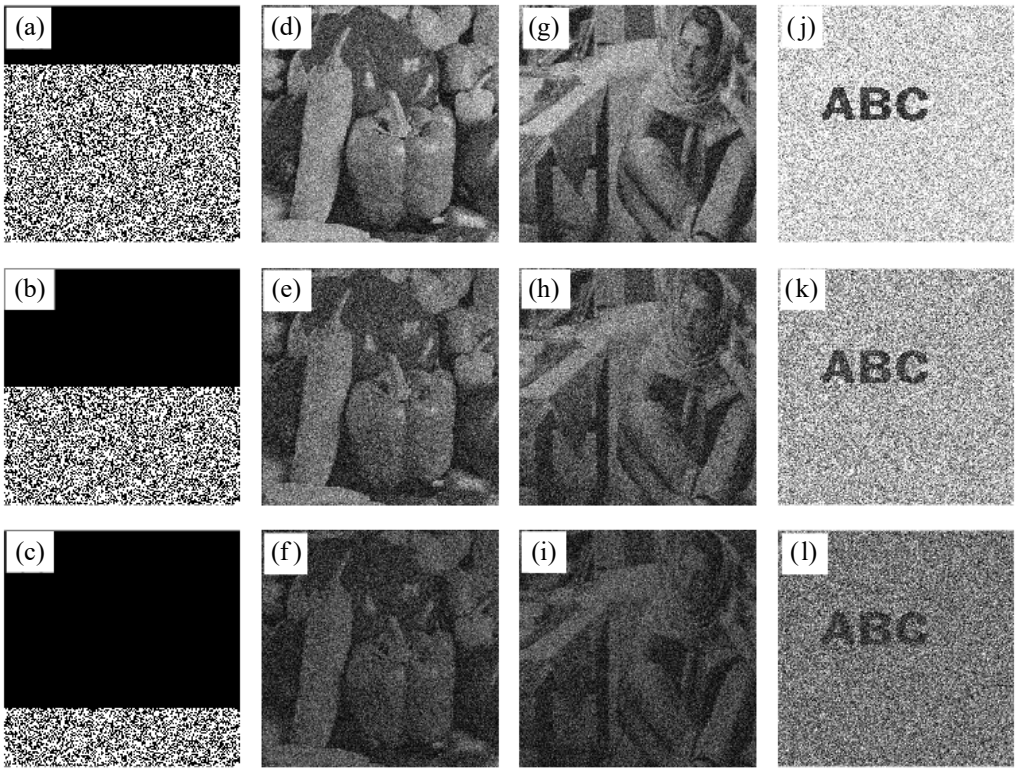

Fig. 10. Occlusion results for the grayscale *Barbara*, *Peppers* and binary image with some degree of occlusion. (a–c) The cipertext image with 25%, 50%, and 75% occlusion; correspondingly recovered grayscale (d–f) *Peppers*, (g–i), *Barbara*, and (j–l) binary image.

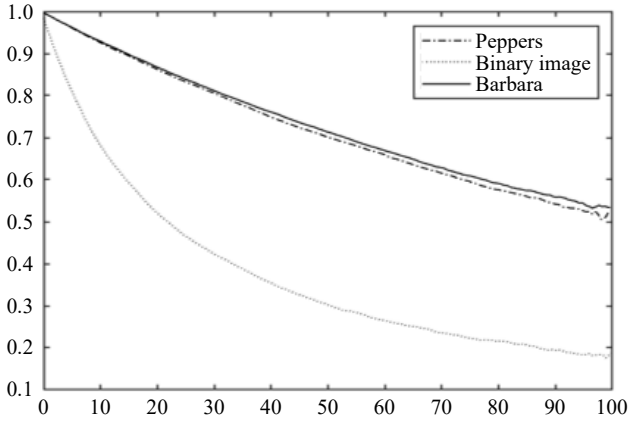

Fig. 11. CC plot against percentage of occlusion for the grayscale *Barbara*, *Peppers* and binary image.

as the binary image after 25% occlusion. Figure 10(e, h, k) and (f, i, l) displays the decrypted versions of these photos, with occlusion percentages ranging from 50% to 75%. Here, it is demonstrated that the suggested strategy can resist an occlusion assault.

Figure 11 illustrates a CC plot against the percentage of occlusion as part of an investigation on the scheme's performance against occlusion attack (see below). The graph shows that *Peppers*' and *Barbara*'s grayscale pictures can withstand occlusion up to almost 99%, while the results for binary images are good, although the necessary information is transmitted up to 80%. Even when the encrypted image is up to 50% obscured, the recovered image can still be recognized, even though its quality decreases as the amount of obscured region increases. The plot of CC shows how occlusion affects the larger range of occluded region.

