Optica Applicata, Vol. LV, No. 3, 2025
DOI: 10.37190/oa/204262

Secure cryptographic scheme based on generalized Reed–Muller (GRM) codes and Laguerre–Gaussian vortex beams (LGVB) for optical image encryption in Fourier transform

Vipin Yadav[1], Seema Thakran[1], Hukum Singh[2,*]

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

[2] Department of Applied Sciences, School of Engineering, Tezpur University, Napaam, Tezpur, Assam, India

[*]Corresponding author: hukumsingh@tezu.ernet.in

In the era of modern technologies, developing effective crypt-coding systems is crucial when it comes to transmitting huge amounts of protected data quickly. Most encrypted image transmission systems do not sufficiently examine the effect of bit mistakes occurring during transmission. This problem is regarded as one that should be addressed by a competent coding scheme. In this paper, we have proposed an image encryption scheme based on generalized Reed–Muller (GRM) codes, QZ synthesis method, and Laguerre–Gaussian vortex beams (LGVB). In the proposed algorithm, GRM codes encode the image and add redundancy to it which increases its error-resistant quality. An encoded image is decomposed into two square images and each image is phase-encoded and modulated using random phase masks. The modulated image is then propagated through the Fourier domain. Vortex Fresnel array and the QZ decomposition operations are used to add security to generate the private keys. The proposed cryptosystem is robust against basic cryptographic attacks. The use of GRM codes adds on error correction capabilities in the cryptosystem. The correlation coefficient of the original and encrypted images is dropped to 0.3%, demonstrating the effectiveness of the encryption in randomizing the image data. System performance is tested by evaluating the mean-squared error, peak signal-to-noise ratio, structural similarity index measure and correlation coefficients.

Keywords: generalized Reed–Muller (GRM) codes, Laguerre–Gaussian vortex beams (LGVB), QZ decomposition, vortex Fresnel array, random phase mask, Reed–Muller (RM) codes.

1. Introduction

Error-correcting codes (ECCs) are employed in a variety of fields such as information and communication systems. Error-correcting code-based information encryption is a compelling concept for covert communication. Similar to information encryption, error-correcting codes alter the algebra structure of the information sequence to provide

parity bits. Therefore, converting an error correction code into an encryption system is convenient [1,2]. A primary picture is encoded using two random phase masks as part of a primary image encryption approach. The input plane and the spatial frequency plane are where the two masks are positioned. A stationary white noise is created as a result. During the decoding procedure, the encrypted image is first Fourier converted, then multiplied by the random phase mask's complex conjugate, and lastly, the Fourier inverse transform is implemented to decrypt the image. This is proposed by REFREGIER and JAVIDI [3].

To enhance the strength of DRPE-based encryption algorithms [4-7], various transforms have been implemented such as fractional Fourier transform [8], Fresnel transform [9-13], and gyrator transform [14]. WANG *et al*. [15] proposed an algorithm based on random modulus decomposition (RMD). In random modulus decomposition-based algorithms, two complex parts with equal moduli are separated from a picture; one portion is used as the cipher-text and the other as the private key. To increase the security of encryption, researchers later devised number of breakdown techniques, including polar decomposition and the QZ synthesis algorithms [16]. SHEN *et al*. [17] developed a new cryptosystem using DRPE and QZ modulation to enhance security against known plain-text attack (KPA) and chosen plain-text attack (CPA). Further, SHEN *et al*. [18] also suggested a QZ synthesis-based encryption that is practical and resistant to specialized attacks. Further, SINGH and YADAV [19] published a scheme based on an asymmetric multi-image wavelength multiplexing cryptosystem [20-22] using the QZ algorithm and unequal modulus decomposition [23]. In most of these cryptosystems, the security keys are the computationally generated RPMs. These methods are not robust enough against brute force attacks if one has access to high-performance computing resources. Due to the need for more secure picture data encryption methods, researchers developed the SPM to replace the RPM and improve security and key space. Fractional order vortex speckle (FOVS) patterns are used by MANDAPATI *et al*. [24].

In 1984, "a combined encryption and error correction", basically, encryption, decryption, encoding, and decoding, is introduced by a mix of cryptographic methods and error-correcting codes. After that number of researches has been done on error-correcting encryption algorithms. RAO and NAM [25] proposed a private-key algebraic-coded cryptosystem (PRAC) based on a public-key cryptosystem in 1986 incorporating basic algebraic Bose–Chaudhuri–Hocquenghem codes (BCH codes). The system, which concatenates error correction and encryption, is referred by them as joint encryption and error correction (JEEC). They supplemented this scheme PRAC against the attack with a syndrome-error table. In the same year, NIEDERREITER [26] developed a novel public-key cryptosystem, which he designated the N public key. However, in the interest of security, both of them forego the ability to remove errors. Research was going on in this field and in 2006, MATHUR *et al*. [27] raised the high diffusion cipher which is based on the substitution-permutation network (SPN) structure. Encryption and error correction are combined in this method, which diffuses the muddled message using high diffusion codes. In the event that one of the bytes is not rectified in the interference channel, the decryption will remain incorrect, resulting in an increased com-

plexity. An approach utilizing interleaved and low-density parity-check (LDPC) code was introduced in 2006 by Xiao *et al*. [28]. In 2010, Adamo *et al*. [29] proposed a scheme named error correction based cipher (ECBC) which combines encryption and error correction in one step. It effectively enhances the algorithm while preserving its complete error correction capability. It significantly slows down the process, and if one block is decoded incorrectly, consecutive blocks will be decoded incorrectly as well.

In 2013, Cankaya *et al*. [30] applied the linear error correction (LEC) code, permutation and compression to the cryptosystem. In 2014, Li *et al*. [31] presented a scheme used in satellite communications that incorporates advance encryption standard (AES) and LDPC. In 2015, Yao *et al*. [32] raised a JEEC scheme based on chaos and turbo code. The majority of them achieved this through straightforward error correction and cascading encryption. The level of efficiency was exceedingly low, and the security was obtained at the expense of error correction capability.

It is noticed that traditional encryption techniques like AES, RSA, and IDEA are observed to be applied to binary or text data. The high correlation among pixels makes the image encryption process highly difficult. Therefore, we proposed a novel secure optical cryptosystem based on double random phase encryption (DRPE) and generalized Reed–Muller (GRM) codes for improved security and error correction capability.

GRM codes are the generalized form of Reed–Muller codes introduced by Dass and Wasan [33] in 1983, named GRM codes of order $r + (\mathrm{r} + 1)_{m,s}$. In 2012, Tyagi and Rani [34] further extended their research on GRM codes of order $r + (\mathrm{r} + 1)_{m,s}$ and established new construction using multiples of GRM codes of order $r + (\mathrm{r} + 1)_{m,s}$. They also presented recursive methods of GRM and DGRM codes [35]. It was observed that researchers showed keen interest in GRM codes of order $r + (\mathrm{r} + 1)_{m,s}$ and studied structural and algebraic properties such as weight distributions, duality, and minimum weight codewords of these codes [36-38].

In this paper, we have focused on developing an image encryption technique based on GRM codes and QZ synthesis using vortex array (VA) in the Fourier domain. To the best of the author's knowledge, no study has been reported that contains error-correcting and detecting GRM codes, QZ decomposition, and vortex array based encryption scheme. GRM codes are used to encode the image so that it can correct the errors that occurred in the encryption process. Further, the encoded image is decomposed into two equal parts and each part is encrypted separately. The QZ synthesis method is applied in the encryption process to combine two encrypted images which provides a security key. Vortex arrays are used with random phase mask to add more security in the system as it is generated from Laguerre–Gaussian beams and possess a unique pattern and not possible to clone as one cannot identify the physical process. The rest of the paper is organized as follows. In Section 2, the theoretical explanations, results of GRM codes, QZ decomposition, the Fourier transform, Laguerre–Gaussian vortex beams and mathematical formulation of vortex array are presented. In Section 3, we have provided a detailed explanation of the proposed cryptosystem. The numerical simulations in support of the proposed scheme are discussed in Section 4. Lastly, the conclusion is given in Section 5.

