Asian Journal of Physics
Vol. 33, Nos 3 & 4 (2024) 269-286
Available on: www.asianjournalofphysics.com

A secure image encryption method using toroidal vortex phase masks, QR decomposition, and gyrator transform

Hukum Singh[1] and Kehar Singh[1,2]

[1]Department of Applied Sciences, The NorthCap University, Gurugram-122 017, India

[2]Optics and Photonics Center, Indian Institute of Technology Delhi, New Delhi-110 016, India

Dedicated to Professor Anna Consortini for her significant contributions and pioneering works in the field of atmospheric turbulence and her continuous commitment to promote optics at global level

This paper introduces a security-enhanced hybrid image encryption method that employs toroidal vortex phase masks (TVPMs) and QR decomposition, with gyrator transform. The TVPMs used are intricate phase masks created by combining the phases of radial Hilbert transform (RHT) and the toroidal zone plate (TZP). The QR decomposition, a mathematical operation, is employed for matrix decomposition, serving as a replacement for the conventional phase-truncated Fourier transform (PTFT) method. The cryptosystem exhibits asymmetry, given that the encryption and decryption procedures are not the same as they rely on different sets of security keys. The keys produced during the encryption are utilized in the decoding system to retrieve the input image. System performance is tested by evaluating the mean-square error, peak signal-to-noise ratio, key sensitivity, cropping effect, correlation coefficients, 3-D mesh, histograms, and noise-attacks. © Anita Publications. All rights reserved.

Doi: 10.54955/AJP.33.3-4.2024.269-286

Keywords: Gyrator transform, Toroidal phase mask, Hilbert transform, QR decomposition, Performance evaluation.

1 Introduction

In the present era, images serve as a medium for transmitting information in daily life. The optical image handling strategies employed in information security structures exhibit substantial effectiveness and have garnered considerable attention. Numerous encoding methods were developed in the last few years [1-18] since the Double Random Phase Encoding (DRPE) technique was initially proposed by Refregier and Javidi in 1995 [1]. The DRPE was considered as one of the most attractive image encoding schemes due to its potential advantages in fast parallel computing and low energy consumption as compared to electronic digital processing. To bolster system security, numerous variants of the DRPE-based cryptosystem have been investigated. These include methods such as the fractional Fourier transform (FrFT) [19-25], Fresnel transform (FrT) [26-30], Fresnel wavelet transform (FWT) [31], fractional Mellin transform (FrMT) [32-35], gyrator transform (GT) [36-41], gyrator wavelet transform (GWT) [42-44], and fractional Hartley transform [45-54]. However, many of the DRPE-based cryptosystems are found to be susceptible to various attacks, including the chosen-cipher attack (CCA) [55], known-plaintext attack (KPA) [56-59], and chosen-plaintext attack (CPA) [60,61].

To tackle the weak security related issues of symmetric cryptosystems, asymmetric cryptosystems were proposed. Qin and Peng [62] introduced the pioneering work involving phase-truncated Fourier transform (PTFT) technique to overcome the linearity associated with symmetric routines. Because the decryption keys differ from the encryption keys, Cai *et al* [63] asserted that the equal modulus decomposition

Corresponding author
e mail: hukumsingh@ncuindia.edu (*Hukum Singh*)

(EMD)-based cryptosystem is nonlinear. Aburturab [64] proposed a single-channel color information security system using lower uper decomposition (LUD) in the GT domain. Xiong and Qian [65] proposed a hybrid attack-free optical cryptosystem based on two random masks and lower-upper decomposition with partial pivoting (LUDP). The LUDP method has also been used by Anshula and Singh [66]. Anjana *et al* [67] used orthogonal triangular decomposition with colum pivoting.

QR decomposition (QRD) has been used for a variety of applications such as matrix compression [68], discriminative clustering analysis [69], and security enhancement. Su *et al* [70] proposed a novel blind double image algorithm based on the QRD. Experimental results demonstrate that this algorithm achieves not only higher invisibility of watermarking but also stronger robustness against common image processing and geometric attacks. Abuturab [71] introduced a multiple color-image authentication system based on the HIS color space and QRD in the GT domain. The encrypted image undergoes the QRD, splitting it into Q and R parts. These parts are individually encoded through the GT. The system's compactness and feasibility are achieved through a single-channel image encryption method.

Rakheja *et al* [72] used 3D Lorenz chaotic system, linear canonical transform, and the QRD. Rakheja *et al* [73] also proposed a nonlinear image operation that involves compression, and utilizes the QRD, and the Hybrid Multi-resolution Wavelet (HMW) domain. The QRD technique not only generates ciphertext but also yields secret keys, facilitating compression due to the sparse matrix nature of the resulting ciphertext. This method demonstrates high resilience against various attacks.To further bolster security in optical image encryption schemes and fortify them against intruders, Anshula and Singh [74] proposed a new approach employing devil's toroidal lens masks (DTLMs) and QRD in the GT domain. Anjana *et al* [75] described an audio and image encryption scheme based on the QRD and random modulus decomposition in the Fresnel domain. Mehra and Nishchal [76] introduced a novel optical asymmetric fingerprint image encryption technique that utilizes the QRD in the GWT domain. They enhance the key space by combining the Gerchberg-Saxton phase retrieval algorithm, GWT, and QRD. A book by Golub and Van Loan [77] is a valuable source for information on matrix computations. Reference [78] may also be referred to for the QRD.

None of the previously mentioned techniques utilize the novel Toroidal Vortex Phase Mask (TVPM) in the GT domain through the QRD. The GT offers advantages like computational ease and convenience in optical execution. The proposed scheme in the present paper enhances security by expanding the key-space using the TVPM. These phase masks are easily located during decoding and offer self-centering properties. Additionally, they possess the capability of incorporating multiple keys within a single mask, providing a wide range of security parameters. The QRD technique is employed to derive private keys utilized in the decryption process. The public key, TVPM, is fashioned through the combination of Radial Hilbert Transform (RHT) and a toroidal Fresnel mask (Fig 1). This asymmetric cryptosystem is engineered to withstand basic attacks on phase-truncated FT, ensuring heightened security and robustness. Numerical simulations have been conducted to demonstrate the system's elevated level of optical security.

The paper is organized as follows: Section 2 presents a comprehensive theoretical background for our proposed approach. Section 3 details the proposed cryptosystem. In Sec 4, simulation analyses are conducted to assess the security level, including statistical and attack analyses. Section 5 compares our approach with other related works. Conclusions are drawn in Sec 6. Finally, Sec 7 describes the future outlook by mentioning: (i) use of artificial intelligence tools such as deep learning for evaluating the susceptility of cryptosystems to various attacks, and for designing systems with better security, (ii) use of quantum science and technology, and (iii) use of metasurfaces for safer and miniaturized cryptosystems.

2 Theoretical background

2.1 Gyrator transform (*GT*)

The GT of a function can be written [36-41] as,

$$G(u,v) = G^{\alpha}\{f(x_i, y_i)\}(u, v) = \oint_{-\infty}^{+\infty} \oint_{-\infty}^{+\infty} f(x_i, y_i)\, K_{\alpha}(x_i, y_i; u, v)\, dx_i\, dy_i \tag{1}$$

where the kernel $K_{\alpha}(x_i, y_i\,; u, v)$ is defined as,

$$K_{\alpha}(x_i, y_i\,; u,v) = \frac{1}{|\sin\alpha|} \exp\left[2i\pi \frac{(x_i\, y_i + uv)\, \cos\alpha - x_i\, v - y_i\, u}{\sin\alpha}\right] \tag{2}$$

Here, α is the transform angle and $G(u,v)$ is the output of the GT.