3.2.2. Noise attack analysis

The quality of a communication channel may be degraded at any time by the presence of noise. Even if you encrypt a message before sending it, the receiver may have prob-

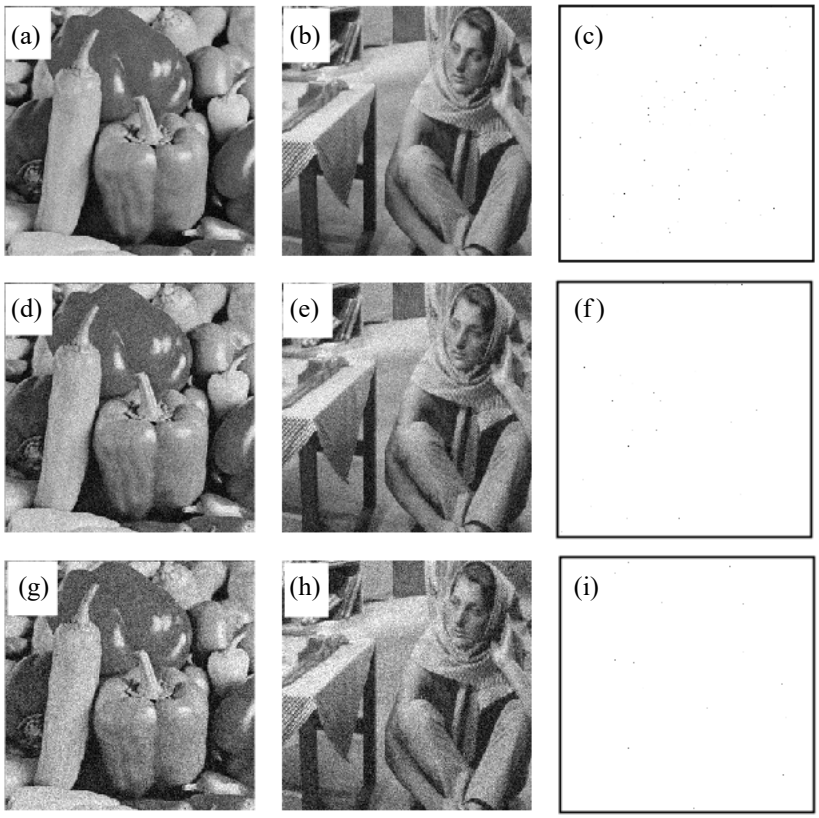

Fig. 12. The decryption results obtained for images of *Peppers*, *Barbara* and binary image after contaminating encrypted image with noise strength (a–c) $K = 2500$, (d–f) $K = 5000$, and (g–h) $K = 7500$, respectively.

lems decrypting it if they are hacked. The recommended approach has been evaluated for its efficacy against such assaults. The ciphertext (CT) generated using the suggested approach is tainted (CT′) by normal random noise N with zero mean and unit variance, according to the following equation:

$$\mathrm{CT}' = \mathrm{CT} + K \times N \tag{38}$$

where K refers to noise strength.

Figure 12 displays decrypted images of *Peppers* (a, d, g), *Barbara* (b, e, h), and a binary figure (c, f, i) that were originally affected by noise of strengths $K = 2500$, 5000 and 7500, respectively. The proposed approach is effective since noise invasions into grayscale images are readily rejected. Grayscale images with considerable noise may be recovered using the proposed method. Unfortunately, the processing of binary pictures is different. Figure 13 depicts the outcomes of this analysis. Binary images captured at $K = 50$, $K = 75$, $K = 100$, $K = 250$, and $K = 500$ will be subjected to a noise attack, and the effectiveness of the proposed technique will be assessed. The outcome indicates that up to $K = 500$, the method is similarly resistant to noise assaults on binary image. Figure 14(a) and (b) shows a plot of CC *versus* noise intensity K, demonstrating the robustness of grayscale images with a CC = 0.94. Figure 14(c) shows the findings for a binary image up to $K = 500$, after which the CC begins to decline.