2. Theoretical background

In this section, GRM codes, QZ decomposition, generation of vortex array from Gaussian beams are discussed in detail.

2.1. Reed–Muller (RM) codes

In RM codes, a block of k bits of data is encoded into n bits of data (codeword) where $n > k$ for data transmission (see Fig. 1).

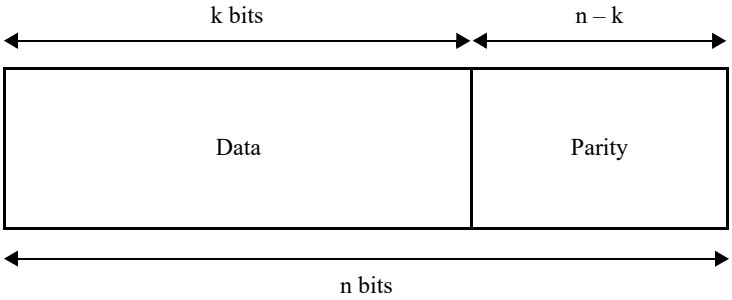

Fig. 1. RM codeword of length n and k is the number of input symbols.

Definition: Let m and r be the integers with $0 \le r \le m$, RM(r, m) codes of order r have the following parameters:

Block length: $n = 2^m$

Dimension: $k = 1 + \binom{m}{0} + \binom{m}{1} + \binom{m}{2} + ... + \binom{m}{r}$

Minimum distance: $d_{\min} = 2^{m-r}$

Here, n is the size of the codeword; k is the size of the message; $d_{\min}$ is the hamming distance which defines the error-correcting capability of the RM codes.

2.2. Generalized Reed–Muller codes of order $r + (r + 1)_{m,s}$

In 1983, DASS and WASAN, obtained a new class of generalized Reed–Muller codes, now known as GRM codes of order $r + (r + 1)_{m,s}$ by extending/shortening a r-th order of RM codes [33].

Definition: A GRM code of order $r + (r + 1)_{m,s}$ is generated by basis vectors $\{v_0, v_1, v_2, ..., v_m\}$ and vectors product of $\{v_0, v_1, v_2, ..., v_m\}$ taken r or fewer at a time along with some s vector products $\left(1 \le s < \binom{m}{r+1}\right)$ of these vectors taken $(r + 1)$ at a time.

Parameters of GRM codes are as follows:

Code length: $n = 2^m$;

Dimension: $k = 1 + \binom{m}{0} + \binom{m}{1} + \binom{m}{2} + ... + \binom{m}{r} + s$, where $1 \le s < \binom{m}{r+1}$;

Minimum distance: $d_{\min} = 2^{m-r-1}$.

Let $\mathbf{x} = (x_0, x_1, ..., x_{n-1})$ and $\mathbf{y} = (y_0, y_1, ..., y_{n-1})$ be two binary tuples. We define the following logic (Boolean product) of **x** and **y**:

$$\mathbf{x} \cdot \mathbf{y} = (x_0 \cdot y_0, x_1 \cdot y_1, ..., x_{n-1} \cdot y_{n-1}) \tag{1}$$

where '·' denotes the logic product, *i.e.*,

$$\begin{cases} x_i \cdot y_i = 1 & \text{if} \quad x_i = y_i = 1 \\ x_i \cdot y_i = 0 & \text{if} \quad x_i = 0 \quad \text{or} \quad y_i = 0 \end{cases} \tag{2}$$

2.3. GRM encoder/generator matrix

$\mathbf{G}(r, m)$ denotes the generator matrix of an RM(r, m) code, then the generator matrix $\mathbf{G}(r, m, s)$ of a GRM code of order $r + (r + 1)_{m,s}$ is written as,

$$\mathbf{G}(r, m, s) = \begin{pmatrix} \mathbf{G}(r, m) \\ \mathbf{X} \end{pmatrix} \tag{3}$$

where $\mathbf{G}(r, m)$ is generator of an RM(r, m) code and **X** is a matrix containing some s vector products of $v_0, v_1, v_2, ..., v_m$ taken $(r + 1)$ at a time.

Example: Let $m = 4$ and $r = 1$ and $s = 1$, the generator matrix of GRM code of order $1 + (2)_{4,1}$ is given by

$$\mathbf{G}(1, 4, 1) = \left(\begin{array}{c|c} v_0 & 1111111111111111 \\ v_4 & 0000000011111111 \\ v_3 & 0000111100001111 \\ v_2 & 0011001100110011 \\ v_1 & 0101010101010101 \\ v_1 v_2 & 0001000100010001 \end{array}\right) \tag{4}$$

2.4. Generation of vortex Fresnel array (VFA)

The optical vortex phase mask is used in the suggested approach to expand the key space and improve security. Given that they have their own centre masks, these masks are useful for positioning during decoding. Their security is enhanced by the fact that they are diffractive optical elements (DOEs), which are extremely difficult to replicate. Furthermore, these masks have several essential characteristics in one, which adds to the security criteria. In spiral waves with angular momentum, optical vortices (OV) are especially important. They are used in astronomy, bio-photonics, quantum computing, encryption, and the creation of vortex lens or phase mask systems, among other fields. The azimuthal phase dependence of optical vortices is $\exp(il\theta)$. The wave's

phase change over one full rotation around the vortex point is represented by the topological charge (TC), represented by l. This charge can be either an integer or a fraction.

2.5. Laguerre–Gaussian (LG) beam

Light beams with Laguerre–Gaussian (LG) intensity distributions and helical phase profiles are categorized as structured light beams. The beam profile is defined using a quantized parameter known as the mode number, which can take values extending to infinity. LG modes are also linked to optical vortices; when light with a helical wave-

