Optics Communications 533 (2023) 129265

Contents lists available at ScienceDirect

Optics Communications

journal homepage: www.elsevier.com/locate/optcom

Fingerprint image encryption using phase retrieval algorithm in gyrator wavelet transform domain using QR decomposition

Isha Mehra [a,*], Naveen K. Nishchal [b]

[a] Department of Applied Sciences & Humanities, ABES Engineering College, Ghaziabad, Uttar Pradesh, India
[b] Department of Physics, Indian Institute of Technology Patna, Bihta, Patna 801 106, India

ARTICLE INFO

Keywords:
Gyrator wavelet transform
GS phase retrieval algorithm
QR decomposition

ABSTRACT

In this paper, we propose a novel optical asymmetric fingerprint image encryption technique that uses QR decomposition in gyrator wavelet transform domain. A fingerprint image is bonded with a phase mask generated with Gerchberg–Saxton phase retrieval algorithm, which is gyrator wavelet transformed. This output is further applied to QR decomposition scheme and different keys are generated through it. The process is iterated to enhance the level of security. A Haar wavelet has been used in the study. Different phase images, gyrator transform orders and the parameters of the wavelet help achieve imperceptibility and robustness. The asymmetric keys make the system attack free like Brute force attack, known plain text attack, and special attack. Numerical simulations carried out on a MATLAB platform demonstrate the security, privacy, and validity of the proposed encryption scheme.

1. Introduction

Securing personal and professional data using optical systems has drawn considerable attention of scientific community in recent times. Data transferred in raw form will be more vulnerable to attacks. So, there is a need of developing highly efficient encryption mechanisms. The encryption mechanism can be digital and optical. Various digital schemes have been developed in the literature for enhancing security [1,2]. Optical encryption technique offers strong information security with ultra high speed and parallel processing capabilities. Double random phase encryption (DRPE) procedure was first put forward in 1995, which was improved by large number of researchers applying various optical transforms [3–5]. The basic DRPE was later proved to be vulnerable to various applicable attacks because of its symmetric property [6–10]. Phase-truncated Fourier transform (PTFT) was proposed as an asymmetric and non-linear cryptosystem by Qin and Peng [11]. Different encryption schemes based on PTFT method has been developed which were further found vulnerable to special attack [12–15]. Efficient cancelable biometric recognition system has been developed using PTFT approach [16]. The Gerchberg–Saxton(GS) phase retrieval algorithm and its modified version have been used as a tool in encryption schemes for developing object dependent phase-only functions [17–21].

Equal modulus decomposition (EMD) is a coherent superposition-based method. It is one of the new techniques for securing confidential information, in which the cipher text is derived from the plain text [22–25]. EMD encoding scheme resists known plaintext attack. Color image encryption using vectorial light and controllable optical vortex array have been also used for optical encryption [26,27]. Such schemes use a light beam which consist of spatially separated controllable orthogonal states of optical vortices.

In one of our previous studies, gyrator wavelet transform (GWT) was introduced as a new tool for dealing with the optical information processing applications [28–30]. It is a generalized transform that emerges from cascading two transforms, gyrator transform (GT) and wavelet transform (WT). Recently, a new technique based on the sparse matrix compression and storage has been implemented. This technique comprises of orthogonal–triangular decomposition (QR decomposition). The QR decomposition has found application in image compression and watermarking algorithms [31,32]. QR decomposition produces sparse matrix which can be used as ciphertext and product of two orthogonal and triangular matrices act as decryption keys. This makes system asymmetric.

It is known that asymmetric cryptosystem due to its nonlinear characteristics increases the complexity of an optical cryptosystem and is resistant to many attacks. In this paper, we propose an optical asymmetric fingerprint image encryption scheme using QR decomposition in GWT domain. The input phase masks have been generated from GS phase retrieval algorithm (phase image of Lena has been used in the algorithm). To the best of our knowledge, this is the first time that GWT

* Corresponding author.
E-mail addresses: Isha.mehra@abes.ac.in (I. Mehra), nkn@iitp.ac.in (N.K. Nishchal).

https://doi.org/10.1016/j.optcom.2023.129265
Received 7 November 2022; Received in revised form 4 January 2023; Accepted 5 January 2023
Available online 14 January 2023

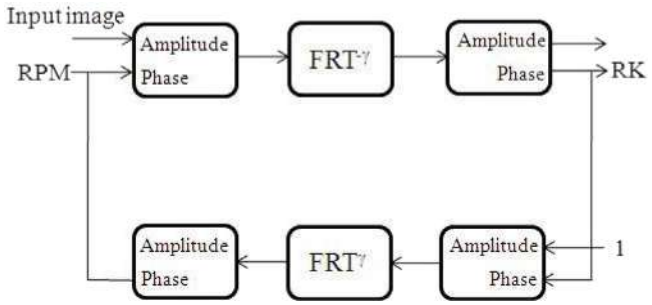

Fig. 1. Phase generation through modified G-S Phase retrieval algorithm.

domain QR decomposition scheme has been used for biometric security application.

In the proposed cryptosystem, instead of using random phase directly, the phases for encryption have been generated through modified GS phase retrieval algorithm [20]. If the attacker tries to decrypt input image of a fingerprint, it may result into decryption of used Lena image, whose generated phase has been used as encryption keys. This step will provide hindrance for the receiver which will disable the identity of the sender and the authenticity of the ciphertext. Thus, the economic interests of the users will be protected from original data loss. As far as the security issues are concerned, the proposed cryptosystem can resist the attack of iterative algorithm because of the use of the phase modulation technique

Numerical simulations carried out on MATLAB platform demonstrate the security, privacy, and validity of the proposed technique. The proposed scheme is found robust against occlusion and noise attacks. Section 2.1 of the paper briefly describes GS phase retrieval algorithm. Section 2.2 explains orthogonal triangular decomposition method. Section 3 describes proposed asymmetric cryptosystem. Section 4 comprises of scheme verification and validation results. Section 5 comprises different attacks which are applied on proposed cryptosystem and the last section concludes the study with highlights of the contribution.

2. Different schemes

2.1. Modified GS phase retrieval algorithm

The block diagram of the modified GS algorithm [18–20] is shown in Fig. 1.