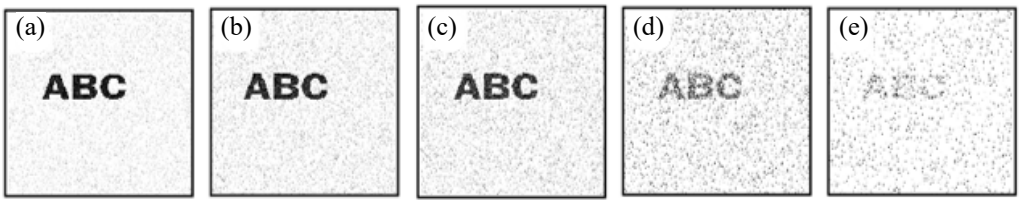

Fig. 13. Decryption results obtained for binary image taken with (a) $K = 50$, (b) $K = 75$, (c) $K = 100$, (d) $K = 250$, and (e) $K = 500$.

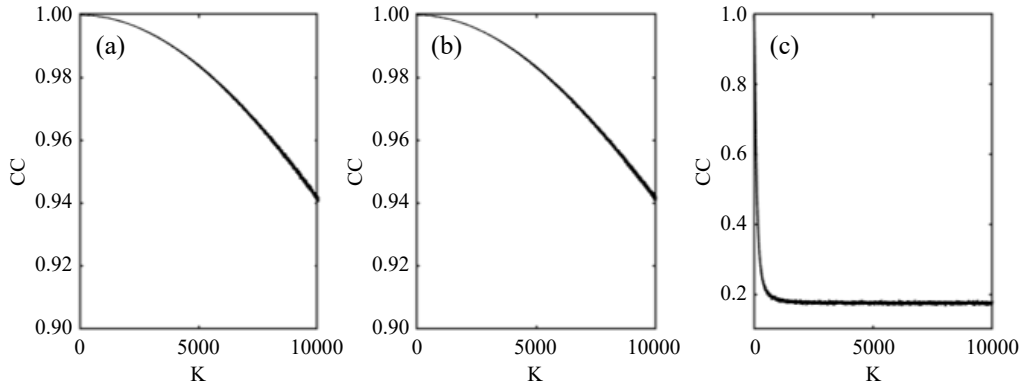

Fig. 14. CC plot against noise strength K for input images of (a) *Peppers*, (b) *Barbara*, and (c) binary image.

A good encryption algorithm should be able to resist noise attacks. Attacks with 0.01, 0.05, and 0.1 salt-and-pepper noise are performed as shown in Fig. 12(c, f, i). It can be seen that the decryption images after adding 0.1 salt-and-pepper noise are still identifiable. Therefore, our algorithm has good robustness and can efficiently resist noise attacks.

3.2.3. Classical cryptographic attacks

The suggested solution to specific ciphertext concerns depends on unique umbrella maps and the Yang–Gu mixture algorithm [24, 43]. Numerous studies [14, 19, 26] have demonstrated that if a system can withstand a particular plaintext assault, it can also withstand a more generalized plaintext assault [4]. Therefore, neither chosen ciphertext nor known plaintext can be used to break the offered technique.

3.3. Key sensitivity analysis

As the keys are essential to the security of any encryption mechanism, the scheme must be sensitive to these parameters. The proposed mechanism has been shown to work via the use of a key sensitivity analysis. An additional key, represented by $D(u, v)$, is used in the proposed system; it is a sequence of a random phase key, $R(u, v)$, and binary phase variation, $b(u, v)$. Key1 refers to the private key used in the system. Increasing the scheme's key space relies heavily on the Fresnel parameters. Figure 15 demonstrates the MSE statistical metric visually to show how sensitive *Barbara*'s image is to different Fresnel transform orders. According to the statistics, MSE is zero only for the accurate values of the Fresnel orders and is high otherwise. All characteristics of umbrella maps are extremely sensitive to modifications, as shown by SACHIN *et al*. [43]. Figure 16 shows the incorrect findings that were utilized during decryption. They include a value of a, b, c, and d are 0.8742, 0.453, 1.8, and 0.6, where $x_0 = 5.178$ and