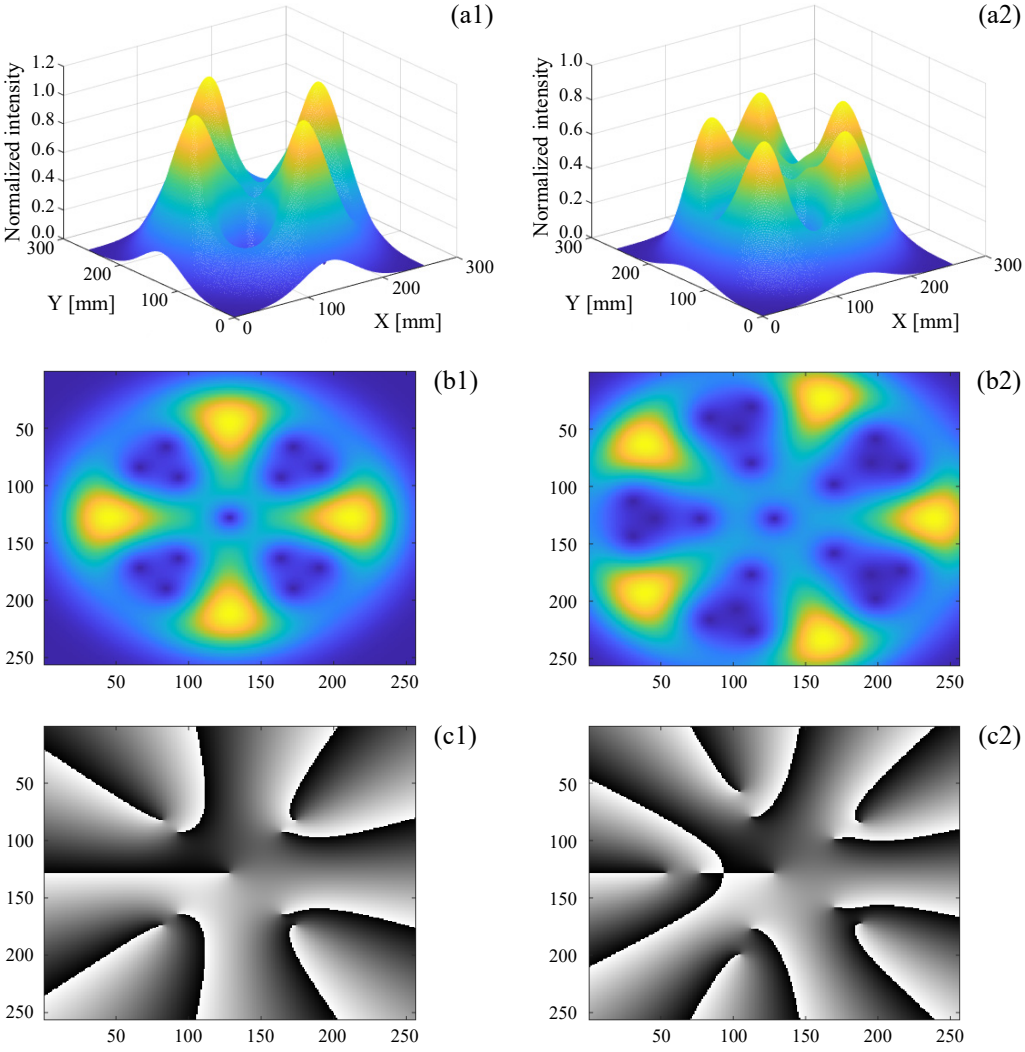

Fig. 2. Generation of the optical vortex arrays. (a1, a2) 3D, (b1, b2) 2D and (c1, c2) phase maps of the optical vortex array generated by the vortex beams with $l_n = l_1 + \Delta l$, $l_1 = 1$, $\Delta l = 4$ and 5.

front propagates in a corkscrew-like manner, an optical vortex is formed. The electric field amplitude of an LG mode, which propagates along the z-direction, can be represented as a coherent superposition of vortex beams [39]. For the LG beam in cylindrical coordinates, the light field is expressed as [40]

$$E(r, \varphi, z) = \sqrt{\frac{1}{\omega^2(z)}} \sqrt{\frac{2p!}{\pi(p+|l|)!}} \exp\left[-\frac{r^2}{\omega^2(z)}\right]\left[\frac{2r^2}{\omega^2(z)}\right]^{|l/2|} \exp(i l_n \varphi) \exp(ikz) \tag{5}$$

where p is the radial index, l_n is the topological charge, $\omega(z)$ is the spot size at a distance z, φ is the azimuth angle, $k = 2\pi/\lambda$ is wave number.

If $p = 0$, the coherent superposition of vortex beams can be expressed as

$$E(r, \varphi, z) = \sum_{n=1}^{N} A(r) B(r, l_n) \exp(i l_n \varphi) \tag{6}$$

where N denotes the number of OAM nodes and the value of topological charge l_n arithmetic sequence,

$$A(r) = \frac{\sqrt{2/\pi}}{w(z)} \exp\left(\frac{-r^2}{w^2(z)}\right) \tag{7}$$

$$B(r, l_n) = \sqrt{\frac{1}{l_n!}} \left(\frac{r\sqrt{2}}{w(z)}\right)^{l_n} \tag{8}$$

Figure 2 shows the example of the optical vortex array with sub-beams $N = 4$ and $N = 5$, and $l_n = l_1 + \Delta l$. Figure 2(a1)–(c1) shows the 3D, 2D maps and the phase diagram of the optical vortex array, which consists of four sub-beams, where $l_1 = 1$ and $\Delta l = 4$. Figure 2(a2)–(c2) shows the 3D, 2D maps and the phase diagram of the optical vortex array, which consists of five sub-beams, where $l_1 = 1$ and $\Delta l = 5$.

2.6. Fresnel zone plate (FZP)

A Fresnel zone plate (FZP) function is mathematically written as,

$$\text{FZP} = \exp\left[-i\frac{\pi(x^2 + y^2)}{\lambda f}\right] \tag{9}$$

where λ and f are respectively the wavelength and focal length, and x and y are the coordinates on X and Y axis of the Fresnel zone plate.

2.7. VFA phase key

A VFA phase key is obtained by combining Eq. (6) and (8) as follows,

$$E(r, \varphi) \cdot \mathrm{FZP} = \sum_{n=1}^{N} A(r) B(r, l_n) \exp(i l_n \varphi) \exp\left(-\frac{\pi r^2}{\lambda f}\right) \tag{10}$$

$$\mathrm{VFA}_{l_n, \lambda, f} = \sum_{n=1}^{N} A(r) B(r, l_n) \exp\left[i l_n \varphi + \left(-\frac{\pi r^2}{\lambda f}\right)\right] \tag{11}$$

Figure 3 shows the construction of VFA key using Fresnel zone plate (a) and phase value of optical vortex array (b) [41,42] for $N = 4$. A new VFA phase key is produced as shown in Fig. 3(c).

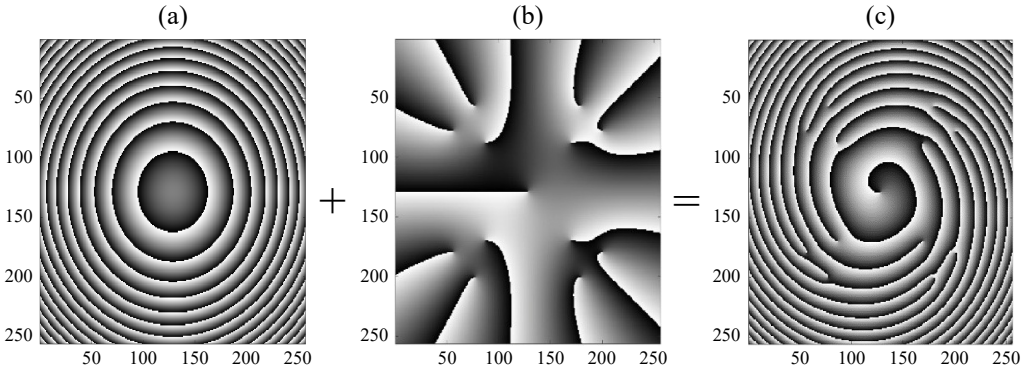

Fig. 3. Generation of the VFA key using (a) + (b) = (c), using FZP with values λ = 632.8 nm, f = 500 mm and phase maps of the optical vortex array generated by the vortex beams with $N = 4$.

2.8. QZ decomposition

In this decomposition method, two square matrices say, **A** and **B** are decomposed in two upper quasi triangular matrices (**AA**, **BB**) and two unitary matrices (**Q**, **Z**). Mathematically, [**AA**, **BB**, **Q**, **Z**] = **QZ**(**A**, **B**). Taking the transpose of **BB** and extracting the diagonal elements from it, which act as private in proposed system. The result is stored as $\mathbf{BB}_1$ which is lower triangular matrix:

$$\mathbf{BB}_1 = \mathrm{transpose}(\mathbf{BB}) - \mathrm{diag}(\mathbf{BB}) \tag{12}$$

Then, both upper triangular matrix **AA** and lower triangular matrix $\mathbf{BB}_1$ are combined to get the synthesis matrix, say **M**. The synthesis method is shown in Fig. 4.