It is defined through the following steps:

1. Any complex function $f_n'(x,y)$ after nth iteration is given as

$$f_n'(x,y) = |f(x,y)| \exp\{i2\pi r_n(x,y)\} \tag{1}$$

Here, the exponential term is the random phase mask (RPM) which is bonded with input image.

2. Now the complex function $f_n'(x,y)$ is fractional Fourier transformed (FRT) with some arbitrary fractional order α' as,

$$F_{n+1}(u,v) = \Im^{\alpha'}[f_n'(x,y)] = \left|F_{n+1}(u,v)\right| \exp\{i\varphi_n(u,v)\} \tag{2}$$

3. Replace amplitude of above equation with unity

$$F'_{n+1}(u,v) = 1 \times \exp\{i\varphi_n(u,v)\} \tag{3}$$

4. Now perform FRT to $F_{n+1}'(u,v)$ of order α' as

$$F''_{n+1}(x,y) = \Im^{-\alpha_1}[F'_{n+1}(u,v)] = \left|F''_{n+1}(x,y)\right| \times \exp\{i\varphi_n'(x,y)\} \tag{4}$$

Here, the exponential term is the random key (RK) which will act as an input phase for next cycle.

5. Replace amplitude of Eq. (4) with input intensity

$$f'_{n+1}(x,y) = |f(x,y)| \times \exp\{i\varphi_n'(x,y)\} = |f(x,y)| \times \exp\{ir_{n+1}(x,y)\} \tag{5}$$

The convergence of the iteration process is completed with the computation of the mean square error (MSE) as defined in Eq. (1), reaching the minimum value.

2.2. Orthogonal triangular decomposition method

In orthogonal–triangular decomposition or QR decomposition [31, 32] scheme, a given matrix $M \in R^{n\times n}$ having linear independent columns is transformed into an orthogonal matrix Q (satisfying condition $Q \times Q^{T} = I$), an upper triangular matrix R and a permutation matrix P. In case of a complex matrix decomposition, Q is obtained as a unitary matrix (satisfying condition $Q \times Q^{*} = I$) rather than orthogonal matrix. Statistically it can be expressed as,

$$M \times P = Q \times R \tag{6}$$

Here, Q^{T} and Q^{*} represent transpose and transpose conjugate of Q matrix. 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 so its storage and transmission will take less memory and bandwidth as compared to other data. QR decomposition produces sparse matrix which is an intermediate ciphertext and product of two orthogonal and triangular matrices serves as decryption keys. This makes system asymmetric.

Recently, we proposed GWT, a new tool for dealing with various optical information processing applications [28], where GT has been generalized by combining it with WT. This combination provides multi-resolution analysis of the rotation spectrum in position-spatial frequency planes. As we know, the GT of a two-dimensional (2D) real function $f(x_i, y_i)$ is expressed as,

$$\begin{aligned} G(x_0,y_0) &= G^{\alpha}[f(x_i,y_i)](x_0,y_0) \\ &= \frac{1}{|\sin\alpha|}\int f(x_i,y_i)K_{\alpha}(x_i,y_i,x_0,y_0)dx_i dy_i \end{aligned} \tag{7}$$

where (x_i, y_i) and (x_o, y_o) indicate the input and output plane coordinates, respectively. The transform kernel is denoted as,

$$K_{\alpha}(x_i,y_i,x_0,y_0) = \exp\left(i2\pi\frac{(x_0y_0 + x_iy_i)\cos\alpha - (x_iy_0 + x_0y_i)}{\sin\alpha}\right) \tag{8}$$

Here, α is GT transform angle. For $\alpha = 0$, it is the identity transform. For $\alpha = \pi/2$, it is the direct/inverse FT with rotation of the coordinates at $\pi/2$. A 2D GWT of the signal $f(x_i, y_i)$ is defined as follows [28],

$$\begin{aligned} &GW_f(a_1,a_2,b_1,b_2) = \\ &\frac{1}{\sqrt{a_1a_2}}\int_{-\infty}^{\infty}\int_{-\infty}^{\infty}\int_{-\infty}^{\infty}\int_{\infty}^{\infty}\frac{1}{|\sin\alpha|}f(x_i,y_i)h^{*}\left(\frac{x_0-b_1}{a_1},\frac{y_0-b_2}{a_2}\right) \\ &\times K_{\alpha}(x_i,y_i,x_0,y_0)dx_i dy_i dx_0 dy_0 \end{aligned} \tag{9}$$

If

$$\frac{1}{|\sin\alpha|}K_{\alpha}(x_i,y_i,x_0,y_0) = 1$$

or

$$K_{\alpha}(x_i,y_i,x_0,y_0) = |\sin\alpha|$$

This reduces to ordinary GT operation. The inverse GWT will be a two-step process; in the first step Eq. (7) is inverse WT operated [28].

$$\begin{aligned} &IWT[GW_f(a_1,a_2,b_1,b_2)] = \\ &\frac{1}{C}\int_{-\infty}^{\infty}\int_{-\infty}^{\infty}\int_{-\infty}^{\infty}\int_{-\infty}^{\infty}\frac{1}{a_1^3a_2^3}W_f(a_1,a_2,b_1,b_2)f(x_i,y_i) \\ &\times h\left(\frac{x_0-b_1}{a_1},\frac{y_0-b_2}{a_2}\right)da_1da_2db_1db_2 \end{aligned} \tag{10}$$

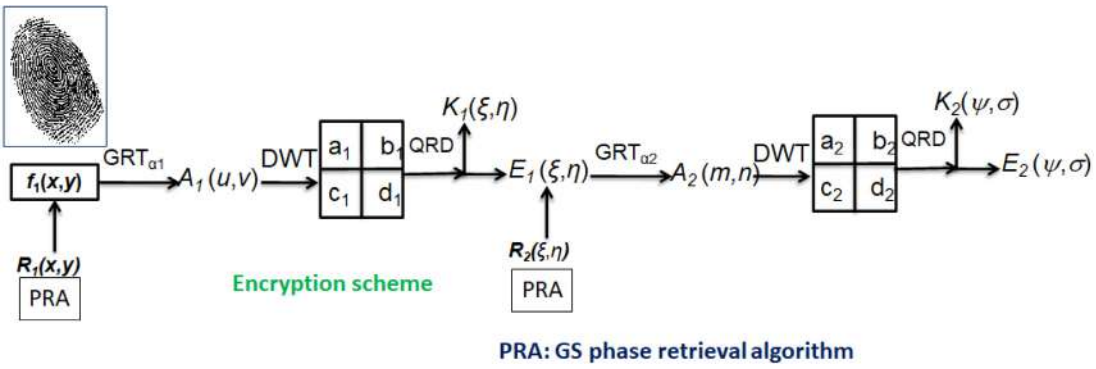

Fig. 2a. Block diagram for encryption.