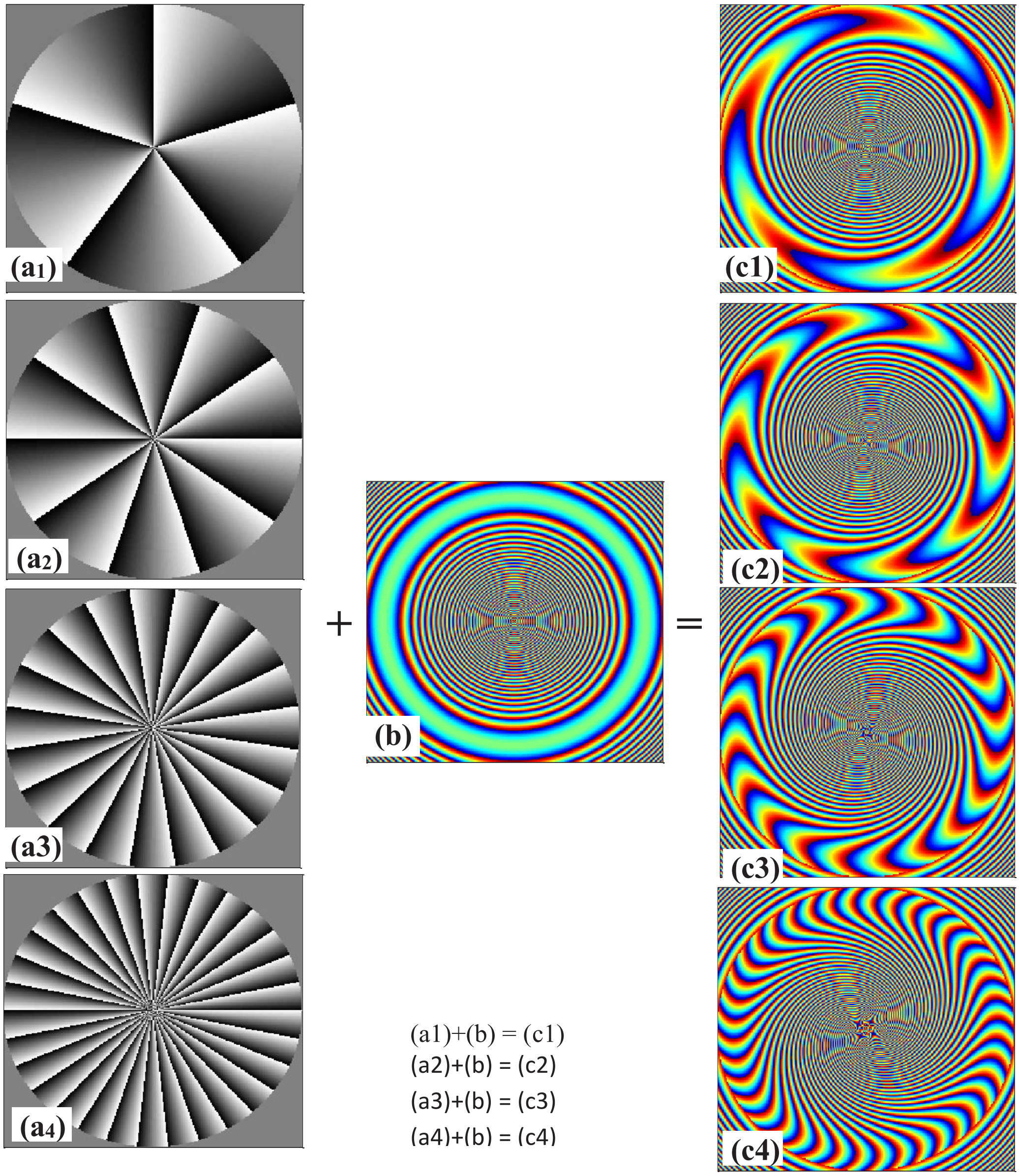


Fig 1. (a1-a4): RHT with $L = 5$, 10, 20, and 30, (b) Toroidal Lens mask, $\lambda = 632.8$ nm, $f = 160$ mm, pixel space scaling factor = 0.023, $r = 4.2$ cm, and $r_0 = 2.60$ cm. (c1-c4) Toroidal vortex phase mask. (Symbols are defined in sub-sec. 2.2 below).

2.2 Construction of the optical toroidal vortex phase mask (*TVPM*)

Phase of the TVPM key is obtained by taking the product of RHT and toroidal Fresnel mask (Fig 1) as follows [79-83],

$$\phi(x,\theta) = exp\left[i\left(L\theta - \frac{\pi(r-r_o)^2}{\lambda \times f}\right)\right] \tag{3}$$

where L is the topological charge of the vortex. λ and f are respectively the wavelength of the illuminating light and focal length of the toroidal lens. r and r_o are respectively the radii of zone plate and ring focus, and are positive constants.

2.4 Principle of QR *decomposition* [68-78]

The QR decomposition refers to the orthogonal-triangular decomposition of a matrix, commonly executed through the following definition:

$$[\mathrm{Q}, \mathrm{R}] = qr\,(\mathrm{A}) \tag{4}$$

The coefficients in the matrix representing the image denote the image pixel values. R is an $n \times n$ upper triangular matrix, and Q is an $n \times n$ unitary matrix meeting the condition Q×Q* = I = Q*×Q, where Q* represents the conjugate transpose of Q. A notable property of the R matrix is observed when the columns of matrix A exhibit correlation: the absolute values of the elements in the first row of R matrix tend to be larger compared to those in other rows. Orthogonal triangular decomposition is a matrix factorization technique in which a given matrix $\mathrm{E} \in \mathrm{R}^{n\times n}$ is decomposed to give an orthogonal matrix Q, an upper triangular matrix R and a permutation matrix P. In case of a complex matrix, instead of the orthogonal matrix, the decomposition gives a unitary matrix Q. Mathematically, it can be considered as if $\mathrm{E} \in \mathrm{R}^{n\times n}$ has linearly independent columns. In such a case, it can be factored [83] as

$$\mathrm{E} \times \mathrm{P} = \mathrm{Q} \times \mathrm{R} \tag{5}$$

If 'E' is considered as an image, its QR decomposition with column pivoting is given by the following equation [74,75].

$$\mathrm{E} = \mathrm{Q} \times \mathrm{R} \times \mathrm{P}^{-1} \tag{6}$$

Q is a matrix with orthonormal columns i.e. $\mathrm{Q}^{\mathrm{T}}\times\mathrm{Q} = 1$. If E is ($n\times n$) square matrix, then Q is orthogonal matrix i.e. ($\mathrm{Q}\times\mathrm{Q}^{\mathrm{T}} = 1$ or $\mathrm{Q}^{\mathrm{T}}\times\mathrm{Q} = 1$). R is a $n\times n$ upper triangular matrix with nonzero diagonal entries. R is nonsingular (diagonal elements are nonzero). P is a sparse matrix. P is selected such that the diagonal entries of R are non-increasing. In case of image encryption, inverse of P acts as ciphertext and Q×R serves as the private asymmetric key. As inverse of P is a sparse matrix where most of the elements are zero, its storage and transmission will take less memory and bandwidth as compared to the case when P is not sparse. The QRD produces sparse matrix which is an intermediate ciphertext and product of two orthogonal and triangular matrices serves as decryption keys. This process makes the scheme nonlinear.

3 Overview of the encryption and decryption schemes

Figure 2 presents the flowchart illustrating the encryption process of the proposed system. The initial input image, denoted as $I(x, y)$, serves as the basis for encryption. The primary keys for the encryption process are RPM and TVPM, which represent two phase masks. The encryption is executed as follows:

Step 1: Initially, the input image I undergoes multiplication with an RPM. Then, a GT is applied to the product of $I(x, y)$ and RPM, followed by a division of the transform spectrum utilizing the QRD. This process yields the first private key, *Key* 1, and generates an intermediate output $g_1(u,v)$, as represented by the following equations:

$$[\mathrm{Q}_1, \mathrm{R}_1, \mathrm{P}_1] = \mathrm{QRD}\{\mathrm{GT}^{\,\alpha}\,[I(x, y)\times\mathrm{RPM}]\} \tag{7}$$

Private key

$$Key\ 1 = \mathrm{Q}_1 \times \mathrm{R}_1 \tag{8}$$

$$g_1(u,v) = \mathrm{P}_1^{-1}(u,\ v) \tag{9}$$

The QRD operation, results in three products Q_1, R_1 and P_1. Symbol '×' denotes matrix multiplication, and the notation $\{.\}^{-1}$ represents the inverse matrix operation.

Step 2: The intermediate output $g_1(u, v)$ undergoes multiplication with the TVPM. The resultant is subjected to the inverse of GT i.e. $\mathrm{GT}^{-\beta}$, followed by a second QRD operation, resulting in the second private key, *Key* 2, and the final cipher image represented as E. The pertinent equations are given below:

$$[\mathrm{Q}_2, \mathrm{R}_2, \mathrm{P}_2] = \mathrm{QRD}\{\mathrm{GT}^{-\beta}\,[g_1(u,v)^*\ \mathrm{TVPM}]\} \tag{10}$$

Private key

$$Key\ 2 = \mathrm{Q}_2{\times}\mathrm{R}_2 \tag{11}$$

$$\mathrm{E} = \mathrm{P}_2^{-1}(x, y) \tag{12}$$

In this process, Q_2, R_2 and P_2 denote the three products derived from the second QRD operation. The proposed scheme incorporates within its operation, the utilization of the inverse matrices of two permutation matrices. This entire encryption process culminates in the generation of two private keys, namely, Private Key 1 and Private Key 2, which are subsequently employed in the decryption process.

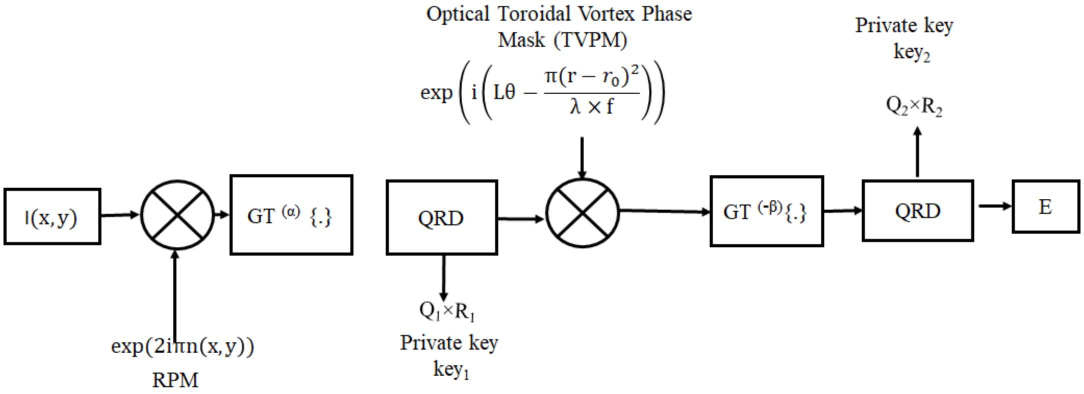


Fig 2. Flow diagram of the encryption process.