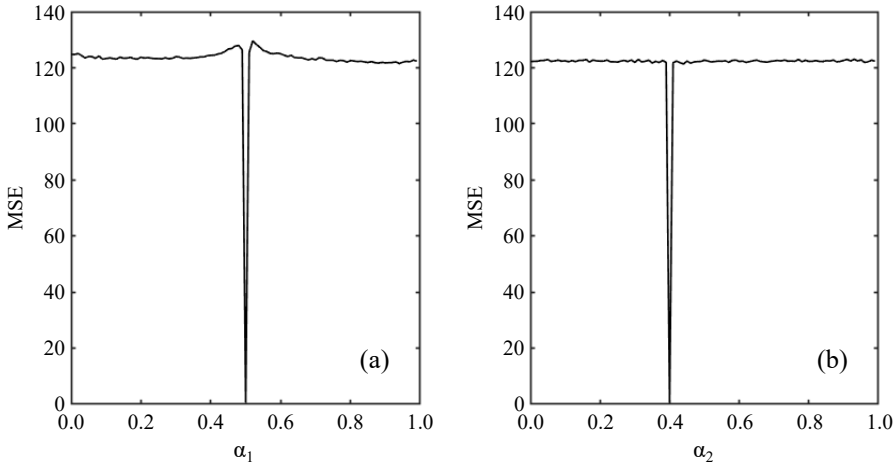

Fig. 15. The sensitivity plots of Fresnel transform orders in terms of statistical parameter MSE for *Barbara* image.

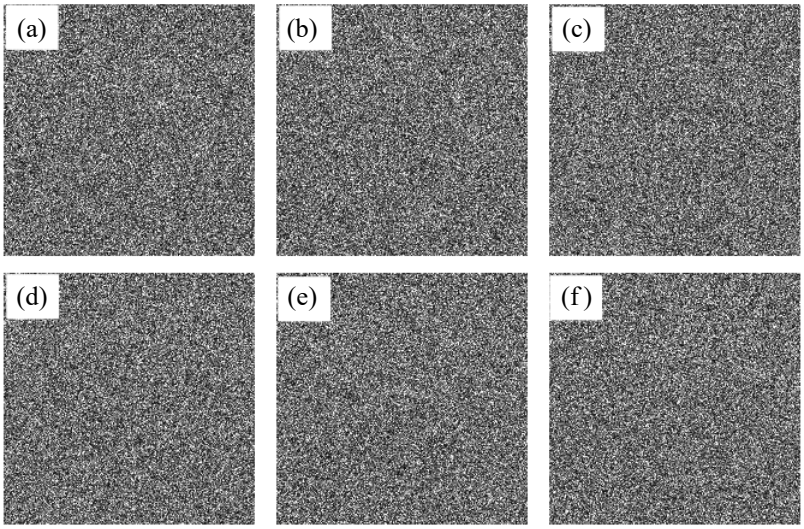

Fig. 16. Decryption results for input image of *Barbara* with wrong values of (a) $a = 0.8742$, (b) $b = -0.453$, (c) $c = 1.8$, (d) $d = 0.6$, (e) $x_0 = 5.178$, and (f) $y_0 = 0.17$.

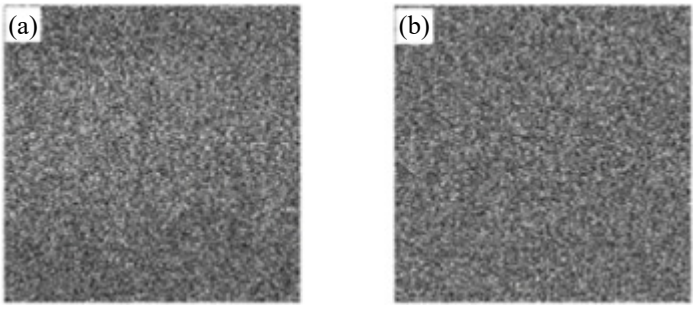

Fig. 17. Decryption results for wrong key (a) DPM2, and (b) Key1 for input image of *Barbara*.

$y_0 = 0.17$. The repercussions of employing the incorrect private key (DPM2, Key1) are also examined. Figure 17 displays deciphering errors caused by using DPM2 and Key1 incorrectly. Regardless of the input image, the outcome is constant. The results reveal that the suggested system is sensitive to the keys and experimental conditions.

4. Comparison analysis

Recent approaches, such as those described by WANG *et al*. [35], SUI *et al*. [41], ABUTURAB [3], CHEN *et al*. [7] and others are examined and contrasted with the proposed method. In a study Table 2 provides brief explanations of these various transforms based on their transform domains, nature, image types, implementation, statistical metrics, and performance against cyberattacks. The idea demonstrates a high degree of accuracy in the face of private keys and fractional coefficients in the Fourier

transform. It is likewise resistant to noise attacks and occlusion attacks. This proposed system is impenetrable by standard cryptographic attacks. Hence, the proposed method excels in key space, key sensitivity, and attack analysis.