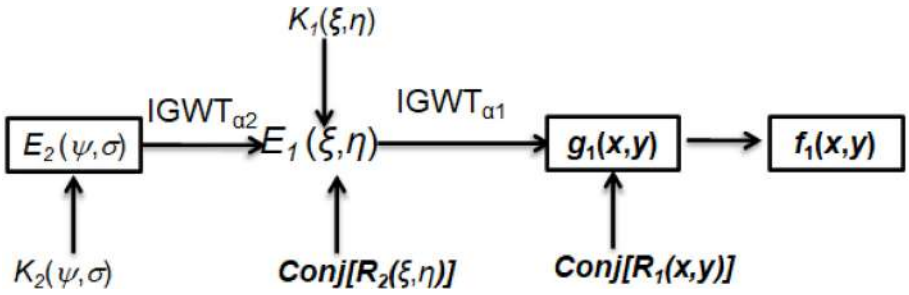

Fig. 2b. Block diagram for decryption using asymmetric keys.

where C is a constant. The inverse GT corresponds to the GT at rotation angle '-α'. It is defined as,

$$R_{-\alpha}\{f(x_i, y_i)\}(x_0, y_0) = R_{-\alpha}\{f(-x_i, y_i)\}(-x_0, y_0) \tag{11}$$

Thus,

$$IGT\{IWT[GW_f(a_1, a_2, b_1, b_2)]\} = f(x_i, y_i) \tag{12}$$

where the input image $f(x_i, y_i)$ is achieved through inverse GT operation.

3. Asymmetric cryptosystem scheme

Fig. 2a displays schematic diagram of the encryption procedure. The fingerprint image is used as the data to be secured, represented here by $f(x, y)$.

The encryption process can be divided into following steps:

Step 1: A phase mask generated through modified GS phase retrieval algorithm is employed on fingerprint image $f(x, y)$.

Step 2: This bonded image is Gyrator wavelet transformed of the order α_1.

To execute this, at first, the bonded image $im(x, y)$ is GT operated with order α_1.

$$A_1(u, v) = GT^{\alpha_1}[im(x, y)](u, v) = \frac{1}{|\sin\beta|}\iint im(x, y)\exp i2\pi r_1(x, y) \times K_\beta(x, y, u, v)dxdy \tag{13}$$

The obtained spectrum is single level WT operated using 'Haar' wavelet. This results into four frequency sub-bands. After each transform is performed the size of the square which contains the most important information is reduced by a factor of 4 that is why four sub-bands are formed termed as approximation coefficient, horizontal coefficient, vertical coefficient and diagonal coefficient.

All these sub-bands are then position multiplexed. As we have different sub bands (approximation, horizontal, vertical and diagonal) each of size 128 × 128 pixels, so all these sub bands are placed on the 256 × 256 pixels sized matrix whose all elements are one. This has been done on MATLAB digitally.

$$G_1(m, n) = DWT\{A_1(u, v)\} = \{W_{LL}, W_{HL}, W_{LH}, W_{HH}\} \tag{14}$$

Step 3: $G_1(m, n)$ obtained is further decomposed using QR decomposition technique to give private key — key1 and intermediate ciphertext $[Q1, R1, P1] = E_1(\xi, \eta)$

$$key1 = Q1 \times R1 \tag{15}$$

Step 4: Another phase mask generated through modified GS phase retrieval algorithm is employed on first ciphertext $E_1(\xi, \eta)$. The whole process is iterated resulting into final encrypted image, $E_2(\Psi, \sigma)$.

The decryption process is shown in Fig. 2b. The final ciphertext is bonded with the private key $k_2(\Psi, \sigma)$. It is further inverse Gyrated wavelet transformed and simultaneously two keys are applied which in combination form a new asymmetric key ie. $\{k_1(\xi, \eta) \times \text{conj}[R_2(\xi, \eta)\}$. Further, the process is repeated which results into a decrypted image $f_1(x, y)$.

Here, the system is completely asymmetric, as the encryption keys are $R_1(x, y)$ and $R_2(\xi, \eta)$ while decryption keys are $k_2(\Psi, \sigma)$ and $\{k_1(\xi, \eta) \times \text{conj}[R_2(\xi, \eta)]\}$ which are different from encryption keys. Along with these main keys, type of wavelet, GWT orders at different levels enhances the key space.

4. Computer experiment

We performed the numerical simulation using MATLAB 7.10. A fingerprint image of size 256 × 256 pixels is used as an input image to be secured as shown in Fig. 3(a).

An image of Lena has been used to generate phase image using GS algorithm. Its phase image is shown in Fig. 3(b). The fingerprint image to be encrypted is bonded with a generated phase mask, which is then gyrated wavelet transformed employing "Haar" wavelet. All coefficients of Haar wavelet have been shown in Fig. 4(a)–(d), respectively. The parameters of the wavelet serve as additional keys to the security system. All these are position multiplexed and is further applied to QR

Fig. 3. (a) Fingerprint image and (b) phase image of Lena generated through modified GS algorithm.