The decryption algorithm differs from the encryption process as the proposed system operates asymmetrically. The decryption process occurs as follows when the two private keys generated during the encryption step are available.

Step 1: The final output of the encryption process, E serves as an input during the decryption process. Initially E undergoes multiplication with the conjugate of TVPM, followed by a GT^{β} applied to the resulting function. The outcome of this transformation is denoted as g(u, v), representing an intermediate matrix.

$$g(u,v) = \{\mathrm{GT}^{\beta}\,[\mathrm{E}] \times \mathrm{TVPM}^*\} \tag{13}$$

where * defines the complex conjugate.

Step 2: The final decrypted image is generated by multiplying the intermediate matrix g(u, v) with the private key Key1 and then subjecting the product to the inverse GT. This process ultimately yields the decrypted image,

$$I(x, y) = \mathrm{GT}^{-\alpha}\,[g(u,\ v){\times}\text{Private Key 1}] \tag{14}$$

4 Simulated testing and assessment

The proposed scheme's performance was evaluated for speed, using a personal computer configured with an Intel(R) Core(TM) i3-2328 CPU @ 2.20 GHz-2.71 GHz, 2GB RAM, operating Windows 10, and running MATLAB R2019a (Version 9.6.0.1174912) 64-bit (win64). Two grayscale images, Capsicum and Text (OPT), are displayed respectively in Figs 3(a) and 3(b). Both images have a size of 256×256 pixels and serve as the input images for encryption in the proposed technique. Figures 3(c, d) illustrate the inverses of the P matrix derived from the input images using the proposed algorithm. Figures 3(e, f) display the initial set of private keys generated for the input images using the proposed algorithm. Additionally, Figs 3(g, h) show another set of private keys generated for the input images during the decryption algorithm. Figures 3(i, j) show the final encrypted images resulting from the encryption process. Additionally, Figs 3(k, l) illustrate the two random generated phase masks known as RPMs. When, we go through the decryption process with right set of decryption keys, we get the decrypted images which are similar to the original input images. The TVPM masks are formulated using specific parameter values: a wavelength $\lambda = 632.8$ nm, a focal length $f =$ 180 mm, and a pixel space scaling factor = 0.023. The transform/rotation angles selected for GT are $\alpha = 0.5\pi$ and $\beta = 0.7\pi$.

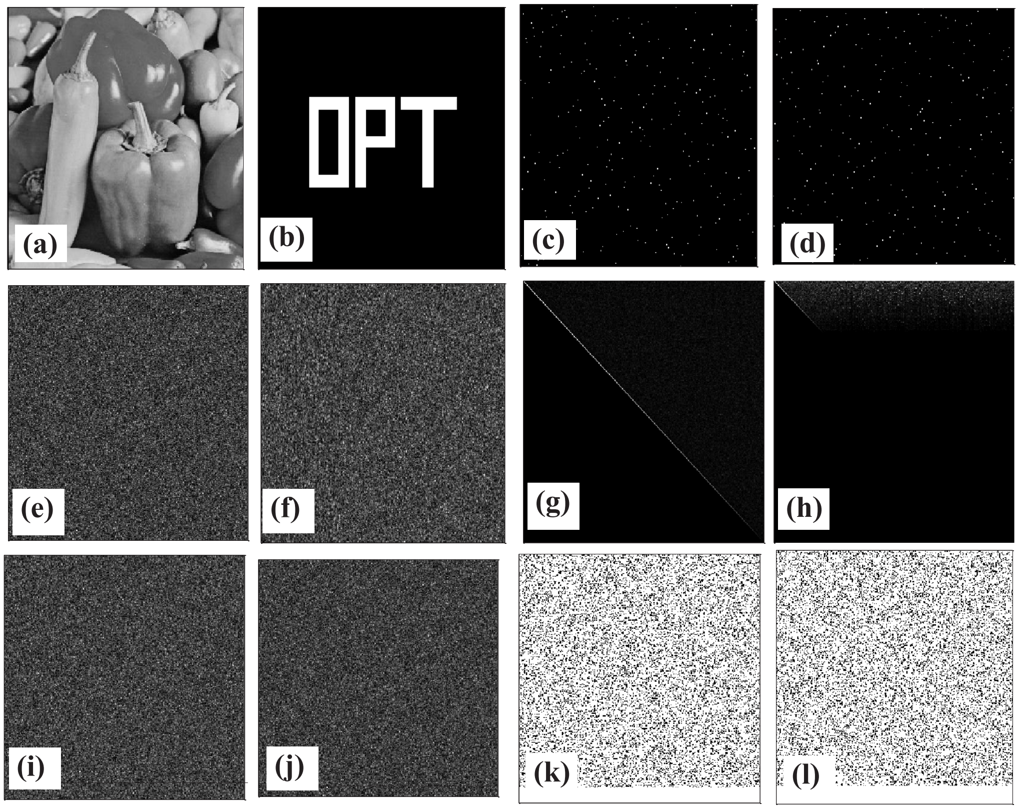


Fig 3. (a, b): Input images of Capsicum and OPT (c, d): Inverses of matrix P for the Capsicum and text images, (e, f):Two keys for the two cases (g, h): Two private keys for the images (i, j); Encrypted images for two cases, and (k, l); RPMs for the two images.

4.1 Statistical evaluation

To assess the credibility and effectiveness of the proposed technique, calculations for Mean-Square-Error (MSE) and Peak Signal-to-Noise Ratio (PSNR) were carried out. These evaluations were performed between the decrypted image, denoted as $I_d(x, y)$ and the original image, denoted as $I_0(x, y)$, to determine their authenticity and measure the strength of the proposed methodology.

$$\mathrm{MSE}\left(I_d(x,y), I_0(x,y)\right) = \sum_{x=1}^{M}\sum_{y=1}^{N}\frac{|I_d(x,y) - I_o(x,y)|^2}{M\times N} \tag{15}$$

where $M \times N$ is the number of pixels of the original image. Smaller MSE value indicates the high similarities between the original and decrypted image.

$$\mathrm{PSNR} = 10\times\log_{10}\left(\frac{255^2}{\sqrt{\mathrm{MSE}}}\right) \tag{16}$$

The calculated value of MSE for capsicum image is $4.15 \times e^{-25}$ and for OPT image is $5.41 \times e^{-26}$. The PSNR value for the capsicum image is 291.95 dB and for the OPT image 300.80 dB. These values illustrate the effectiveness of our scheme.

4.2 Security assessment

4.2.1 Key robustness assessment

In order to assess the sensitivity of the technique, a study was made on the effect of deviation in the correct values of the key, on the decrypted image quality. The specified parameters include $\alpha = 0.5\pi$, $\beta = 0.7\pi$ for the GT transform angles and TVPM parameters such as wavelength $\lambda = 632.8$ nm, focal length $f = 180$ mm, and pixel space scaling factor = 0.023. The architecture has been validated against departures in parameters, affirming their influence on the system's performance. Figures 4(a, b) display the decrypted images of OPT and Capsicum with an erroneous wavelength value of $\lambda = 532.8$ nm, while all other keys remain correct. Figures 4(c, d) show the decrypted images, for an incorrect value of $f = 150$ mm.

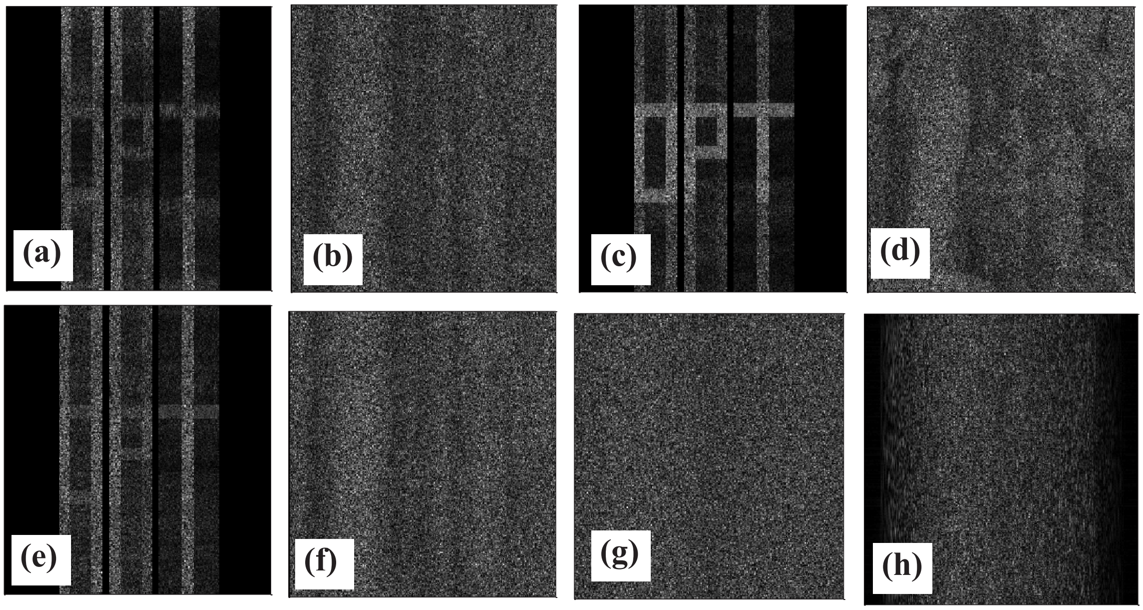


Fig 4. (a, b) decrypted image of OPT and Capcicum with incorrect $\lambda = 532.8$ nm, (c, d) with incorrect focal length $f = 150$ mm, (e, f) with incorrect $L = 24$, (g, h) with incorrect $\alpha = 0.4\pi$.