To ensure the proposed mechanism is effective, it is compared quantitatively and qualitatively to previously presented systems. For a qualitative comparison of the proposed system to other, more recent schemes, see Table 2. Added to that input image and the methodological approach carrying out to the transform domain, distinguishing factors include measurable parameters, permutation approaches, substitution strategies, statistical analysis of the symmetric encryption, resilience against attacks, and encrypted output. The proposed approach is very reactive to shifts in private keys and other parameters. It also outperforms currently used methods by a wide margin in terms of robustness against noise attacks and occlusion attacks. This scheme's key management is similarly simple to that of alternatives that use a random phase mask. The final product is an actual number, making it easy to send and store. Table 3 shows correlation coefficients values *versus* different noise intensities. The proposed method is safe even when compared to more conventional kinds of encryption. The proposed method is superior because it allows for more keys, improves key management, and stands up better against noise attacks. The created encryption has a simple structure that makes it convenient for sending and storing. Tables 4 and 5 provide information entropy and correlation coefficients for the encrypted image horizontally, vertically, and diagonally,

T a b l e 2. Qualitative comparison of proposed scheme to recently exiting schemes.

Basis of discrimination	WANG *et al*. [35]	SUI *et al*. [41]	ABUTURAB [3]	CHEN *et al*. [7]	RAKHEJA *et al*. [22]	Proposed scheme
Transform domain	Fourier	Gyrator	Gyrator and wavelet	Gyrator	Fractional Fourier transform	Fresnel transform
Types of images	Grayscale	Color	Color	Color	Grayscale	Grayscale and binary
Nature	Asymmetric	Asymmetric	Multiple -image encryption	Asymmetric	Asymmetric	Asymmetric
Implementation	Digital and optical	Optoelectronic	Optoelectronic	Optoelectronic	Digital	Optical and digital
Performance against attack	Occlusion and noise attacks	Noise, occlusion and brute-force attacks	Occlusion and noise attacks	Occlusion and parameter sensitivity analysis	Noise, occlusion, and brute-force attacks	Noise, occlusion, and classical cryptographic attacks
Statistical metrices	CC	CC	CC	NCC, PSNR	Entropy, CC, MSE	Entropy, CC, MSE, NMSE, PSNR

T a b l e 3. CC values *versus* different noise intensities for grayscale image.

Noise intensity	25	50	75	100
CC	0.9486	0.8217	0.6720	0.5441

T a b l e 4. Comparison of average information entropy.

	Information entropy
YU *et al*. [45]	7.9988
ANJANA *et al*. [47]	7.9922
SACHIN *et al*. [24]	7.9977
WANG *et al*. [34]	7.9993
SHAH *et al*. [49]	7.9595
Proposed scheme	7.9955

T a b l e 5. Average correlation coefficients.

	Horizontal	Vertical	Diagonal
SACHIN *et al*. [43]	0.0198	0.0224	0.0096
ABUTURAB [44]	–0.0198	–0.0028	–0.0036
YU *et al*. [45]	0.0042	–0.0033	0.0016
WANG *et al*. [34]	0.0070	0.0065	0.0067
SHAH *et al*. [49]	–0.0034	0.02567	–0.01655
CHAI *et al*. [50]	0.0028	0.0029	0.0037
Proposed scheme	0.002034	0.001146	0.000534

provides a fair comparison of the suggested technique to existing ones. The outcomes indicate the strategy's fruitfulness and efficacy. Decorating the pixels in both ways efficiently increases the encrypted image's information entropy.

5. Conclusion

In this research, we provide an approach for encrypting digital images employing the Fresnel transform that is nonlinear and chaotic. The established procedures use a Yang–Gu mixed amplitude-phase retrieval method and a unique chaotic umbrella map. An input visual picture is transformed using a deterministic phase mask and Fresnel transform, and its pixels are then scrambled using an umbrella map. When the picture has been encrypted using a second deterministic mask, the key space and security are both expanded by applying the Fresnel transform to the ciphertext. To evaluate and confirm the effectiveness of the proposed scheme, a comprehensive set of statistical and attack-based analyses were conducted. These included histogram analysis, entropy analysis, key sensitivity analysis, correlation distribution analysis, occlusion attack analysis, noise attack analysis, and assessments against classical cryptographic attacks. The findings indicate that the proposed encryption algorithm exhibits outstanding resilience, particularly in the presence of noise attacks. The experimental results of this work reveal that the recommended picture encryption methodology is superior to other originally proposed image encryption techniques due to its high complexity and greater security.