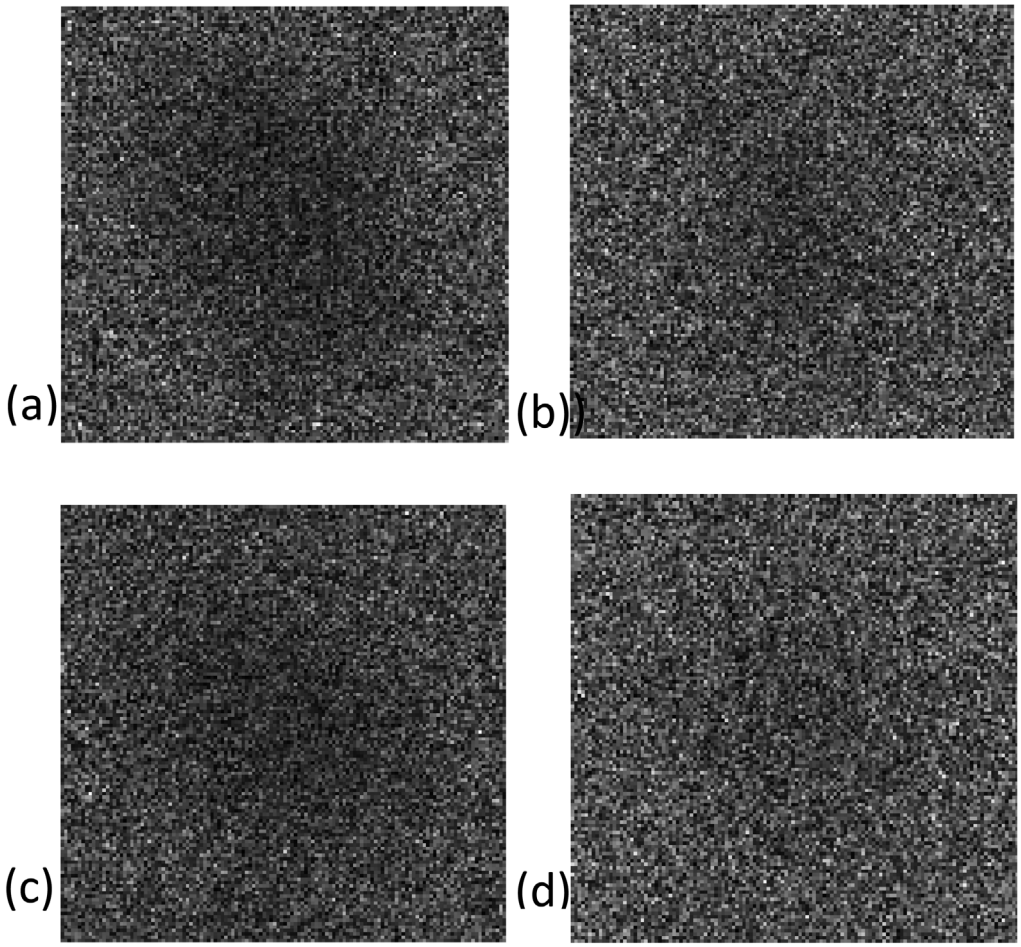

Fig. 4. Wavelet transform of intermediate encrypted image: (a) approximation coefficient, (b) horizontal coefficient, (c) vertical coefficient, and (d) diagonal coefficient.

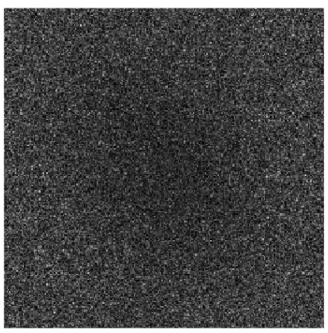

Fig. 5. Level-1 encrypted image.

decomposition scheme and different keys are generated through it. The intermediate ciphertext has been shown in Fig. 5.

Intermediate ciphertext is bonded with phase image of Lena which is generated modified GS algorithm. Then it is gyrator wavelet transformed. All coefficients of Haar wavelet have been shown in Fig. 6(a)–(d), respectively. All coefficients are position multiplexed and is applied to QR decomposition scheme. The final ciphertext has been shown in Fig. 7.

MSE has been evaluated to check the performance of the retrieved original image and the input image. The MSE between original image [Fig. 3(a)] used for encryption and decrypted image [Fig. 8] is 1.054×10^{-28}. The MSE value close to zero indicates that the original image is perfectly retrieved. A graph has been plotted between MSE

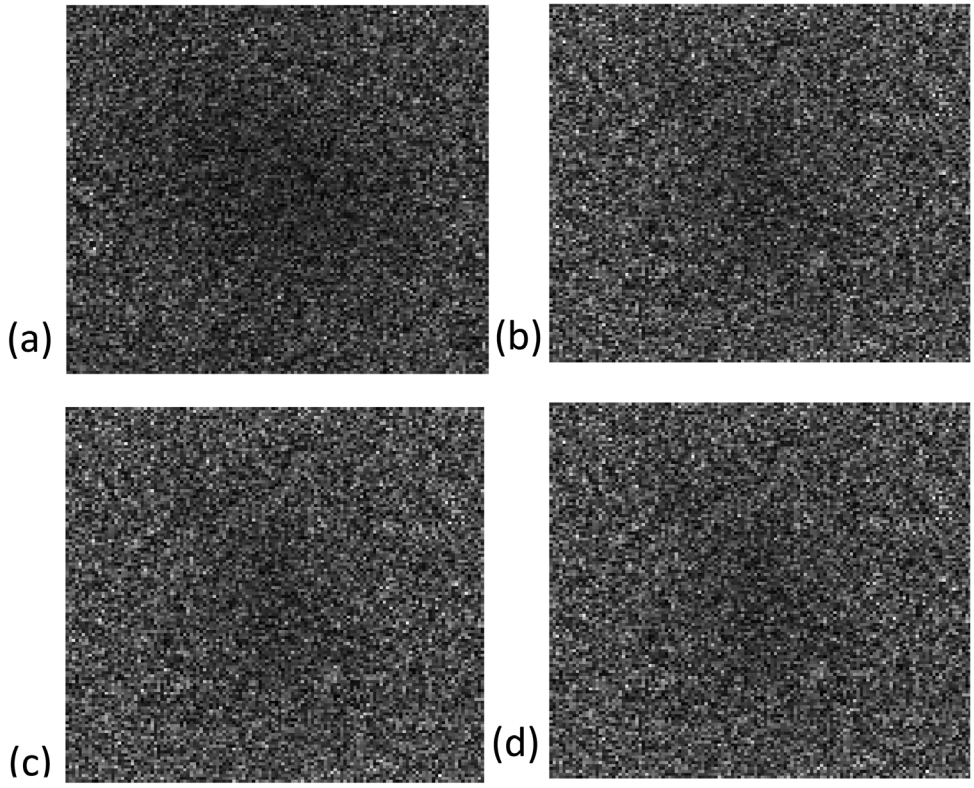

Fig. 6. Wavelet transform of Fig. 5 encrypted image (a) approximation coefficient, (b) horizontal coefficient, (c) vertical coefficient, and (d) diagonal coefficient.