Figure 5 below shows the MSE and PSNR values as a function of the GT transform angle for the capcicum and OPT images. The curves show a sharp increase with the deviations in the transform angle for gray image. However, the increase is not so sharp in case of MSE for the binary object.

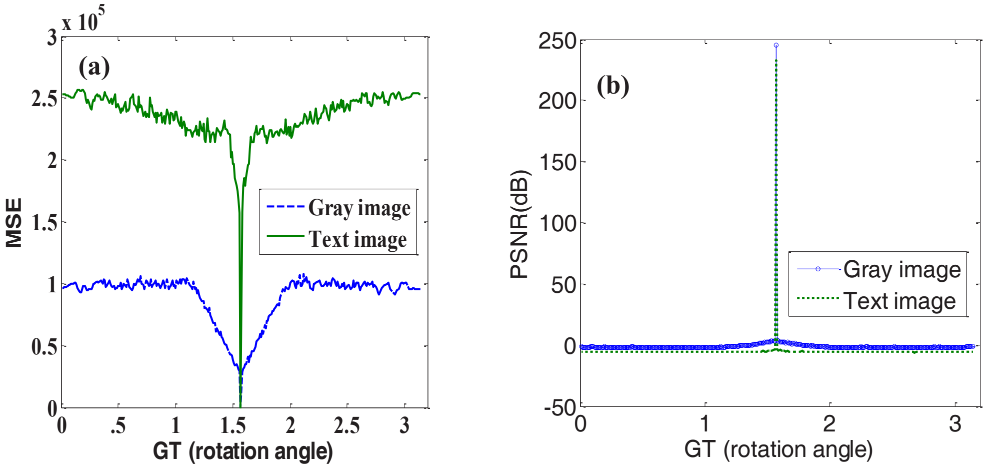


Fig 5. (a) MSE plot for transform angle $\alpha = 0.5\pi$ for images, and (b) PSNR plots against the transform angle $\beta = 0.7\pi$.

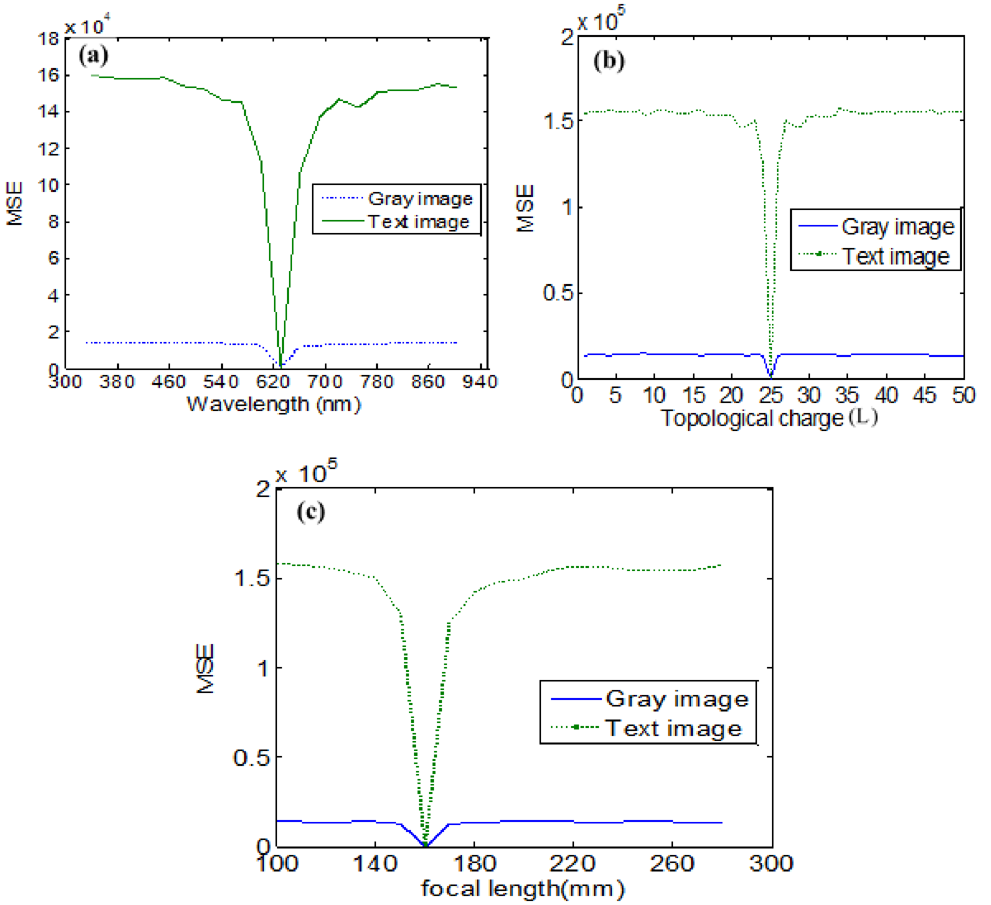


Fig 6. (a) MSE plots corresponding to the wavelength λ = 632.8nm, (b) MSE plots related to topological charge $L = 25$, and (c) MSE plots concerning focal length $f = 160$ mm for grayscale and OPT images.

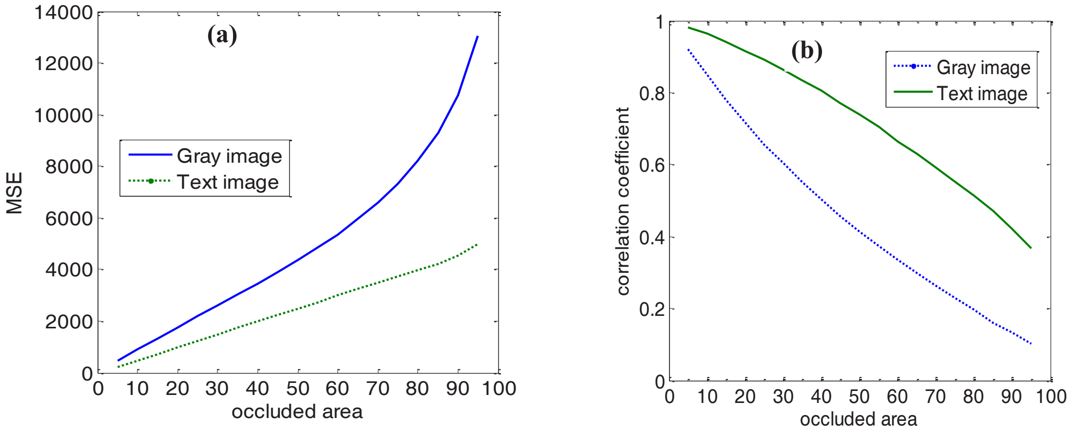
Figure 6(a) below shows the MSE plots against the wavelength λ = 632.8 nm and Fig 6(b) the MSE plots against the topological charge L = 25. Figure 6(c) shows the MSE plots with focal length for the Capsicum and OPT images. The graphs clearly reflect that the scheme is highly sensitive to the deviations in the GT transform angle, in case of the Capcicum image.

4.3 Attack analysis

The attack analysis of the proposed scheme encompasses occlusion attack and noise attack analyses.

4.3.1 Analysis of the impact of occlusion attacks

We analyzed the encrypted images due to the occlusion/cropping attacks. Indeed, most occlusion effect examinations in the past have been conducted solely on encrypted images. Such examinations validate the resilience of the cryptosystem. However, conducting occlusion examinations specifically for the newly introduced TVPM mask verifies not only the system's efficacy but also its stability and robustness. Figure 7(a) is the plots of the MSE against varying occluded areas, while Fig 7(b) presents the plots showcasing Correlation Coefficient (CC) against varying occluded areas for Capsicum and OPT images. These plots reveal our ability to extract the decrypted images, even if a small portion of the encrypted data is lost due to network problems or transmission discrepancies. Indeed, this underscores the scheme's robustness.



Figs 7(a, b). Plots of MSE and CC for different values (%) of occluded areas in case of Capsicum and OPT images.

4.3.2. Analysis based on the correlation-coefficient

The CC analysis involves selecting a thousand pairs of randomly chosen horizontally-, vertically-, and diagonally neighboring pixels between the input image and the encrypted image. The CC is then computed using the following formula,

$$CC = \frac{\sum_{i=1}^{N} (x_i - \bar{x})\,(y_i - \bar{y})}{\sqrt{\sum_{i=1}^{N} (x_i - \bar{x})^2 \sum_{i=1}^{N} (y_i - \bar{y})^2}} \qquad (17)$$

where $\bar{x} = \sum_{i=1}^{N} x_i$ and $\bar{y} = \sum_{i=1}^{N} y_i$ are the mean values of x_i and y_i. It is challenging to derive conclusive information solely from the CC analysis.

Figures 8(a) and 8(b) display the correlation plots for the input images of OPT and Capsicum, respectively in the diagonal direction. Figures 8(c) and 8(d) illustrate the CC plots for the corresponding encrypted images, in the diagonal direction.