In the inverse QZ synthesis method, **AA** can be extracted as a upper triangular matrix from **M**

$$\mathbf{AA} = \mathrm{triau}(\mathbf{M}) \tag{13}$$

Then, **BB** can be calculated using the following mathematical operations:

$$\mathbf{BB} = \mathrm{transpose}(\mathbf{M} - \mathbf{AA}) + \mathrm{diag}(\mathbf{BB}) \tag{14}$$

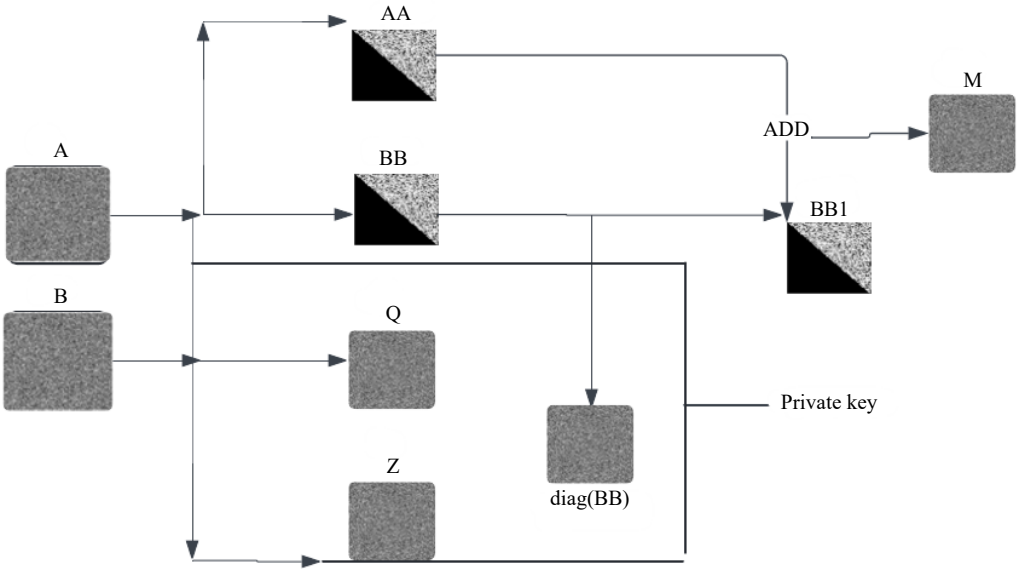

Fig. 4. Flowchart of QZ synthesis method.

To retrieve **A** and **B**, we use private keys Q and Q with the following calculations

$$\mathbf{A} = Q^{-1} * \mathbf{AA} * Z^{-1} \tag{15}$$

$$\mathbf{B} = Q^{-1} * \mathbf{BB} * Z^{-1} \tag{16}$$

3. Proposed cryptosystem

3.1. Encryption process

The following steps are performed for the encryption (see Fig. 5).

Step 1. A binary image $I(x, y)$ is encoded using GRM codes, mathematically, $I(x, y)$ is multiplied with GRM codes matrix. Without loss generality, image I is considered of 256×256 pixels. GRM code matrix 256×512 is used for encoding. Output encoded image is decomposed in two equal size image of size 256×256 and named as E_1 and E_1'. Mathematically, $[E_1 \; E_1'] = \text{GRM} \times I(x, y)$.

Step 2. Create two different random phase masks

$$\text{RPM1} = \exp\left[2\pi i(m_1, n_1)\right] \tag{17}$$

$$\text{RPM2} = \exp\left[2\pi i(m_2, n_2)\right] \tag{18}$$

where (m_i, n_i), $i = 1, 2$ are random matrix of size 256×256 pixels. The random phase masks RPM1 and RPM2 are mapped on E_1 and E_1', respectively. Both outputs are sub-

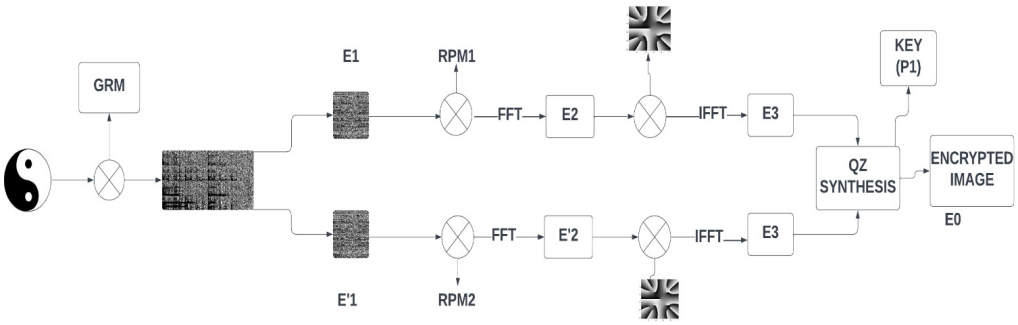

Fig. 5. Flowchart of encryption process.

jected to Fourier transform and stored as E_2 and E_2', respectively. Mathematically, the output is shown as

$$E_2 = \mathrm{FFT}(E_1 \cdot \mathrm{RPM1}) \tag{19}$$

$$E_2' = \mathrm{FFT}(E_1' \cdot \mathrm{RPM1}) \tag{20}$$

Step 3. The outputs of Step 2 are processed through vortex array (VA) and both outputs are subjected to Fourier transform and results are stored in E_3 and E_3'. Mathematically, this step is described as

$$E_3 = \mathrm{IFFT}(E_2 \cdot \mathrm{VA}) \tag{21}$$

$$E_3' = \mathrm{IFFT}(E_2' \cdot \mathrm{VA}) \tag{22}$$

Step 4. QZ synthesis method is applied on E_3 and E_3' to obtain a combined ciphertext E_0. Mathematically, it is described as

$$[\mathbf{AA}, \mathbf{BB}, Q, Z] = \mathrm{QZ}(E_3, E_3') \tag{23}$$

3.2. Decryption process

Step 1. The inverse QZ synthesis method is applied on ciphertext E_0, and the output is propagated through the inverse Fourier lens. Mathematically, it can be written as,

$$[D_3, D_3'] = \mathrm{InvQZ}(E_0) \tag{24}$$

Step 2. The output of Step 1 is propagated through the Fourier domain and phase key of vortex array is applied, the result is stored as D_2 and D_2':

$$D_2 = \mathrm{IFFT}\left[\mathrm{inv}(\mathrm{VA}) \cdot \mathrm{FFT}(D_3)\right] \tag{25}$$

$$D_2' = \mathrm{IFFT}\left[\mathrm{inv}(\mathrm{VA}) \cdot \mathrm{FFT}(D_3')\right] \tag{26}$$

Step 3. The output of Step 2 is bonded with the conjugate of RPM1 and RPM2 and stored as D_1 and D_1':

$$D_1 = \text{conj}(\text{RPM1}) \cdot D_2 \tag{27}$$

$$D_1' = \text{conj}(\text{RPM2}) \cdot D_2' \tag{28}$$

Step 4. In the last step, D_1 and D_1' are concatenated and error is extracted using decoding algorithm of GRM codes and the original image is retrieved.

$$I(x, y) = \text{decode}([D_1 \; D_1']) \tag{29}$$

The schematic representation of the decryption process is presented in Fig. 6.