Fig. 7. Ciphertext.

Fig. 8. Decrypted image obtained after using asymmetric keys.

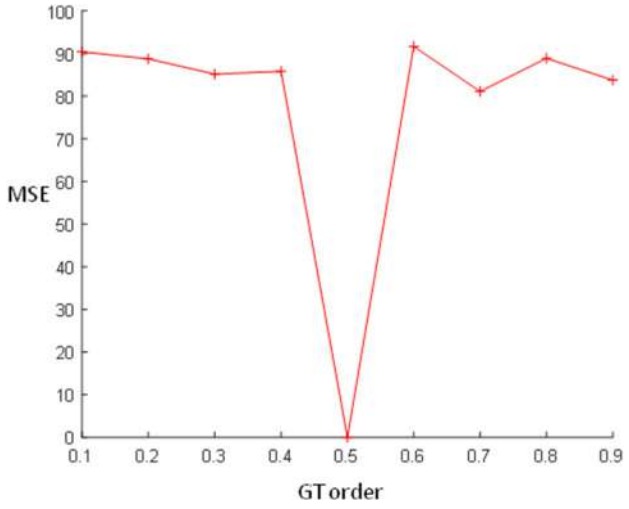

Fig. 9. (Color online) Plot of MSE versus GT orders for the generation of decryption key.

and GT order for level 1 encryption [Fig. 9]. This shows that the error increases as GT order deviates from its original value.

5. Attack analysis

Attack algorithms can be applied to extract the security keys if the complete complex valued-fields are known. For example, in case of known-plaintext attack, several plain images and their corresponding ciphertexts are known [8]. The phase keys can be evaluated through iterative algorithms. But, in this scheme, the asymmetric keys are not pure phase keys rather they are the complex valued keys i.e., two orthogonal and triangular matrices. Thus, without knowledge of the

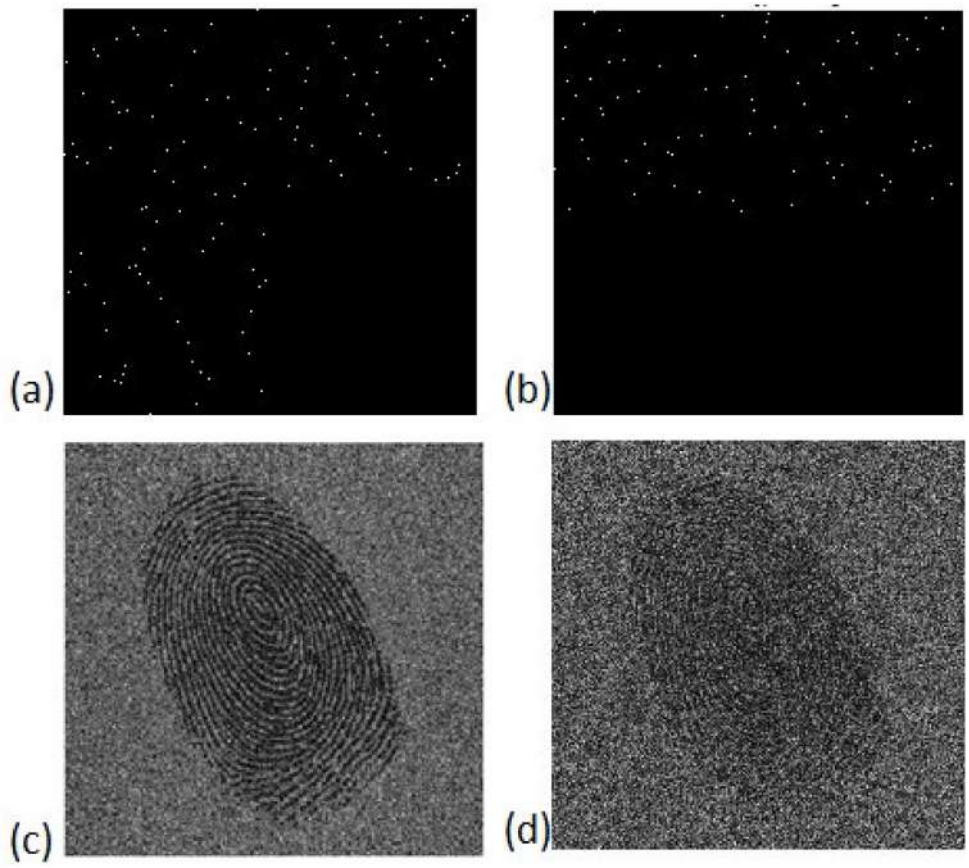

Fig. 10. Occluded Encrypted images (a) 25% occlusion, (b) 50% Occlusion, (c) decrypted images with 25% occlusion, and (d) decrypted images with 50% occlusion.

constraints like amplitude of asymmetric keys it is impossible to apply such attack.

In case of brute force attack, all possible asymmetric keys are searched. As, all the four asymmetric keys for an input image are of 256 × 256 pixels. Out of these, four R_1 and R_2 are the phase keys already generated through phase retrieval algorithm while other two asymmetric keys k_1 and k_2 are complex-valued fields. To find such complex fields it is practically inconceivable through brute force attack [29].

Specific attack is the main attack of amplitude and phase truncation based asymmetric cryptosystem in which phase keys can be obtained through phase retrieval algorithm [29]. In this case, the asymmetric keys are not pure phase keys rather these are complex keys. In addition to this, the rest of the keys have been obtained through GS phase retrieval algorithm. Hence, it can be claimed that the proposed cryptosystem is resistant to the known plaintext attack, specific attack, and brute force attack. The proposed scheme is also evaluated against occlusion where the occluded spaces are replaced by zeros. Figures 10(a) and (b) show occluded encrypted image with 25% and 50% occlusion, respectively and the corresponding decrypted images have been shown in Figs. 10(c) and 10(d), respectively.

The statistical analysis of the proposed crypto mechanism has been shown in Fig. 11. through 3D plot analysis of different test images.