References

[1] Abdelazeem R.M., Youssef D., El-Azab J., Hassab-Elnaby S., Agour M., *Three-dimensional visualization of brain tumor progression based accurate segmentation via comparative holographic projection*, PLoS ONE **15**(7), 2020: e0236835. https://doi.org/10.1371/journal.pone.0236835

[2] Abundiz-Pérez F., Cruz-Hernández C., Murillo-Escobar M.A., López-Gutiérrez R.M., Arellano-Delgado A., *A fingerprint image encryption scheme based on hyperchaotic Rössler map*, Mathematical Problems in Engineering, Vol. 2016, 2016: 2670494. https://doi.org/10.1155/2016/2670494

[3] Abuturab M.R., *Securing multiple information using wavelet transform and Yang-Gu mixture amplitude-phase retrieval algorithm*, Optics and Lasers in Engineering **118**, 2019: 42-51. https://doi.org/10.1016/j.optlaseng.2019.01.015

[4] Archana, Sachin, Singh P., *Cascaded unequal modulus decomposition in Fresnel domain based cryptosystem to enhance the image security*, Optics and Lasers in Engineering **137**, 2021: 106399. https://doi.org/10.1016/j.optlaseng.2020.106399

[5] Archana, Sachin, Singh P., *Cryptosystem based on triple random phase encoding with chaotic Henon map*, [In] Ray K., Roy K.C., Toshniwal S.K., Sharma H., Bandyopadhyay A. [Eds.], *Proceedings of International Conference on Data Science and Applications*, Lecture Notes in Networks and Systems, Vol. 148, Springer, Singapore, 2020: 73-84. https://doi.org/10.1007/978-981-15-7561-7_5

[6] Belokolos E.D., Kharchenko V.O., Kharchenko D.O., *Chaos in a generalized Lorenz system*, Chaos, Solitons & Fractals **41**(5), 2009: 2595-2605. https://doi.org/10.1016/j.chaos.2008.09.049

[7] Chen H., Du X., Liu Z, Yang C., *Color image encryption based on the affine transform and gyrator transform*, Optics and Lasers in Engineering **51**(6), 2013: 768-775. https://doi.org/10.1016/j.optlaseng.2013.01.016

[8] Chen H., Liu Z, Tanougast C., Liu F., Blondel W., *Optical cryptosystem scheme for hyperspectral image based on random spiral transform in gyrator domains*, Optics and Lasers in Engineering **137**, 2021: 106375. https://doi.org/10.1016/j.optlaseng.2020.106375

[9] Davidchack R.L., Lai Y.-C., Klebanoff A., Bollt E.M., *Towards complete detection of unstable periodic orbits in chaotic systems*, Physics Letters A **287**(1-2), 2001: 99-104. https://doi.org/10.1016/S0375-9601(01)00463-7

[10] Deng J., Zhou M., Wang C., Wang S., Xu C., *Image segmentation encryption algorithm with chaotic sequence generation participated by cipher and multi-feedback loops*, Multimedia Tools and Applications **80**, 2021: 13821-13840. https://doi.org/10.1007/s11042-020-10429-z

[11] Dhar S., Singh J., Singh P., Yadav A.K., *Stability and bifurcation analysis of delayed neural network using harmonic balance approach*, [In] *2019 6th International Conference on Signal Processing and Integrated Networks (SPIN)*, Noida, India, IEEE, 2019: 1053-1057. https://doi.org/10.1109/SPIN.2019.8711676

[12] Hasib A.A., Haque A.A.Md.M., *A comparative study of the performance and security issues of AES and RSA cryptography*, [In] *2008 Third International Conference on Convergence and Hybrid Information Technology*, Busan, Korea, IEEE, 2008: 505-510. https://doi.org/10.1109/ICCIT.2008.179

[13] Huang J.-J., Hwang H.-E., Chen C.-Y., Chen C.-M., *Optical multiple-image encryption based on phase encoding algorithm in the Fresnel transform domain*, Optics & Laser Technology **44**(7), 2012: 2238-2244. https://doi.org/10.1016/j.optlastec.2012.02.032

[14] Jiao S., Feng J., Gao Y., Lei T., Yuan X., *Visual cryptography in single-pixel imaging*, Optics Express **28**(5), 2020: 7301-7313. https://doi.org/10.1364/OE.383240

[15] Kumar R., Quan C., *Optical colour image encryption using spiral phase transform and chaotic pixel scrambling*, Journal of Modern Optics **66**(7), 2019: 776-785. https://doi.org/10.1080/09500340.2019.1572807