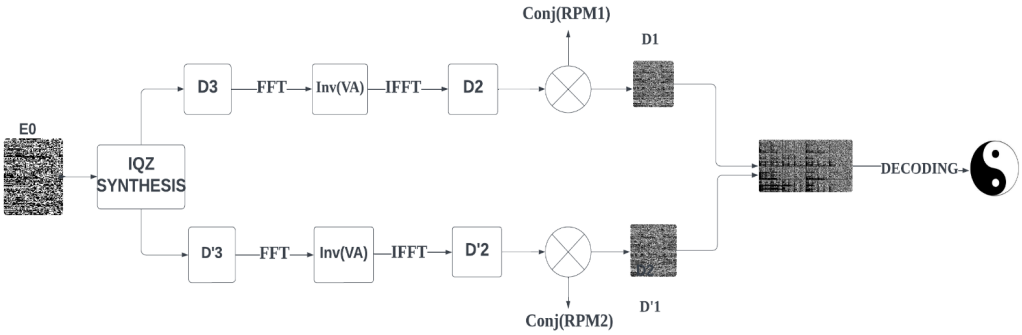

Fig. 6. Flowchart of decryption process.

4. Results and discussion

The proposed cryptosystem performance was evaluated using a personal computer configured with processor 11th Gen Intel(R) Core (TM) i3-1115G4 @ 3.00GHz 2.90GHz, 8GB RAM, operating Windows 11, operating system 64-bit and running MATLAB 2024.

In the proposed method, a binary image is used of size 256×256 pixels. Encryption and decryption results are shown in Fig. 7.

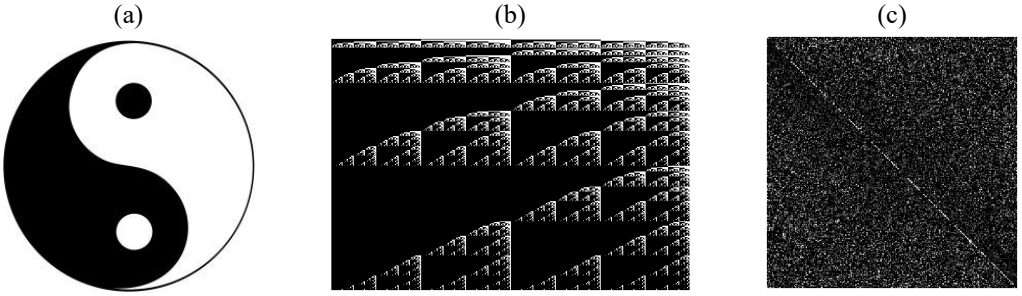

Fig. 7. Validation results of the proposed encryption algorithm. (a) Input image, (b) GRM code image, and (c) ciphertext.

4.1. Performance analysis

The suggested encrypted algorithm's performance was thoroughly assessed using several number of simulations. The evaluation concentrated on a number of important aspects to measure the algorithm's performance and applicability in real-world situations.

4.1.1. Mean squared error (MSE)

A popular statistic for assessing performance and estimating the errors of both encrypted and decrypted pictures is the MSE. A lower MSE value indicates higher image quality and data preservation since it denotes a high value of similarity between the original and decrypted images. The following formula or equation is used to calculate MSE:

$$\text{MSE} = \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{i=1}^{M} \left[I(x, y) - d(x, y) \right]^2 \tag{30}$$

The MSEs value in the proposed scheme is 1.8×10^{-2}.

4.1.2. Peak signal-to-noise ratio (PSNR)

The quality of encoded and decoded images is assessed using a performance metric called the peak signal-to-noise ratio (PSNR). It determines how much noise or distortion is introduced during the encryption, decryption, or transmission processes in relation to the maximum possible power of the signal or input image. A higher PSNR value denotes less distortion.

Using a logarithmic scale, the mean squared error (MSE) between the original and reconstructed image is computed to determine PSNR.

$$\text{PSNR} = 10 \log \frac{\text{MAX}^2}{\text{MSE}} \tag{31}$$

The maximum pixel intensity value, or MAX, in this case is 255 for an 8-bit image. The standard unit of measurement for PSNR is decibels (dB). Interestingly, the rebuilt images with the original binary image have 261.1 dB PSNR value.

4.1.3. Structural similarity index measure (SSIM)

SSIM is used to evaluate the picture quality by comparing a recovered image with the input image. An SSIM value of 1 indicates the recovery of a high-quality image. SSIM could have a value anywhere from –1 to 1. The similarity is calculated using the following formula:

$$\text{SSIM}(I, I') = \frac{(2\mu_I \mu_{I'} + c_1)(2\sigma_{I,I'} + c_2)}{(\mu_I^2 + \mu_{I'}^2 + c_1)(\sigma_I^2 + \sigma_{I'}^2 + c_2)} \tag{32}$$

where μ_I and $\mu_{I'}$ denote the pixel sample mean of image I and I', respectively; σ_I^2 and $\sigma_{I'}^2$ are the variance of I and I', respectively; $\sigma_{I,I'}$ is cross-correlation of I and I'. The variables c_1 and c_2 stabilize the division with weak denominator.

4.2. Statistical analysis

The 3D plot, entropy analysis and correlation between the input image and encryption image is discussed in this section.

4.2.1. 3D plot analysis

3D plot of encrypted images reflects the security of the cryptosystem. In this scheme, we have encrypted two different images and could not find the difference between the encrypted images of both input images. We can see the similarity between the encrypted images in Fig. 8, which suggest that we cannot predict the input images by just checking the structure plot of encrypted images. *Lena* image and binary *Logo* image are encrypted and their 3D plot are shown in Fig. 8.

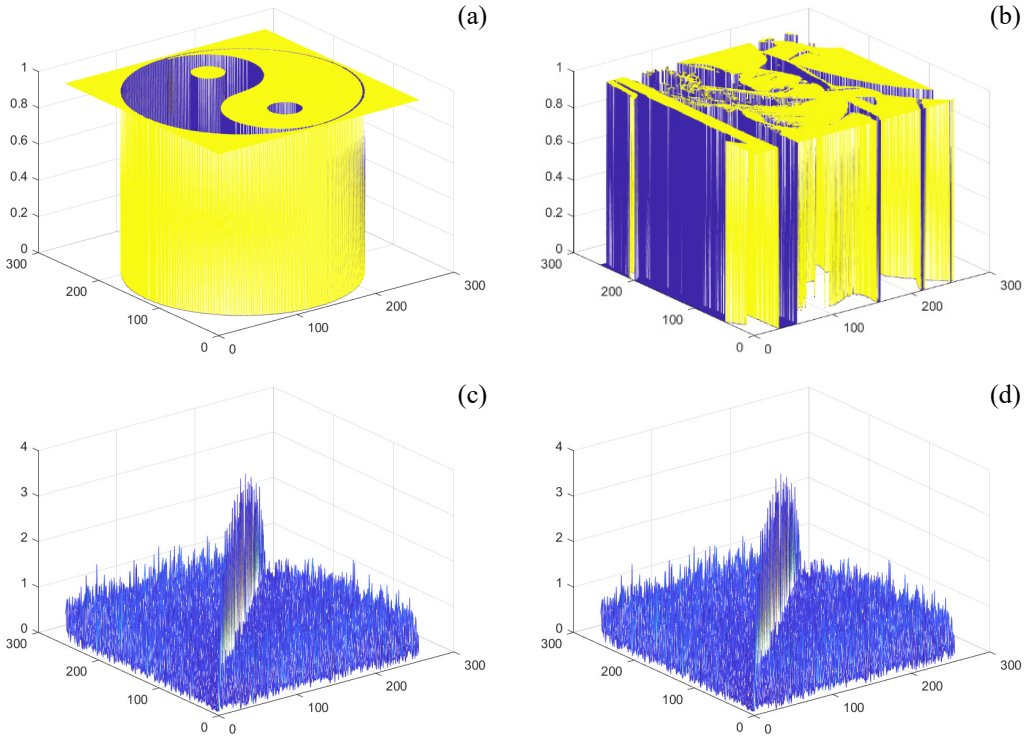

Fig. 8. (a) 3D plot of *Logo* binary image, (b) *Lena* image plot, (c) 3D plot of encrypted *Logo* image, and (d) 3D plot of encrypted *Lena* image.