5.1. Histogram analysis

The ciphertext image histogram describes an image encryption quality in a better way. A proper cryptosystem tends to encrypt an input data into random information thus its related ciphertext histogram varies relatively. Fig. 12(a) shows histogram of input biometric image and Fig. 12(b) shows histogram of Lena image whose modified phase has been used for encryption and decryption. Fig. 12(c) shows the histogram of final encrypted image. In order to check security issues a cameraman image and Lena image has been taken for decryption purpose. Again, its phase has been generated using modified GS phase retrieval algorithm but could not retrieve input biometric image successfully with CC as 0.1251 and MSE as 94.025.

Fig. 13(a) shows cameraman image whose phase is used for decryption multiple times. Fig. 13(b) shows histogram of cameraman image whose generated phase is used a wrong key and Fig. 13(c) shows the decrypted input image with wrong phase key. Fig. 13(d) shows the histogram of corresponding decrypted image as a wrong key. This analysis shows that the histogram of decrypted images obtained from two different phase keys are entirely different. Hence, this enhances the security of the proposed cryptosystem.

6. Conclusion

It is known that asymmetric cryptosystem due to its nonlinear characteristics increases the complexity of an optical cryptosystem and is resistant to many attacks. In this paper, we propose an optical asymmetric cryptosystem of fingerprint image using QR decomposition scheme in GWT domain. QR decomposition asymmetric scheme has been used for fingerprint encryption. Also, key space has been enhanced due to the combination of GS algorithm, GWT, and QR decomposition. The different phase masks as well as the parameters of the GWT; gyrator angle, level and type of mother wavelet, position of different frequency bands in the intermediate frequency planes and the output planes

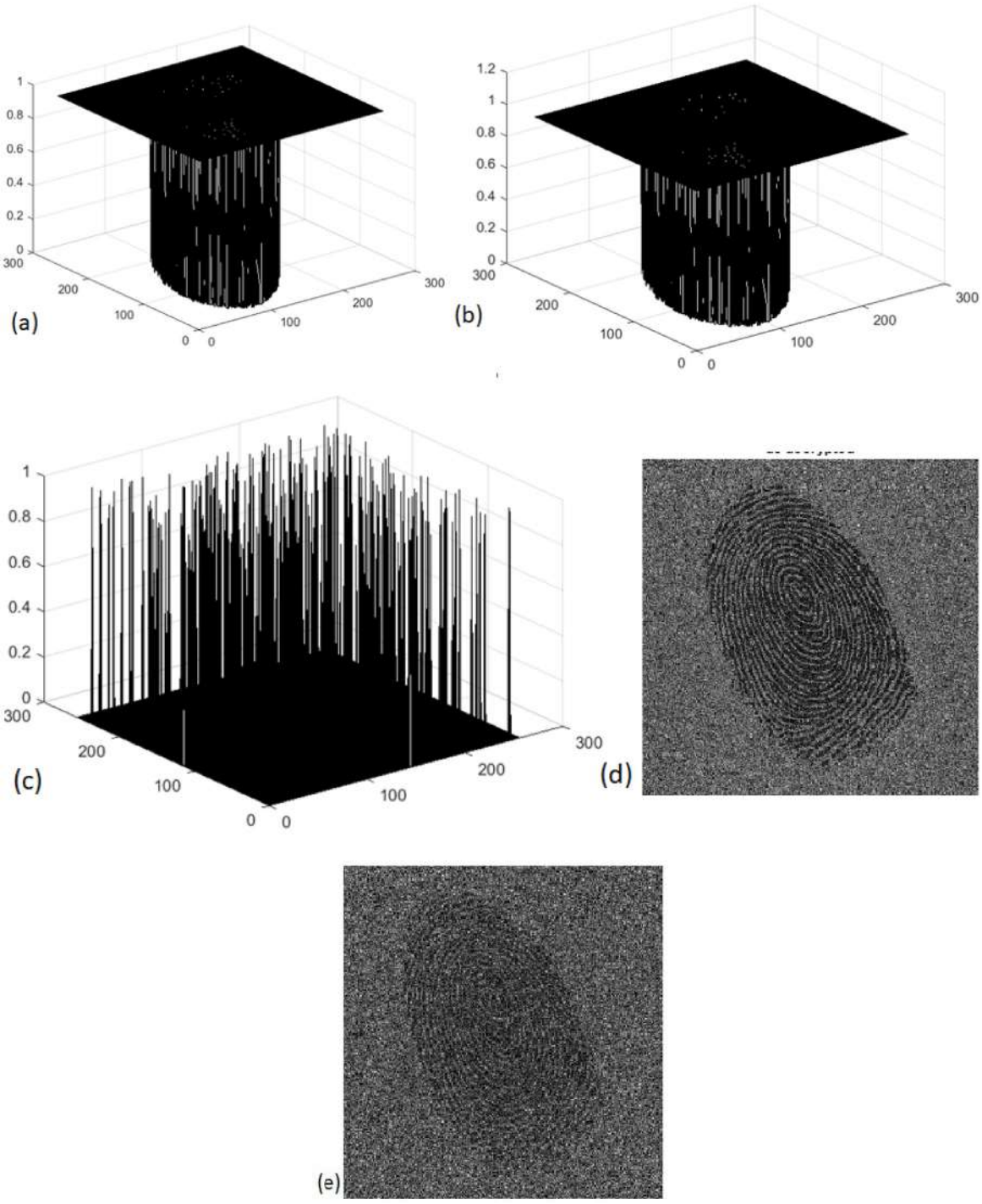

Fig. 11. Three-dimensional plots of (a) Input image (b) decrypted image with correct keys, (c) encrypted image, (d) decrypted image with 25% occlusion of ciphertext, and (e) decrypted image with 50% occlusion of ciphertext.

constitute the keys to the proposed cryptosystem. The study would find application in securing biometrics since it requires less memory and space but without any compromise with the level of security. This cryptosystem is applicable to binary and grey scale images as well. The memory size will increase in case of grey scale images.

Declaration of competing interest

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

Data availability

Data will be made available on request.

Acknowledgments

One of the authors, N. K. Nishchal wishes to acknowledge the financial support from the Scientific and Engineering Research Board, Govt. of India, under Grant No. CRG/2021/001763.