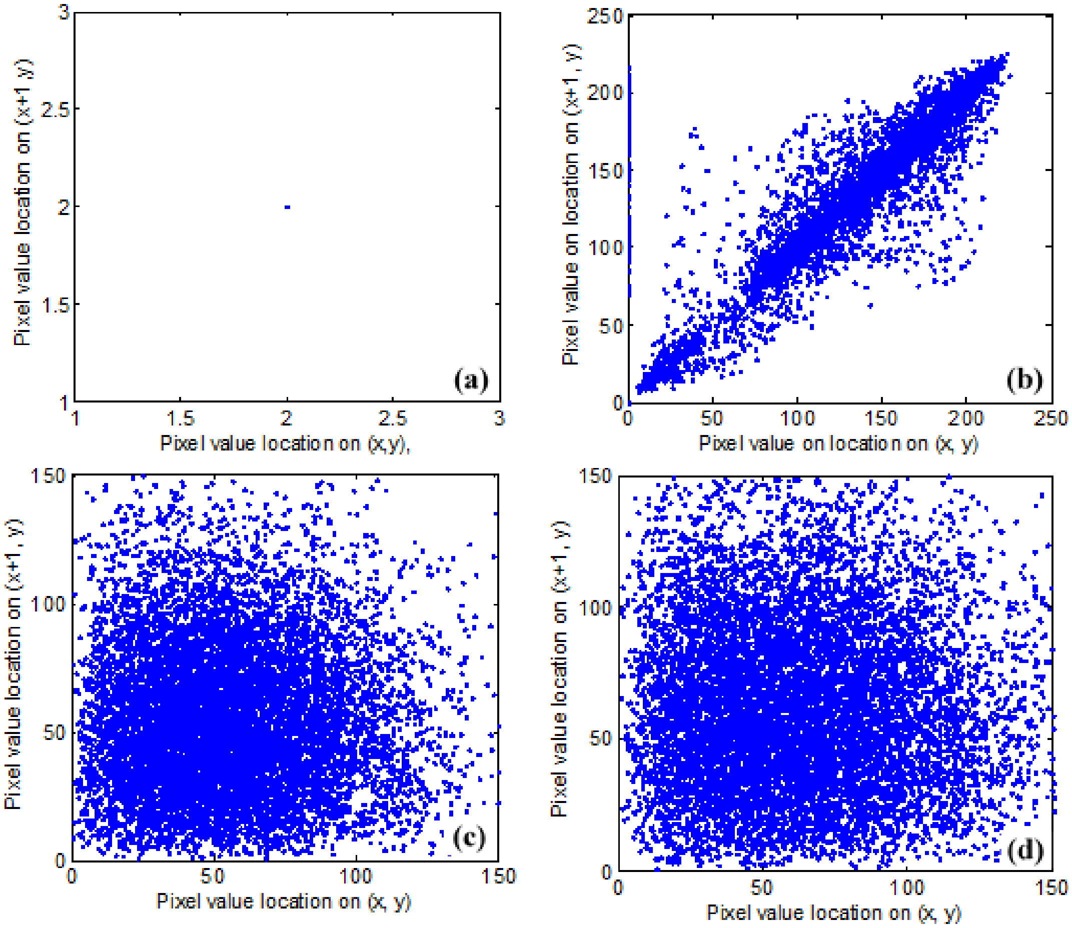


Fig 8. Correlation plots in the diagonal direction: (a, b) for the input images of OPT and Capsicum, respectively; (c,d) for the encrypted images of OPT and Capsicum, respectively.

4.3.3. Three D mesh analysis

Mesh plots are also important characteristics that are used to evaluate the efficacy of a cryptosystem by comparing the original-, encrypted-, and the decrypted images. Figures 9(a, b) represent the 3D mesh plots of the input images of OPT and Capsicum, respectively. Figures 9(c, d) are 3D mesh plots of encrypted images of OPT and Capsicum, respectively, and Figs 9(e, f) represent 3D mesh plots for the decrypted images of OPT and Capsicum, respectively. It can be seen that the 3D mesh plots of encrypted images are similar for the binary and gray images. Thus an attacker cannot find the correct image by looking at the mesh plots.

4.3.4. Histogram Analysis

Histogram analysis has been performed for the input-, encrypted-, and decrypted images. The histogram plots of input of Capcicum image and OPT are depicted in Figs 10(a, b). The histograms of encrypted grayscale and binary images look similar as shown in Figs 10(c, d). Therefore, we conclude that the hacker would not be able to gain any meaningful information from theses histograms.

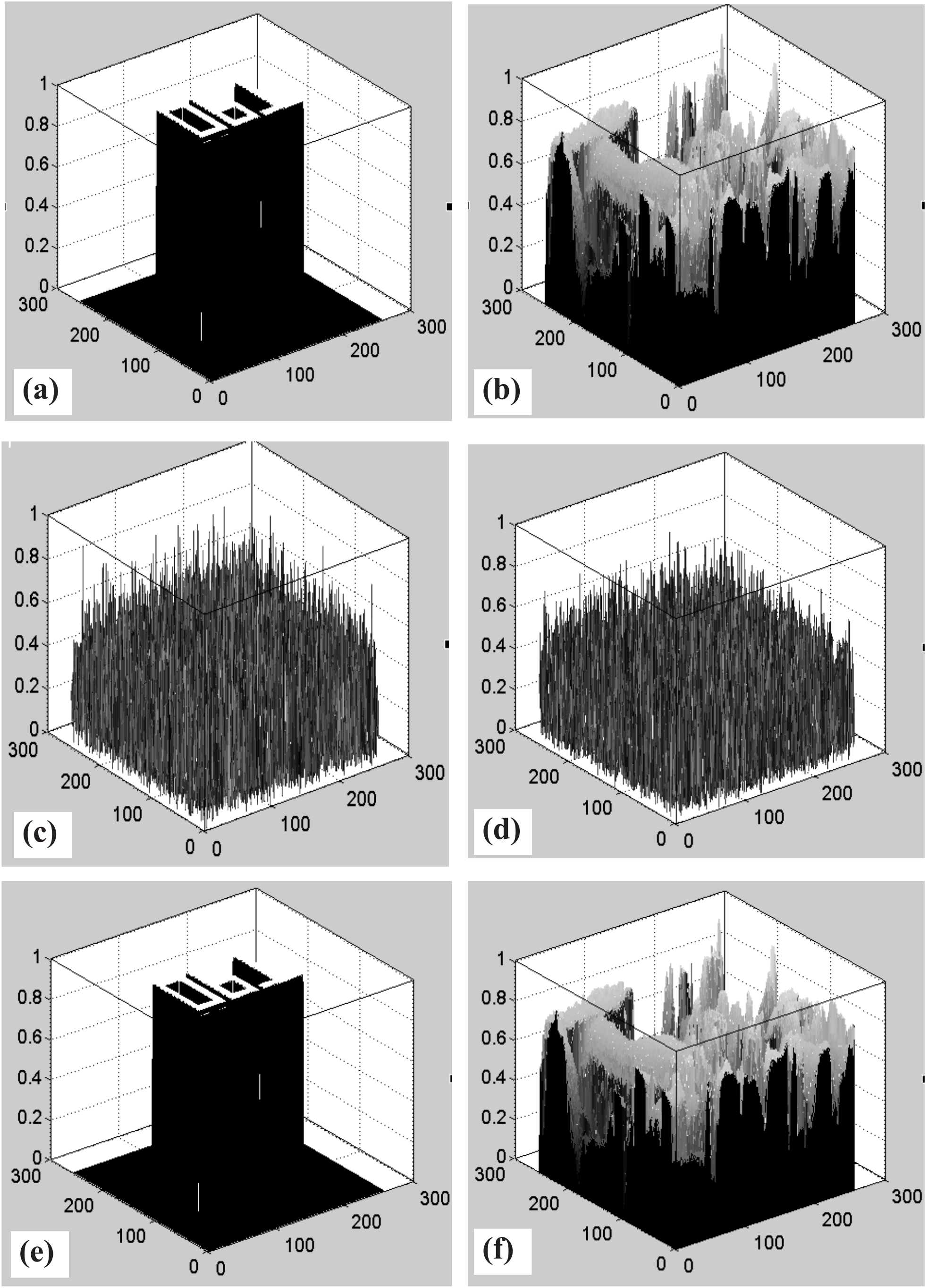


Fig 9. 3D mesh plots of : (a, b) input images of OPT and Capsicum, respectively; (c,d) encrypted images of OPT and Capsicum, respectively; and (e, f) decrypted images of OPT and Capsicum, respectively.