[16] KUMAR S., KUMAR A., SAMET B., DUTTA H., *A study on fractional host–parasitoid population dynamical model to describe insect species*, Numerical Methods for Partial Differential Equations **37**(2), 2021: 1673-1692. https://doi.org/10.1002/num.22603
[17] KUMARI E., MUKHERJEE S., SINGH P., KUMAR R., *Asymmetric color image encryption and compression based on discrete cosine transform in Fresnel domain*, Results in Optics **1**, 2020: 100005. https://doi.org/10.1016/j.rio.2020.100005
[18] NISHCHAL N.K., *Optical Cryptosystems*, IOP Publishing, 2019.
[19] 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: 1044-1046. https://doi.org/10.1364/OL.31.001044
[20] RAKHEJA P., SINGH P., VIG R., *An asymmetric image encryption mechanism using QR decomposition in hybrid multi-resolution wavelet domain*, Optics and Lasers in Engineering **134**, 2020: 106177. https://doi.org/10.1016/j.optlaseng.2020.106177
[21] RAKHEJA P., SINGH P., VIG R., KUMAR R., *Double image encryption scheme for iris template protection using 3D Lorenz system and modified equal modulus decomposition in hybrid transform domain*, Journal of Modern Optics **67**(7), 2020: 592-605. https://doi.org/10.1080/09500340.2020.1760384
[22] RAKHEJA P., YADAV S., TOBRIA A., *A novel image encryption mechanism based on umbrella map and Yang-Gu algorithm*, Optik **271**, 2022: 170152. https://doi.org/10.1016/j.ijleo.2022.170152
[23] REFREGIER P., JAVIDI B., *Optical image encryption based on input plane and Fourier plane random encoding*, Optics Letters **20**(7), 1995: 767-769. https://doi.org/10.1364/OL.20.000767
[24] SACHIN, SINGH P., *A novel chaotic Umbrella map and its application to image encryption*, Optical and Quantum Electronics **54**, 2022: 266. https://doi.org/10.1007/s11082-022-03646-3
[25] SACHIN, KUMAR R., SINGH P., *Modified plaintext attacks in a session for an optical cryptosystem based on DRPE with PFS*, Applied Optics **61**(2), 2022: 623-628. https://doi.org/10.1364/AO.446070
[26] SACHIN, KUMAR R., SINGH P., *Unequal modulus decomposition and modified Gerchberg Saxton algorithm based asymmetric cryptosystem in Chirp-Z transform domain*, Optical and Quantum Electronics **53**, 2021: 254. https://doi.org/10.1007/s11082-021-02908-w
[27] SITU G., ZHANG J., *Double random-phase encoding in the Fresnel domain*, Optics Letters **29**(14), 2004: 1584-1586. https://doi.org/10.1364/OL.29.001584
[28] STALIN S., MAHESHWARY P., SHUKLA P.K., MAHESHWARI M., GOUR B., KHARE A., *Fast and secure medical image encryption based on non linear 4D logistic map and DNA sequences (NL4DLM_DNA)*, Journal of Medical Systems **43**, 2019: 267. https://doi.org/10.1007/s10916-019-1389-z
[29] 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: 17-26. https://doi.org/10.1016/j.optlaseng.2015.06.005
[30] TASHIMA H., TAKEDA M., SUZUKI H., OBI T., YAMAGUCHI M., OHYAMA N., *Known plaintext attack on double random phase encoding using fingerprint as key and a method for avoiding the attack*, Optics Express **18**(13), 2010: 13772-13781. https://doi.org/10.1364/OE.18.013772
[31] TOKER D., SOMMER F.T., D'ESPOSITO M., *A simple method for detecting chaos in nature*, Communications Biology **3**, 2020: 11. https://doi.org/10.1038/s42003-019-0715-9
[32] UNNIKRISHNAN G., JOSEPH J., SINGH K., *Optical encryption by double-random phase encoding in the fractional Fourier domain*, Optics Letters **25**(12), 2000: 887-889. https://doi.org/10.1364/OL.25.000887
[33] UNNIKRISHNAN G., SINGH K., *Double-random fractional Fourier domain encoding for optical security*, Optical Engineering **39**(11), 2000: 2853-2859. https://doi:10.1117/1.1313498
[34] WANG X., LI Y., *Chaotic image encryption algorithm based on hybrid multi-objective particle swarm optimization and DNA sequence*, Optics and Lasers in Engineering **137**, 2021: 106393. https://doi.org/10.1016/j.optlaseng.2020.106393
[35] 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: 8-16. https://doi.org/10.1016/j.optlaseng.2015.09.008