4.2.2. Correlation distribution analysis

The CC value is predominantly found within the interval [–1, 1], with values approaching 1 signifying a robust positive linear correlation and implying a considerable level of resemblance between input and decrypted images. A value in proximity to –1, conversely, denotes a strong inverse correlation between pixel intensities, signifying a negative relationship. A value in the vicinity of zero indicates a tenuous or non-existent

T a b l e 1. The correlation of adjacent pixels.

Correlation of adjacent	Before encryption	After encryption
Horizontal pixels	0.9435	–0.0073
Vertical pixels	0.9438	0.0052

linear correlation, implying that the two sets of data points are dissimilar. The value of CC between input and decoded images for the proposed scheme is shown in Table 1.

In contrast to decrypted images, which bear a striking resemblance to the original input images, cipher images have an arbitrary pixel distribution and have no correlation with the input images that were captured. The efficacy and resilience of the suggested methodology in safeguarding image integrity and ensuring confidential communications were further validated by these outcomes.

4.3. Error correction analysis

We discuss about the error correction capabilities of GRM codes in the DRPE cryptosystem.

4.3.1. GRM code error correcting capabilities

We used GRM codes constructed by shortening the *r*-th Reed–Muller codes. The Hamming weight of the GRM code is $d_{\min} = 2^{m-r}$. In our scheme, we used $m = 9$, $r = 4$, and $s = 0$ generates GRM encoder matrix of order 256×512. Weight of the code is

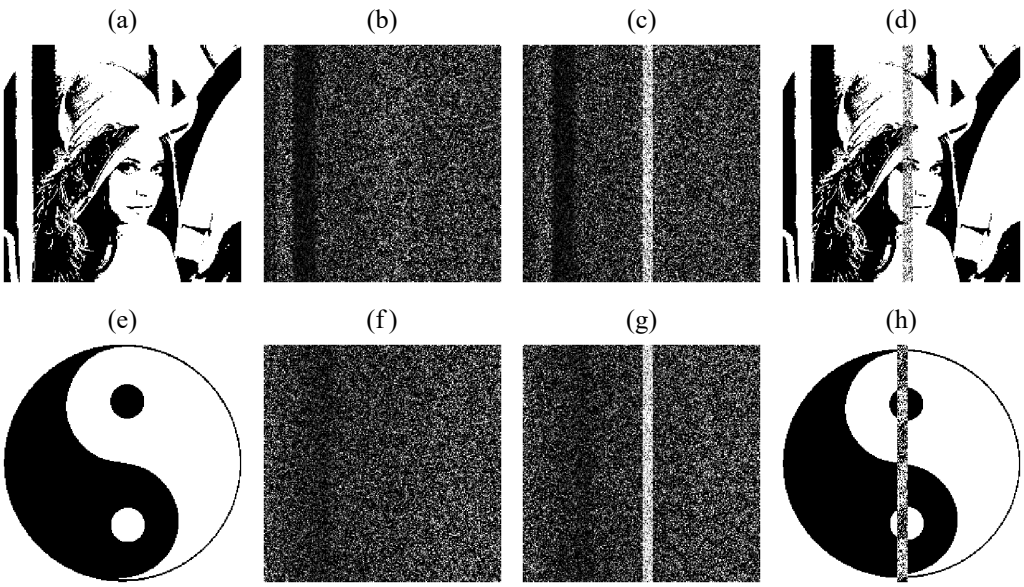

Fig. 9. (a, e) Input binary image of *Lena* and *Logo*, (b, d) the corresponding cipher image, (c, e) the error added vertically in some part of the encryption image, and (d, f) error reflects in the decryption image.

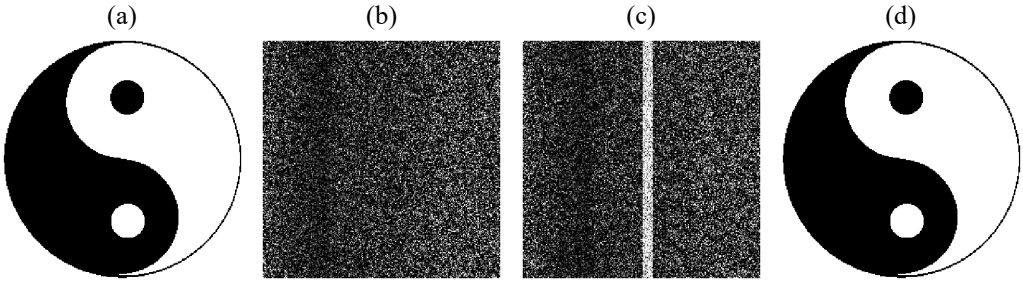

Fig. 10. (a) Input binary image of *Logo*, (b) the corresponding cipher image, (c) the error added vertically in some part of the encryption image, and (d) error-free in decryption image.

$2^{9-4} = 32$ which can correct up to 15 errors. GRM codes is implemented along row-wise over the input image matrix:

- Input data: 256×256 binary matrix,
- GRM code: 256×512 binary matrix,
- Encoded data: 256×512 matrix,
- Error added: 256×512 matrix contains maximum 15 ones in every row.

In DRPE encryption scheme, an error can be occurred either caused by attacks or channel disturbance. Here, we compare the DRPE scheme of encryption with or without using the GRM codes.

4.3.2. DRPE encryption without using GRM codes

The encryption process of two different input images (*Lena* and *Logo*) is shown in Fig. 9.

4.3.3. Encryption using GRM codes

In the proposed scheme error correcting GRM codes are used to correct error. Figure 10 represents the components in the encryption process. It can be seen that the errors are removed using the codes and the decrypted image is retrieved as original image.

4.4. Robustness analysis

A system is secured and robust if it is resistant to attacks. The proposed cryptosystem is tested against contamination attacks and classical cryptographic attacks (CPA, QPA) and found to be robust.

4.4.1. Contamination attack analysis

The scheme is highly secured and has been tested against noise contamination attack. To verify this, we have done the analysis on noise attack with Gaussian noise. The encrypted image after adding the noise is as follows:

$$E_0' = E_0(1 + kG) \tag{33}$$

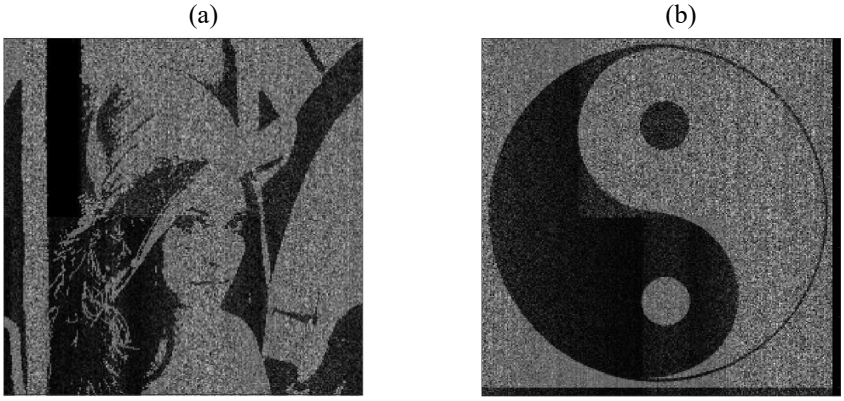

Fig. 11. Decrypted image recovered from noise contaminated image with values of (a) $k = 0.3$, and (b) $k = 0.5$.

where E_0' and E_0 are contaminated encrypted image and encrypted image, respectively, G denotes the Gaussian random noise with zero mean and 1 variance, and k denotes the coefficient of strength of the noise. In our analysis, encrypted image is contaminated with values of $k = 0.3$ and 0.5, the corresponding decrypted image is shown in Fig. 11.