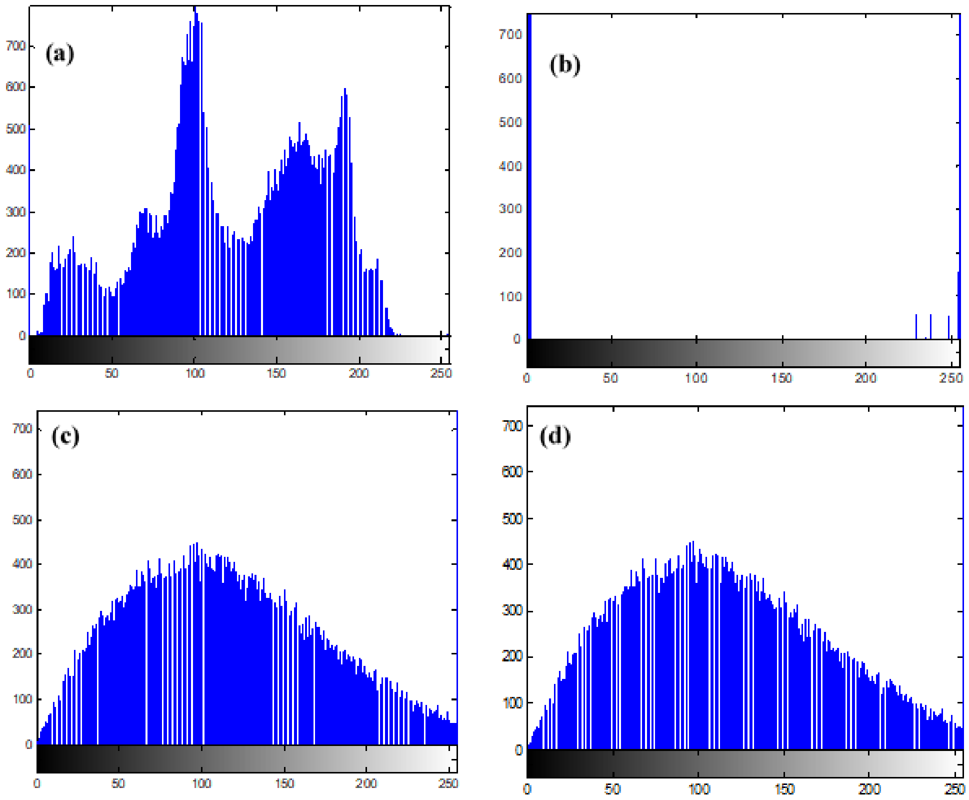


Fig 10. Histogram plots of : (a) Capsicum image, (b) text image (OPT); and (c, d) encrypted images of Capsicum and OPT, respectively.

4.3.5. Analysis of the effects of noise

The encrypted images during image processing and transmission stages are vulnerable to various types of noises. The impact of these noises can significantly affect the quality of the decrypted images. In our study, we consider Gaussian noise in the encoded image, which affects the ciphered images as discussed in [82-84]

$$\mu'(\rho, \sigma) = \mu(u, v) + kG \tag{18}$$

where $\mu(u, v)$ represents the encrypted picture and $\mu'(\rho, \sigma)$ denotes the noisy image with k as the noise factor/strenth, and G representing the Gaussian noise with a standard deviation of 0.02 within the range of 0 to 1. In Fig 11, the MSE plot demonstrates the impact of varying noise factors on the decrypted image, showing the noticeable effects of noise on the decrypted image at different noise factor levels.

5 Conclusion

Combining a TVPM mask with QRD within the gyrator transform domain is an innovative approach in designing an asymmetric cryptosystem. This combination enhances security and provides unique cryptographic properties to the system. Enhancing the security, confidentiality, and robustness of the QRD-based encryption technique stands as the primary objective of the proposed scheme. This emphasis aims at fortifying the encryption method against potential vulnerabilities and bolster its overall reliability. Primarily, its robustness is attributed to the incorporation of a secure and novel TVPM phase mask. This mask's complexity makes it challenging to replicate accurately without possessing precise information about all the parameters employed in its construction. Another notable feature is its speed. The encryption process can be swiftly executed digitally, and it also offers the capability of hybrid implementation.

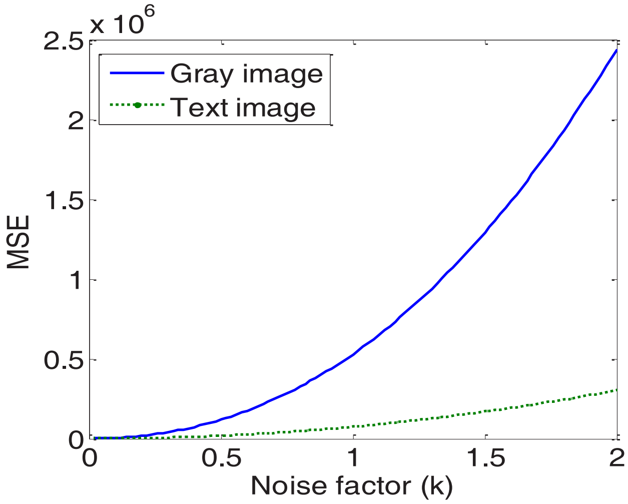


Fig 11. MSE graph illustrating the impact of varying noise factor (k) on OPT (text image) and Capsicum (gray image).

Another feature is its asymmetric nature. In this cryptosystem, the RPM and TVPM serve as public keys, while the specific decryption keys are derived through QRD during the encryption process. This generation of unique feature aids in thwarting known-plaintext attacks, enhancing the system's resistance against such intrusion attempts. An additional feature is the generation of a sparse cipher text matrix through partial pivoting. The scheme has undergone verification using various metrics such as Mean- Squared- Error (MSE) and Peak Signal-to-Noise Ratio (PSNR) to assess its effectiveness and robustness. The analysis indicates the scheme's capability to recover the original image even amidst distortions like occlusion. The scheme's key space is notably extensive, and simulation results affirm the robustness and efficiency of the proposed cryptosystem. The system described in the present paper has also been tested based on the Kirckoff's principle which states that the security of a cryptosystem resides in the key, even though the system architecture/algorithm is known to the hacker. It is found that our system passes the test.

6 Outlook for future

During the last 28 years or so, the subject of optical cryptography has grown into a major sub-area of the wider subject of optical information processing/ information optics. Though attempts have been made to develope 'all-optical' cryptosystems, in general the cryptosystems are still hybrid in nature i.e. some tasks performed by optical technology while others achieved by digital electronics-centred technology. A plethora of literature on the subject now exists, consisting of research publications, books, and conference proceedings. In this connection, Refs [84-89] may be noted.

Some of the systems that were considered as hitherto secure have been shown vulnerable to various types of attacks. The number of such vulnerable systems is on the increase due to the use of artificial intelligence tools such as deep learning. Another concern is the size of the existing table-top cryptosystems because of the use of bulk optical components and devices. As a result, the quest for new safer and lighter systems continues unabated. Three major trends seem to have emerged to combat these problems, namely the use of artificial intelligence tools, quantum science and technology, and metasurfaces. It is expected that the ultimate solution for building a safe cryptosystem would come from the recent initiatives in quantum science and technology, and nanophotonics including optical metamaterials for miniaturizing the systems, and artificial intelligence tools. All these trends are evident from the increasing emphasis on research and development in these areas [90-101]. Due to the restricted scope of the present paper, it is not possible to give an extended list of the relevant publications concerning the above mentioned hot areas.

References

1. Refregier P, Javidi B, Optical image encryption based on input plane and Fourier plane random encoding, *Opt Lett*, 20(1995)767–769.
2. Singh K, Unnikrishnan G, Nishchal N K, Photorefractive optical processing for data security, In, Photorefractive Fiber and Crystal Devices: Materials, Optical Properties, and Applications, VII, Proc SPIE 4803(2002)205–219.
3. Javidi B (ed), Optical and Digital Techniques for Information Security, (Springer New York USA), 2005.
4. Naughton T J, Sheridan J T, Optics in information systems, SPIE Int Techn Group News Lett, 16(2005)1–12.
5. Singh K, John R, Joseph *J.* Encrypted holographic memories for information security*, Bull Laser Spectrosc Soc* (*India*), 15(2005-6)1–19.
6. Matoba O, Nomura T, Perez-Cabre E, Millan M S, Javidi B, Optical techniques for information security, *Proc IEEE*, 97(2009)1128–1148.
7. Alfalou A, Brosseau C, Optical image compression and encryption methods, *Adv Opt Photon,* 1(2009)589–536.
8. Millan M S, Perez-Cabre E, Optical data encryption, In *Optical and Digital Image Processing: Fundamentals and Applications*, Cristobal G, Schelkens P, Thienpont H (eds), (Wiley N Y), 2011, pp 739–767. .
9. Kumar A, Singh M, Singh K, Speckle coding for optical and digital data security applications, In *Advances in Speckle Metrology and Related Techniques*, *(*ed) Kaufmann G, Chap 6, (Wiley-VCH Weinheim, Germany), 2011, pp 239–299.
10. Liu S, Guo C, Sheridan J T, A review of optical image encryption techniques, *Opt Laser Technol*, 57(2014)327–342.
11. Chen W, Javidi B, Chen X, Advances in optical security systems, *Adv Opt Photon*, 6(2014)120–155.
12. Yadav A K, Vashisth S, Singh H, Singh K, Optical cryptography and watermarking using some fractional canonical transforms and structured masks, in *Advances in Optical Science and Engineering*, (eds) Lakshminarayanan V, Bhattacharya I, Chap 5, pp 25–36, Springer Proceedings in Physics, 166 (Springer India), 2015.
13. Alfalou A, Situ G, Peng X, He W, Rastogi P, 3DIM-DS 2015: Optical image processing in the context of 3D imaging, metrology, and data security, *Opt Lasers Eng*, 89(2015)1–202 (Special issue).
14. Kumar P, Joseph J, Singh K, Double random phase encoding based optical encryption systems using some linear canonical transforms: weaknesses and countermeasures, In: Healy J, Alper Kutay M., Ozaktas H, Sheridan J (eds), *Linear Canonical Transforms.* Springer Series in Optical Sciences, 198, pp 367–396, (Springer New York), 2016.
15. Javidi B, Carnicer A, Yamaguchi M, Nomura T, Perez-Cabre E, Millan M S, Nishchal S K, Torroba R, Barrera J F, He W, Peng X, Stern A, Rivenson Y, Al Falou A, Brosseau, C, Guo C, Sheridan J T, Situ, G, Naruse M, Matsumoto T, Juvells I, Lancis J, Chen W, Chen X, Pinkse Prpijn, W H, Mosk A P, Markman A, Roadmap on optical security, *J Opt* (*IOP*), 18(2016)1–39.
16. Singh K, Photorefractive optical cryptography: a personal tour, In *Advances in Optical Science and Engineering*, Springer Proceedings in Physics194, (Eds) Bhattacharya I, Chakrabarti S, Reehal H S, Lakshminarayanan V, (Springer Nature Singapore Pvt Ltd), 2017.
17. Alfalou A (ed), Advanced Secure Optical Image Processing for Communications, (IOP Publ, Bristol, U K), 2018.
18. Nishchal N K, Optical Cryptosystems, (IOP Publishing, Bristol, UK), 2020.
19. Unnikrishnan G, Singh K, Double random fractional Fourier-domain encoding for optical security, *Opt Eng*, 39(2000)2853–2859.
20. Unnikrishnan G, Joseph J, Singh K, Optical encryption by double-random phase encoding in the fractional Fourier domain, *Opt Lett*, 25 (2000)887–889.
21. Hennelly B, Sheridan J T, Fractional Fourier trandform-based image encryption: phase retrieval algorithm, *Opt Commun*, 226(2003)61–80.