[36] WANG X., LI Y., JIN J., *A new one dimensional chaotic system with application in image encryption*, Chaos, Solitons & Fractals **139**, 2020: 110102. https://doi.org/10.1016/j.chaos.2020.110102

[37] ZHOU N., PAN S., CHENG S., ZHOU Z., *Image compression–encryption scheme based on hyper-chaotic system and 2D compressive sensing*, Optics & Laser Technology **82**, 2016: 121-133. https://doi.org/10.1016/j.optlastec.2016.02.018

[38] ZHU H., GE J., QI W., ZHANG X., LU X., *Dynamic analysis and image encryption application of a sinusoidal-polynomial composite chaotic system*, Mathematics and Computers in Simulation **198**, 2022: 188-210. https://doi.org/10.1016/j.matcom.2022.02.029

[39] YANG F., MOU J., MA C., CAO Y., *Dynamic analysis of an improper fractional-order laser chaotic system and its image encryption application*, Optics and Lasers in Engineering **129**, 2020: 106031. https://doi.org/10.1016/j.optlaseng.2020.106031

[40] YE G., WU H., LIU M., SHI Y., *Image encryption scheme based on blind signature and an improved Lorenz system*, Expert Systems with Applications **205**, 2022: 117709. https://doi.org/10.1016/j.eswa.2022.117709

[41] SUI L., LIU B., WANG Q., LI Y., LIANG J., *Double-image encryption based on Yang-Gu mixture amplitude-phase retrieval algorithm and high dimension chaotic system in gyrator domain*, Optics Communications **354**, 2015: 184-196. https://doi.org/10.1016/j.optcom.2015.05.071

[42] GONG L.-H., LUO H.-X., WU R.-Q., ZHOU N.-R., *New 4D chaotic system with hidden attractors and self-excited attractors and its application in image encryption based on RNG*, Physica A: Statistical Mechanics and its Applications **591**, 2022: 126793. https://doi.org/10.1016/j.physa.2021.126793

[43] SACHIN, ARCHANA, SINGH P., *Optical image encryption algorithm based on chaotic Tinker Bell map with random phase masks in Fourier domain*, [In] Ray K., Roy K.C., Toshniwal S.K., Sharma H., Bandyopadhyay A. [Eds.], *Proceedings of International Conference on Data Science and Applications*, Lecture Notes in Networks and Systems, Vol. 148. Springer, Singapore, 2020: 249-262, https://doi.org/10.1007/978-981-15-7561-7_20

[44] ABUTURAB M.R., *A superposition based multiple-image encryption using Fresnel-domain high dimension chaotic phase encoding*, Optics and Lasers in Engineering **129**, 2020: 106038. https://doi.org/10.1016/j.optlaseng.2020.106038

[45] YU S.-S., ZHOU N.-R., GONG L.-H., NIE Z., *Optical image encryption algorithm based on phase-truncated short-time fractional Fourier transform and hyper-chaotic system*, Optics and Lasers in Engineering **124**, 2020: 105816. https://doi.org/10.1016/j.optlaseng.2019.105816

[46] SHEN Y., TANG C., XU M., LEI Z., *Optical asymmetric single-channel cryptosystem based on QZ synthesis for color images*, Optics & Laser Technology **153**, 2022: 108254. https://doi.org/10.1016/j.optlastec.2022.108254

[47] ANJANA S., RAKHEJA P., YADAV A., SINGH P., SINGH H., *Asymmetric double image encryption, compression and watermarking scheme based on orthogonal-triangular decomposition with column pivoting*, Optica Applicata **52**(2), 2022: 283-295. https://doi.org/10.37190/oa220210

[48] WANG M.M., ZHOU N.R., LI L., XU M.T., *A novel image encryption scheme based on chaotic apertured fractional Mellin transform and its filter bank*, Expert Systems with Applications **207**, 2022: 118067. https://doi.org/10.1016/j.eswa.2022.118067

[49] SHAH A.A., PARAH S.A., RASHID M., ELHOSENY M., *Efficient image encryption scheme based on generalized logistic map for real time image processing*, Journal of Real-Time Image Processing **17**, 2020: 2139-2151. https://doi.org/10.1007/s11554-020-01008-4

[50] CHAI X., ZHI X., GAN Z., ZHANG Y., CHEN Y., FU J., *Combining improved genetic algorithm and matrix semi-tensor product (STP) in color image encryption*, Signal Processing **183**, 2021: 108041. https://doi.org/10.1016/j.sigpro.2021.108041

Received February 26, 2025
in revised form June 25, 2025