4.4.2. Plaintext attacks

In the proposed cryptosystem, we have checked the robustness of our scheme against plaintext attacks, *i.e.*, known-plaintext attacks (KPA) and chosen plaintext attacks (CPA). In KPA, if an attacker has information about a pair of plain-text and the corresponding ciphertext, then they may try to obtain the secret key using this information. In CPA, the attacker already has the information about the encryption process and he tries to implement the encryption process to obtain the secret keys. In both the attacks, the attacker can obtain the decryption keys and can apply these keys on other ciphertext. It might happen that an attacker is able to get the original image. Due to the fact,

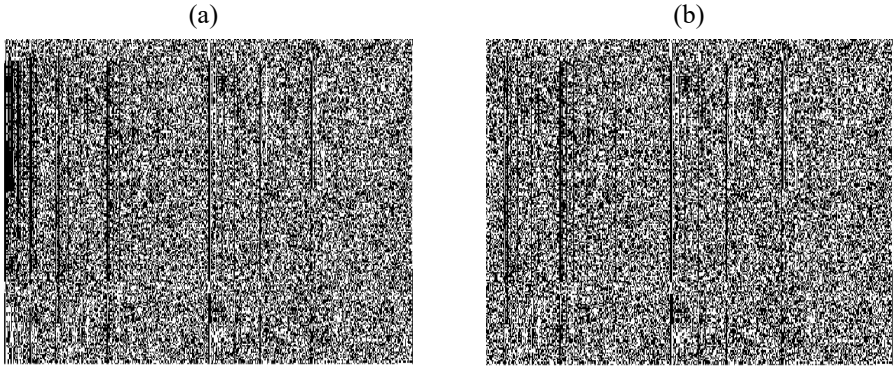

Fig. 12. Decipher image of (a) *Lena* and (b) *Logo* retrieved by their exchanged private keys.

that our scheme is asymmetric, which means the private keys will change with each input image. As a result, CPA and KPA are ineffective. To check the robustness against these attacks, encrypted image of *Lena* and *Logo* is deciphered with wrong (exchanged) private keys. The results are shown in Fig. 12, which proves the robustness of the scheme against the aforementioned attacks.

4.4.3. Comparison results

In Table 2, comparison is discussed with proposed and existing schemes.

T a b l e 2. Comparison of proposed scheme with other existing schemes.

Parameters	KONYAR *et al*. [43]	SINGH [10]	Proposed scheme
Mathematical transformation	–	LCT, GT	FT, IFT
MSE	0.842	3.09×10^{-28}	1.8×10^{-28}
Parameters	RS code, data hiding algorithm	VFA, DRPE	GRM code, DRPE, VFA
Strength	Prone to KPA, CPA	Prone to deep learning	Prone to deep learning
Error correction code	Reed–Solomon code	–	GRM code
PSNR	48 dB	296 dB	261 dB

5. Conclusion

In this paper, we have introduced an image encryption and error correction algorithm that utilizes the GRM codes and QZ synthesis method with a vortex array in the Fourier domain. The original image is more difficult for unauthorized users to recover when vortex array is used. We have improved the security encryption technique by using the QZ synthesis approach. Binary pictures are used for the validation of the suggested encryption technique. The scheme is tested against basic attacks chosen plain-text attacks (CPA) and known plain-text attacks (KPA). The comparison of the scheme with existing schemes showed that the proposed scheme is highly efficient and secure. The suggested encryption algorithm's performance is assessed using several numbers of statistical metrics, such as the correlation coefficient and information entropy. To retrieve the original image, all of the encryption keys are required. According to experimental results, our technology can fix big, corrupted blocks in photos, something that other previously published methods have not been able to do.

Author contributions
Hukum Singh: review, drafting, software analysis. Vipin Yadav: writting, research, mathematical analysis, draft preparation. Seema Thakran: supervision, review, coding analysis.

Data availability
On request, the corresponding author will provide the supporting documentation for the findings reported in this study. During the current investigation, no datasets were created or examined.

Conflict of interest
The authors claim that publishing this research does not present any conflicts of interest. They have no conflicting interests.

Acknowledgement
The authors gratefully acknowledge the funding from the Anusandhan National Research Foundation (ANRF), Science & Engineering Research Board (SERB), Core Research Grant (CRG) scheme, Govt. of India, Grant No. CRG/2023/005504-G.

References

[1] KAMBLE A.J., VENKATESH T., *Some applications of error-correcting codes*, Journal of Computer and Mathematical Sciences **6**(11), 2015: 604-611.
[2] PADMAJA M., SHAMEEM S., *Secure image transmission over wireless channels*, [In] *International Conference on Computational Intelligence and Multimedia Applications (ICCIMA 2007)*, Sivakasi, India, 2007: 44-48. https://doi.org/10.1109/ICCIMA.2007.38
[3] 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
[4] YADAV A.K., VASHISTH S., SINGH H., SINGH K., *Optical cryptography and watermarking using some fractional canonical transforms, and structured masks*, [In] Lakshminarayanan V., Bhattacharya I. [Eds.], *Advances in Optical Science and Engineering*, Springer Proceedings in Physics, Vol. 166, Springer, New Delhi, 2015: 25-36. https://doi.org/10.1007/978-81-322-2367-2_5
[5] YADAV P.L., SINGH H., *Security enrichment of optical image cryptosystem based on superposition technique using fractional Hartley and gyrator transform domains deploying equal modulus decomposition*, Optical and Quantum Electronics **51**, 2019: 140. https://doi.org/10.1007/s11082-019-1854-4
[6] BANSAL A., RAKHEJA P., SINGH H., *Double iris image asymmetric encryption mechanism using rear mounted spiral phase mask in hybrid transform domain*, Optical and Quantum Electronics **56**, 2024: 782. https://doi.org/10.1007/s11082-024-06599-x
[7] SINGH H., *Cryptanalysis of a double-image symmetric optical cryptosystem utilizing devil's vortex Fresnel array and the linear canonical transform*, Journal of Modern Optics **71**(19-21), 2024: 700 -715. https://doi.org/10.1080/09500340.2024.2448577
[8] UNNIKRISHNAN G., SINGH K., *Double random fractional Fourier-domain encoding for optical security*, Optical Engineering **39**(11), 2004: 2853-2859. https://doi.org/10.1117/1.1313498
[9] SINGH H., YADAV A.K., VASHISTH S., SINGH K., *Optical image encryption using devil's vortex toroidal lens in the Fresnel transform domain*, International Journal of Optics, Vol. 2015, 2015: 926135. https://doi.org/10.1155/2015/926135
[10] SINGH H., *Cryptosystem based on devil's vortex Fresnel array and Fresnel transform for optical double-image encryption*, Journal of Optics, 2025. https://doi.org/10.1007/s12596-024-02428-2
[11] SACHIN, KUMAR R., SINGH P., *Multiuser optical image authentication platform based on sparse constraint and polar decomposition in Fresnel domain*, Physica Scripta **97**(11), 2022: 115101. https://doi.org/10.1088/1402-4896/ac925d
[12] ABUTURAB M.R., *Multilevel information cryptosystem using generalized singular value decomposition, optical interference, and devil's vortex Fresnel lens encoding*, Optics and Lasers in Engineering **181**, 2024: 108399. https://doi.org/10.1016/j.optlaseng.2024.108399
[13] SHIKDER A., NISHCHAL N.K., *Computer generated hologram encryption using array of vortex beams*, [In] *Digital Holography and 3-D Imaging 2022*, Technical Digest Series (Optica Publishing Group), 2022, paper W2A.13. https://doi.org/10.1364/DH.2022.W2A.13
[14] SHAO Z., DUAN Y., COATRIEUX G., WU J., MENG J., SHU H., *Combining double random phase encoding for colour image watermarking in quaternion gyrator domain*, Optics Communications **343**, 2015: 56-65. https://doi.org/10.1016/j.optcom.2015.01.002