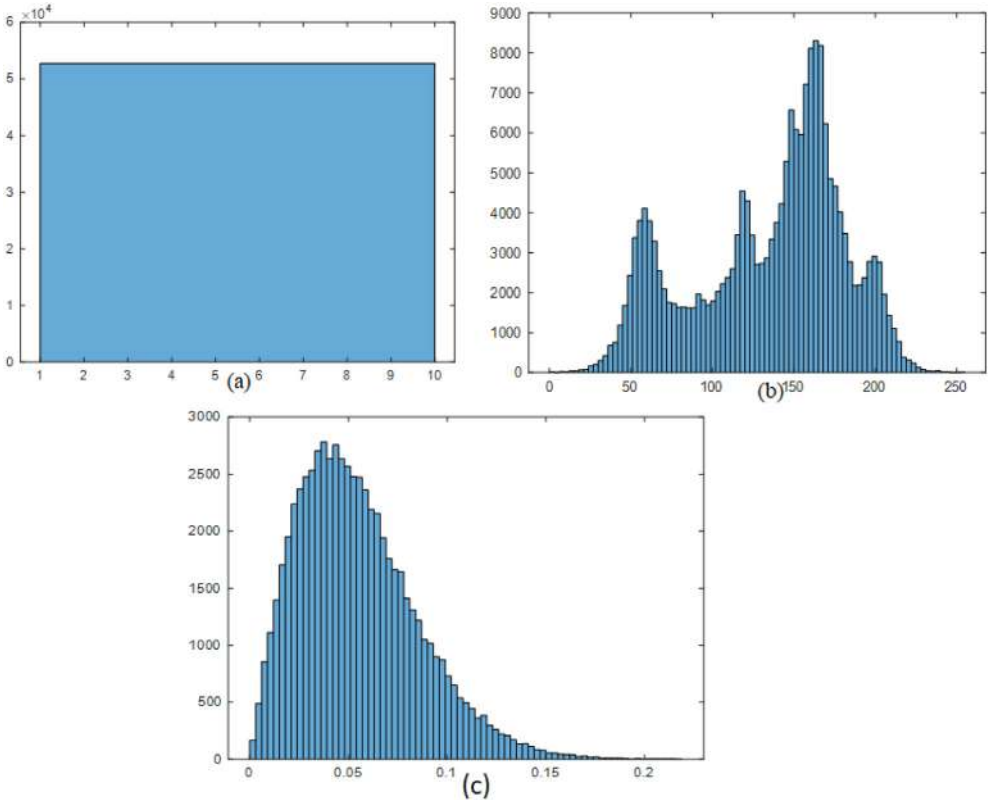

Fig. 12. (a) Histogram of input biometric image, (b) histogram of Lena image whose modified phase has been used for encryption, and (c) histogram of encrypted image.

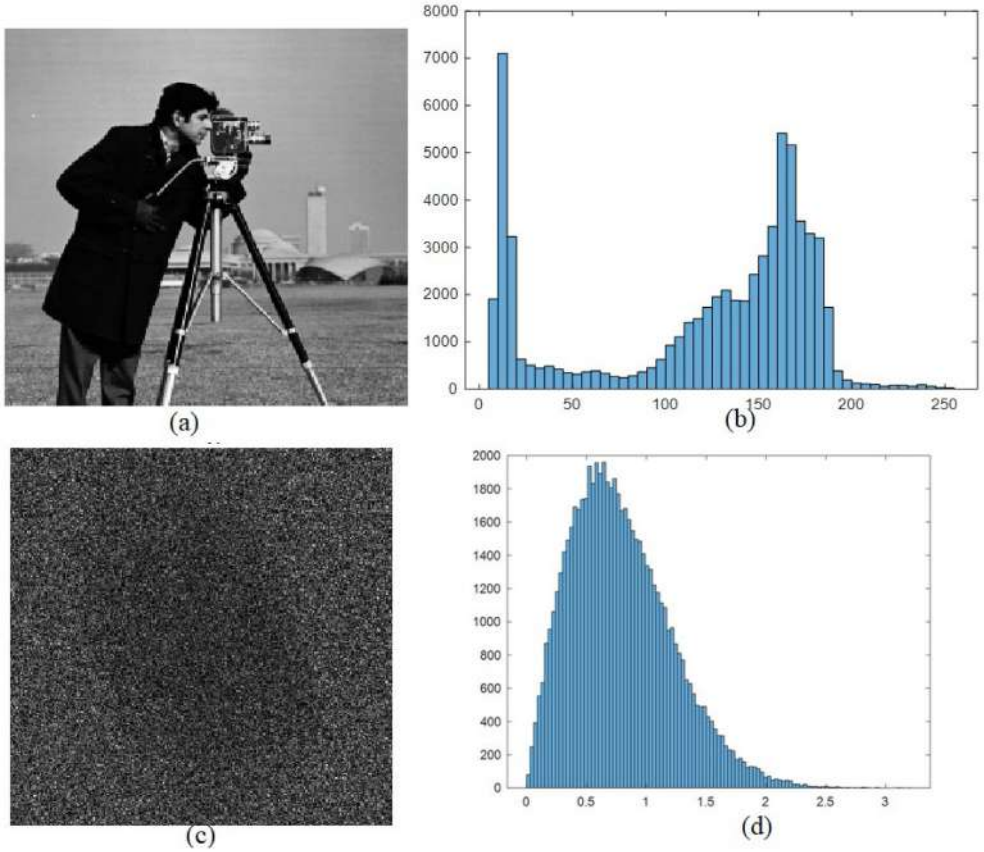

Fig. 13. (a) Cameraman image, (b) histogram of different key image of cameraman, (c) decrypted image with wrong phase key of cameraman, and (d) histogram of decrypted image which is different from histogram of input image resulting into abrupt CC and MSE.

References

[1] K. Kaur, V. Khemchandani, Securing visual cryptographic shares using public key encryption, in: Proc. of the International Conference on Advance Computing Conference, IACC, 2013, pp. 1108–1113, https://ieeexplore.ieee.org/document/6514382.

[2] P. Dixit, A.K. Gupta, M.C. Trivedi, V.K. Yadav, Traditional and Hybrid Encryption Techniques: A Survey, Networking Communication and Data Knowledge Engineering, Springer, New York, 2018, pp. 239–248, https://link.springer.com/chapter/10.1007/978-981-10-4600-1_22.

[3] N.K. Nishchal, Optical Cryptosystems, IoP Publs., Bristol, UK, 2019, https://iopscience.iop.org/book/mono/978-0-7503-2220-1.