22. Joshi M, Shakher C, Singh K, Color image encryption and decryption using fractional Fourier transform, *Opt Commun*, 279(2007)35–42.
23. Lang J, Tao R, Wang Y, Image encryption based on the multiple-parameter discrete fractional Fourier transform and chaos function, *Opt Commun*, 283(2010)2092–2096.
24. Maan P, Singh H, Non-linear cryptosystem for image encryption using radial Hilbert mask in fractional Fourier transform domain, *3D Res*, 9(2018)53; doi.org/10.1007/s13319-018-0205-8.
25. Girija R, Singh H, A cryptosystem based on deterministic phase masks and fractional Fourier transform deploying singular value decomposition, *Opt Quant Electron*, 50(2018)210; doi.org/10.1007/s11082-018-1472-6.
26. Situ G, Zhang J, Double random-phase encoding in the Fresnel domain, *Opt Lett*, 49 (2004)1584–1586.
27. Shi Y, Situ G, Zhang J, Multiple image hiding in the Fresnel domain, *Opt Lett*, 32(2007)1914–1916.
28. Rajput S K, Nishchal N K, Fresnel domain nonlinear image encryption schems based Gerchberg-Saxton phase retrieval algorithm, *Appl Opt*, 53(2014)418–425.
29. Singh H, Yadav A K, Vashisth S, Singh K, Optical image encryption using devil's vortex toroidal lens in the Fresnel transform domain, *Int J Opt,* 2015(2015)926135; doi.org/10.1155/2015/926135.
30. Wang Z, Lv X, Wang H, Hou C, Gong Q, Qin Y, Hierarchical multiple binary image encryption based on a chaos and phase retrieval algorithm in the Fresnel domain, *Laser Phys Lett*,13(2016)036201; doi.10.1088/1612-2011/13/3/036201.
31. Singh H, Cryptosystem for securing image encryption using structured phase masks in Fresnel wavelet transform domain, *3D Res*, 7(2016); doi.org.10.1007/s13319-016-0110-y.
32. Zhou N R, Wang Y, Gong L, Novel optical image encryption scheme based on fractional Mellin transform, *Opt Commun*, 284(2011)3234–3242.
33. Vashisth S, Singh H, Yadav A K, Singh K, Devil's vortex phase structure as frequency plane mask for image encryption using the fractional Mellin transform, *Int J Opt,* 2014(2014)728056; doi.org/10.1155/2014/728056.
34. Vashisth S, Singh H, Yadav A K, Singh K, Image encryption using fractional Mellin transform, structured phase filters, and phase retrieval, *Optik*, 125(2014)5309–5315.
35. Singh H, Watermarking image encryption using deterministic phase mask and singular value decomposition in fractional Mellin transform domain, *IET Image Process,* 12(2018)1994–2001.
36. Rodrigo J A, Alieva T, Calvo M L, Gyrator transform: properties and applications, *Opt Express*, 15(2007)2190–2203.
37. Singh H, Yadav A K, Vashisth S, Singh K, Fully-phase image encryption using double random-structured phase masks in gyrator domain, *Appl Opt*, 53(2014)6472–6481.
38. Singh H, Yadav A K, Vashisth S, Singh K, Double phase-image encryption using gyrator transforms, and structured phase mask in the frequency plane, *Opt Lasers Eng*, 67(2015)145–156.
39. Singh H, Hybrid structured phase mask in frequency plane for optical double image encryption in gyrator transform domain, *J Mod Opt,* 65(2018)2065–2078.
40. Khurana M, Singh H, Asymmetric optical image triple masking encryption based on gyrator and Fresnel transforms to remove silhouette problem, *3D Res*, (2018); doi.org/10.1007/s13319-018-0190-y.
41. Khurana M, Singh H, A spiral-phase rear mounted *triple masking for secure optical image encryption based on gyrator transform, Recent Patents Comput Sci,* 12(2019)80–84.
42. Singh H, Devil's vortex Fresnel lens phase masks on an asymmetric cryptosystem based on phase-truncated in gyrator wavelet transform, *Opt Lasers Eng,* 81(2016)125–139.
43. Mehra I, Fatima A, Nishchal N K, Gyrator wavelet transform, *IET Image Process*. 12 (2017)432–437.
44. Anshula, Singh H, Ensuring security of cryptosystems with DVFM-, modified equal modulus decomposition in the domain of gyrator wavelet transform, *Multimed Tools Appl*, 82(2022)5965–5985.
45. Zhao D, Li X, Chen I, Optical image encryption with redefined fractional Hartley transform, *Opt Commun,* 281(2008) 5326–5329.
46. Li X, Zhao D, Optical color image encryption with redefined fractional Hartley transform, *Optik*, 121(2010)673–677.
47. Singh N, Sinha A, Optical image encryption using improper Hartley transform and chaos, *Optik* 121(2010)918–925.

48. Vilardy J M, Torres C O, Jimenez C J, Double image encryption method using the Arnold transform in the fractional Hartley domain, *SPIE Proc*, 8785(2013)87851R; doi.org/10.1117/12.2022216.
49. Liu Y, Du J, Fan J, Gong L, Single-channel color image encryption algorithm based on fractional Hartley transform and vector operation, *Multimed Tools Appl,* 74(2015)3171–3182.
50. Singh P, Yadav A K, Singh K, Phase image encryption in the fractional Hartley domain using Arnold transform and singular value decomposition, *Opt Lasers Eng*, 91(2017)187–195.
51. Yadav A K, Singh P, Singh K, Cryptosystem based on devil's vortex Fresnel lens in the fractional Hartley domain, *J Opt* (*Springer*), 47(2018)208–219.
52. Yadav A K, Singh P, Saini I, Singh K, Asymmetric encryption algorithm for clour images based on fractional Hartley transform, *J Mod Opt*, 66(2019)629–642.
53. Girija R, Singh H. Triple-level cryptosystem using deterministic masks and modified Gerchberg-Saxton iterative algorithm in fractional Hartley domain by positioning singular value decomposition, *Optik*, 187(2019)238–257.
54. Singh P, Yadav A K, Vashisth S, Singh K, Review of optical image encryption schemes based on fractional Hartley transform, *Asian J Phys,* 28(2019)701–716.
55. Carnicer A, Montes-Usategui M, Arcos S, Juvells I, Vulnerability to chosen-cypher text attacks of optical encryption schemes based on double random phase keys, *Opt Lett,* 30(2005)1644–1646.
56. Peng X, Chang P, Wei H, Yu B, Known-plaintext attack on optical encryption based on double random phase keys, *Opt Lett*, 31(2006)1044–1046.
57. Gopinathan G, Monaghan D S, Naughton T J, Sheridan T J. A known plain-text heuristic attack on the Fourier plane encryption algorithm, *Opt Express,* 14(2006)3181–3186.
58. Liu W, Yang G, Xie H, A hybrid heuristic algorithm to improve known-plaintext attack on Fourier plane encryption, *Opt Express*, 17(2009)13928–13938.
59. 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, *Opt Express*, 18(2010)13772–13781.
60. Peng X, Wei H, Zhang P, Chosen-plaintext attack on lens-less double-random phase encoding in the Fresnel domain, *Opt Lett*, 31(2006)3261–3263.
61. Zhang Y, Xiao D, Wen W, Liu H, Vulnerability to chosen-plaintext attack of a general optical encrypytion method with the architecture of scrambling-then-double random phase encoding, *Opt Lett*, 38(2013)4506–4509.
62. Qin W, Peng X, Asymmetric cryptosystem based on phase-truncated Fourier transform, *Opt Lett,* 35 (2010)118–120.
63. Cai J, Shen X, Lei M, Lin C, Dou S, Asymmetric optical cryptosystem based on coherent superposition and equal modulus decomposition, *Opt Lett*, 40(2015)475–478.
64. Abuturab M R, Single-channel color information security system using LU decomposition in gyrator transform domains, *Opt Commun*, 323(2014)100–109.
65. Xiong Y, Quan C, Hybrid attack free optical cryptosystem based on two random masks and lower upper decomposition with partial pivoting. *Opt Laser Technol*, 109(2019)456–464.
66. Anshula, Singh H, Security enrichment of an asymmetric optical image encryption-based devil's vortex Fresnel lens phase mask and lower upper decomposition with partial pivoting in gyrator transform domain, *Opt Quant Electron*, 53(2021)204; doi.org.10.1007/s11082-021-02854-7.
67. Anjana S, Yadav A K, Singh P, Singh H, Asymmetric double image encryption, compression, and watermarking scheme based on orthogonal-triangular decomposition with column pivoting, *Opt Applicata*, 52(2022)283–295.
68. Boukaram, W H, Turkiyyah G, Ltaief H, Keys D E, Batched QR and SCVD algorithms on GPUs with applications in hierarchical matrix compression, *Parallel Comput*, 74(2018)19–33.
69. Zhi X, Yan H, Fan J, Zheng X, Efficient discriminative clustering via QR decomposition-based linear analysis, *Knowl Based Syst*, 153(2018)117–132.
70. Su Q, Niu Y, Wang G, Jia S, Yue J, Color image blind watermarking scheme based on QR decomposition, *Sign Process,* 94(2014)219–235.
71. Abuturab M R, Multiple color-image authentication system using HIS color space and QR decomposition in gyrator domains, *J Mod Opt*, 63(2016)1035–1050.