[15] Wang Y., Quan C., Tay C.J., *New method of attack and security enhancement on an asymmetric cryptosystem based on equal modulus decomposition*, Applied Optics **55**(4), 2016: 679-686. https://doi.org/10.1364/AO.55.000679

[16] Khurana M., Rakheja P., *Asymmetric healthcare biometric image encryption and watermarking technique using QZ synthesis and QRD algorithm*, Multimedia Tools and Applications **83**, 2024: 76223-76245. https://doi.org/10.1007/s11042-024-18500-9

[17] 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

[18] Shen Y., Tang C., Lei Z., *A double random phase encoding-based asymmetric cryptosystem using QZ modulation*, Journal of Optics **52**, 2023: 189-196. https://doi.org/10.1007/s12596-022-00883-3

[19] Singh H., Yadav P., *An optical vortex-based asymmetric cryptosystem using QZ modulation for the double image encryption in the gyrator transform*, Iran Journal of Computer Science **7**, 2024: 829-842. https://doi.org/10.1007/s42044-024-00196-7

[20] Singh H., Gaur K.S., Thakran S., Singh K., *An asymmetric phase image encryption technique using Arnold transform, singular value decomposition, Hessenberg decomposition, and fractional Hartley transform*, Applied Physics B **130**, 2024: 186. https://doi.org/10.1007/s00340-024-08312-y

[21] Pourjabbar Kari A., Habibizad Navin A., Bidgoli A.M., Mirnia M., *A novel multi-image cryptosystem based on weighted plain images and using combined chaotic maps*, Multimedia Systems **27**(5), 2021: 907-925. https://doi.org/10.1007/s00530-021-00772-y

[22] Singh H., Singh K., *A watermarking-based asymmetric cryptosystem using gyrator transform, QZ modulation, and fractional vortex toroidal phase mask*, Journal of Optics **54**, 2025: 300-313. https://doi.org/10.1007/s12596-024-02329-4

[23] GaurK.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. https://doi.org/10.1016/j.ijleo.2023.171602

[24] 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**(5), 2023: 561. https://doi.org/10.3390/photonics10050561

[25] Rao T.R.N., Nam KH., *Private-key algebraic-coded cryptosystems*, [In] Odlyzko A.M. [Ed.] *Advances in Cryptology — CRYPTO' 86*, Lecture Notes in Computer Science, Vol. 263. Springer, Berlin, Heidelberg, 1987: 35-48. https://doi.org/10.1007/3-540-47721-7_3

[26] Niederreiter H., *Knapsack-type cryptosystems and algebraic coding theory*, Problems of Control and Information Theory-Problemy upravleniya i teorii informatsii **15**(2), 1986: 159-166.

[27] Mathur C.N., Narayan K., Subbalakshmi K.P., *On the design of error-correcting ciphers*, EURASIP Journal on Wireless Communications and Networking, 2006: 42871.

[28] Xiao Y., Zhao Y., Lee M.H., *Encrypting LDPC-codec*, 2006 8th international Conference on Signal Processing, Guilin, China, 2006. https://doi.org/10.1109/ICOSP.2006.345845

[29] Adamo O., Fu S., Varanasi M.R., *Physical layer error correction based cipher*, 2010 IEEE Global Telecommunications Conference GLOBECOM 2010, Miami, FL, USA, 2010: 1-5. https://doi.org/10.1109/GLOCOM.2010.5683788

[30] Cankaya E.C., Nair S., Cankaya H.C., *Applying error correction codes to achieve security and dependability*, Computer Standards & Interfaces **35**(1), 2013: 78-86. https://doi.org/10.1016/j.csi.2012.06.009

[31] Li N., Lin K.F., Lin W.L., Deng Z.L., *A joint encryption and error correction method used in satellite communications*, China Communications **11**(3), 2014: 70-79. https://doi.org/10.1109/CC.2014.6825260

[32] Yao J., Liu J., Yang Y., *Joint encryption and error correction technical research applied an efficient turbo code*, International Journal of Security and Its Applications **9**(10), 2015: 31-46. https://doi.org/10.14257/ijsia.2015.9.10.03

[33] DASS B.K., WASAN S.K., *On codes of order $r + (r + 1)_{m,s}$*, International Journal of Electronics **54**(3), 1983: 471-475. https://doi.org/10.1080/00207218308938744
[34] TYAGI V., RANI S., *New construction of GRM codes*, Asian-European Journal of Mathematics **5**(1), 2012: 1250012. https://doi.org/10.1142/S179355711250012X
[35] TYAGI V., RANI S., *Recursive matrix method for GRM and DGRM codes*, International Electronic Journal of Pure and Applied Mathematics **4**(4), 2012: 263-270.
[36] ABBE E., SHPILKA A., WIGDERSON A., *Reed–Muller codes for random erasures and errors*, IEEE Transactions on Information Theory **61**(10), 2015: 5229-5252. https://doi.org/10.1109/TIT.2015.2462817
[37] BHOWMICK A., LOVETT S., *The list decoding radius of Reed-Muller codes over small fields*, [In] *STOC'15: Proceedings of the Forty-Seventh Annual ACM Symposium on Theory of Computing*, Association for Computing Machinery, New York, NY, USA, 2015: 277-285. https://doi.org/10.1145/2746539.2746543
[38] DUMER I., SHABUNOV K., *Recursive error correction for general Reed–Muller codes*, Discrete Applied Mathematics **154**(2), 2006: 253-269. https://doi.org/10.1016/j.dam.2005.05.013
[39] SINGH S.K., ADACHI Y., KINASHI K., TSUTSUMI N., SAKAI W., JACKIN B.J., *Tailoring large asymmetric Laguerre–Gaussian beam array using computer-generated holography*, Photonics **10**(3), 2023: 247. https://doi.org/10.3390/photonics10030247
[40] TIAN H., ZHUANG X., YAN A., ZHANG H., *A novel multiple-image encryption with multi-petals structured light*, Scientific Reports **14**, 2024: 19559. https://doi.org/10.1038/s41598-024-70425-3
[41] MEHRA I., NISHCHAL N.K., *Fingerprint image encryption using phase retrieval algorithm in gyrator wavelet transform domain using QR decomposition*, Optics Communications **533**, 2023: 129265. https://doi.org/10.1016/j.optcom.2023.129265
[42] WANG X., NIE Z., LIANG Y., WANG J., LI T., JIA B., *Recent advances on optical vortex generation*, Nanophotonics **7**(9), 2018: 1533-1556. https://doi.org/10.1515/nanoph-2018-0072
[43] KONYAR M.Z., ÖZTÜRK S., *Reed Solomon coding-based medical image data hiding method against salt and pepper noise*, Symmetry **12**(6), 2020: 899. https://doi.org/10.3390/sym12060899

Received October 21, 2024
in revised form April 17, 2025