72. Rakheja P, Vig R, Singh P, Double image encryption using 3D Lorenz chaotic system, 2D non-separable linear canonical transform and QR decomposition, *Opt Quant Electron,* 52(2020)103; doi.org.10.1007/s11082-020-2219-8.
73. Rakheja P, Singh P, Vig R, An asymmetric image encryption mechanism using QR decomposition in hybrid multi-resolution wavelet domain, *Opt Lasers Eng*. 134(2020)106177; doi.org/10.1016/j.optlaseng.2020.106177.
74. Anshula, Singh H, Cryptanalysis for double-image encryption using the DTLM in frequency plane with QR decomposition and gyrator transform, *Opt Rev*, 28(2021)596–610.
75. Anjana S, Yadav A K, Singh P, Singh H, Audio and image encryption scheme based on QR decomposition and random modulus decomposition in Fresnel domain, *Opt Applicata*, 52(2022)359–374.
76. Mehra I, Nishchal N K, Fingerprint image encryption using phase retrieval algorithm in gyrator wavelet transform domain using QR decomposition, *Opt Commun*, 533(2023)129265; doi.org/10.1016/j.optcom.2023.129265.
77. Golub G, Van Loan C, Matrix computation, (Johns Hopkins Univ Press), 2013.
78. Strang G, Linear algebra and its applications, 4th edn, (Thomson Learning Inc, USA), 2006.
79. Barrera J F, Henao R, Torroba R, Optical encryption method using toroidal zone plates, *Opt Commun*, 248(2005) 35–40.
80. Barrera J F, Henao R, Torroba R, Fault tolerances using toroidal zone plate encryption, *Opt Commun,* 256(2005)489–494.
81. Singh H, Tirth V, Singh R K, Algahtani A, Islam S, Designing of an optical vortices phase mask and used in the frequency domain of linear canonical transform for double image encryption, *Imaging Sci J*, 68(2022)288–304.
82. Yadav A K, Vashisth S, Singh H, Singh K, A phase-image watermarking scheme in gyrator domain using devil's vortex Fresnel lens as a phase mask, *Opt Commun*, 344 (2015)172–180.
83. Anshula, Singh H, Optical image encryption using various mathematical transforms and structure phase masks: A review, *Asian J Phys*, 28 (2020)825–856.
84. Singh H, Girija, R, Kumar M A, Cryptanalysis of elliptic curve cryptography based on phase truncation in the domain of hybrid gyrator Hartley transform. *Opt Quant Electron*, 55(2023)487; doi.org.10.1007/s11082-023-04765-1.
85. Sachin, Singh P, Singh K, Nonlinear image authentication algorithm based on double fractional Mellin domain, *Nonlinear Dyn*, 111(2023)13579–13600.
86. Mandapati V C, Vardhan H, Prabhakar S, Sakshi, Kumar R, Reddy S G, Singh R P, Singh K, Multi-user nonlinear optical cryptosystem based on polar decomposition and fractional vortex speckle patterns, *Photonics*, 10(2023)561; doi.org/10.3390/photonics10050561.
87. Girija R, Singh H., Singh K., An asymmetric cryptosystem using deterministic phase masks, double random phase encoding, orthogonal encoding and decoding, and fractional Fourier transform, *Asian J Phys*, 32(2023)385–397.
88. Abuturab M R, Multiple single-channel cryptosystem based on QZ decomposition, CMYK color space fusion and wavelength multiplexing, *Opt Quant Electron,* 56(2024)365; doi.org.10.1007/s11082-023-06001-2.
89. Gaur K S, Singh H, Thakran S, Singh K, An asymmetric hybrid cryptosystem based on triple random phase encoding using polar decomposition, QZ modulation, and gyrator domain, *Optik*, 299(2024)171602; doi.org/10.1016/j.ijleo.2023.171602.
90. Dai J-Y, Zhou N-R, Optical quantum image encryption algorithm with QPSO-BP neural neywork based pseudo random number generator, *Quant Inform Process*, 22(2023)318; doi.org/10.1007/s11128-023-04071-5.
91. Gong I, Choi S, Lukin MO, Quantum convolutional neural networks, *Nat Phys*, 15(2019)1273–1278.
92. Gong L-H, He X-T, Chang S, Hua T-X, Zhou N-R, Quantum image encryption algorithm based on quantum image XOR operations, *Int J Theort Phys*, 55(2016)3234–3250.
93. Fang X, Ren H, Gu M, Orbital angular momentum holography for high-security encryption, *Nature Photon*, 14 (2020)102–108.
94. Guo X, Li P, Zhong J, Wen D, Wei B, Liu S, Qi S, Zhao J, Stokes meta-hologram toward optical cryptography, *Nat Commun*, 13(2022)6687; doi.org/10.1038/s41467-022-34542-9.
95. Fan Z, Jia Y, Chen H, Qian C, Spatial multiplexing encryption with cascaded metasurfaces, *J Opt*(IOP), 25(2023)125105; doi.10.1088/2040-8986/ad0659.

96. Liu S, Wu D, Optical encryption in the photonic orbital angular momentum dimension via direct-laser-writing 3D chiral metahelices, *Nano Lett*, 23(2023)2304−2311.

97. Farmani A, Foladi H, Photonic and plasmonic encryption based on reflection-transmission reconfigurable digital coding metasurface in holographic images, *J Hogr Appl Phys*, 3(2023)63–81.

98. Zhang F, Guo Y, Pu M, Chen L, Xu M, Liao M, Li L, Li X, Ma X, Luo X, Meta-optics empowered vector visual cryptography for high security and rapid decryption, *Nature Commun*, 14(2023)1946; doi.org/10.1038/s41467-023-37510-z.

99. Zhou Q, Wang X, Jin M, Zhang L, Xu B, Optical image encryption based on two-channel detection and deep learning, *Opt Lasers Eng*,162(2023)107415; doi.org/10.1016/j.optlaseng.2022.10741.

100. Zhuang X, Yan A, Deep-learning based cipher-text only attack on optical scanning cryptosystem, *Opt Laser Technol*, 157(2023)108744; doi.org/10.1016/j.optlastec.2022.108744.

101. Xue J-d, Wang X-g, Zhou Q-m, Zhang L, Yao M, Deep-learning-assisted optical steganographic encryption via ghost encoding and binary hologram, *Opt Lasers Eng*, 172(2024); doi.org/10.1016/j.optlaseng.2023.107891.

[*Received*: 10.02.2024; *Revised recd*: 01.03.2024; *accepted*: 27.03.2024]

Dr Hukum Singh is currently Professor & Head Department of Applied Sciences, The NorthCap University, Gurugram, India. He obtained Ph D degree from G B Pant University of Agriculture and Technology, Pantnagar, India, in 2003. He has published 84 papers in reputed journals and as well presented 75 papers in national, international conferences and workshops. His name figure out in top 2% world's researcher by Standford University, Scopus data 2022.

Dr Singh has supervised 07 Ph D students and a number of students are working for their Ph D degree under his supervison. He is recipient of Prestigious Deokaran Award for "Glass"- 2018 by the Indian Ceramic Society, CSIR (CGCRI). Under best faculty award, Dr Singh was awarded best researcher award in the academic year 2021-22 by The NorthCap University, Gurugram, India. He is faculty adviser of The NorthCap University OPTICA student Chapter. He is Co-PI and Mentor of DRDO and DST research funded projects. He is senior member of The Optical Society (OPTICA), and The Optical Society of India (OSI). He is Associate Editor of IET Image Processing Journal and a Reviewer of Asian J Phys.

(Front Row: L to R): G S Pati (1st), Prof Kehar Singh (2nd), Prof Anna Consortini (4th), Kanwal Kamra (5th), during Winter College on Optics 1995, ICTP Trieste, Italy