[4] G. Situ, G. Pedrini, W. Osten, Strategy for cryptanalysis of optical encryption in the Fresnel domain, Appl. Opt. 49 (3) (2010) 457–462, http://dx.doi.org/10.1364/AO.49.000457.

[5] N.K. Nishchal, T.J. Naughton, Flexible optical encryption with multiple users and multiple security level, Opt. Commun. 284 (3) (2011) 735–739, http://dx.doi.org/10.1016/j.optcom.2010.09.065.

[6] A. Carnicer, M.M. Usategui, S. Arcos, I. Juvells, Vulnerability to chosen-cyphertext attacks of optical encryption schemes based on double random phase keys, Opt. Lett. 30 (13) (2005) 1644–1646, http://dx.doi.org/10.1364/OL.30.001644.

[7] U. Gopinathan, D.S. Monaghan, T.J. Naughton, J.T. Sheridan, A known-plaintext heuristic attack on the Fourier plane encryption algorithm, Opt. Express 14 (8) (2006) 3181–3186, http://dx.doi.org/10.1364/OE.14.003181.

[8] X. Peng, P. Zhang, H. Wei, B. Yu, Known-plaintext attack on optical encryption based on double random phase keys, Opt. Lett. 31 (8) (2006) 1044–1046, http://dx.doi.org/10.1364/OL.31.001044.

[9] G. Situ, U. Gopinathan, D.S. Monaghan, J.T. Sheridan, Cryptanalysis of optical security systems with significant output images, Appl. Opt. 46 (22) (2007) 5257–5262, http://dx.doi.org/10.1364/AO.46.005257.

[10] Y. Frauel, A. Castro, T.J. Naughton, B. Javidi, Resistance of the double random phase encryption against various attacks, Opt. Express 15 (16) (2007) 10253–10265, http://dx.doi.org/10.1364/OE.15.010253.

[11] W. Qin, X. Peng, Asymmetric cryptosystem based on phase-truncated Fourier transforms, Opt. Lett. 35 (2) (2010) 118–120, http://dx.doi.org/10.1364/OL.35.000118.

[12] X. Wang, D. Zhao, Double image self encoding and hiding based on phase-truncated Fourier transform, Opt. Commun. 284 (19) (2011) 4441–4445, http://dx.doi.org/10.1016/j.optcom.2011.06.025.

[13] X. Wang, D. Zhao, Multiple image encryption based on non-linear amplitude-truncation and phase-truncation in Fourier domain, Opt. Commun. 284 (1) (2011) 148–152, http://dx.doi.org/10.1016/j.optcom.2010.09.034.

[14] X. Wang, D. Zhao, Security enhancement of a phase-truncation based image encryption algorithm, Appl. Opt. 50 (36) (2011) 6645–6651, http://dx.doi.org/10.1364/AO.50.006645.

[15] S.K. Rajput, N.K. Nishchal, Image encryption based on interference that uses fractional Fourier domains asymmetric keys, Appl. Opt. 51 (10) (2012) 1446–1452, http://dx.doi.org/10.1364/AO.51.001446.

[16] A. Alarifi, M. Amoon, M.H. Aly, W. El-Shafai, Optical PTFT asymmetric cryptosystem-based secure and efficient cancelable biometric recognition system, IEEE Access 8 (2020) 221246-221268, https://ieeexplore.ieee.org/document/9288658.

[17] X. Wang, D. Zhao, Double images encryption method with resistance against the specific attack based on an asymmetric algorithm, Opt. Express 20 (11) (2012) 11994–12003.

[18] H.E. Hwang, H.T. Chang, W.N. Lie, Fast double-phase retrieval in Fresnel domain using modified Gerchberg–Saxtonalgorithm for lensless optical security systems, Opt. Express 17 (2009) 13700–13710.

[19] X. Deng, D. Zhao, Single-channel color image encryption using a modified Gerchberg–Saxtonalgorithm and mutual encoding in the Fresnel domain, Appl. Opt. 50 (2011) 6019–6025, http://dx.doi.org/10.1364/AO.50.006019.

[20] H.E. Hwang, H.T. Chang, W.N. Lie, Multiple-image encryption and multiplexing using a modified gerchberg–saxtonalgorithm and phase modulation in fresnel-transform domain, Opt. Lett. 34 (2009) 3917–3919, http://dx.doi.org/10.1364/OL.34.003917.

[21] S.K. Rajput, N.K. Nishchal, Fresnel domain nonlinear optical image encryption scheme based on Gerchberg–Saxtonphase-retrieval algorithm, Appl. Opt. 53 (2014) 418–425, http://dx.doi.org/10.1364/AO.53.000418.

[22] J. Cai, X. Shen, M. Lei, C. Lin, S. Dou, Asymmetric optical cryptosystem based on coherent superposition and equal modulus decomposition, Opt. Lett. 40 (2015) 475–478, http://dx.doi.org/10.1364/OL.40.000475.

[23] H. Chen, C. Tanougast, Z. Liu, L. Sieler, Asymmetric optical cryptosystem for color image based on equal modulus decomposition in gyrator transform domains, Opt. Lasers Eng. 93 (2017) 1–8, http://dx.doi.org/10.1016/j.optlaseng.2017.01.005.

[24] A. Fatima, I. Mehra, N.K. Nishchal, Optical image encryption using equal modulus decomposition and multiple diffractive imaging, J. Opt. 18 (2016) 085701, https://iopscience.iop.org/article/10.1088/2040-8978/18/8/085701.

[25] R. Kumar, B. Bhaduri, Q. Chenggen, Asymmetric optical image encryption using Kolmogorov phase screens and equal modulus decomposition, Opt. Eng. 56 (2017) 113109, http://dx.doi.org/10.1117/1.OE.56.11.113109.

[26] P. Kumar, N.K. Nishchal, A. AlFalou, Color image encryption using vectorial light field through a compact optical set-up, J. Opt. 24 (2022) 064017, https://iopscience.iop.org/article/10.1088/2040-8986/ac6f0d.

[27] P. Kumar, N.K. Nishchal, A. AlFalou, Controllable optical vortex array for image encoding, IEEE Photon. Technol. Lett. 34 (2022) 521–524, https://ieeexplore.ieee.org/abstract/document/9761249/authors#authors.

[28] I. Mehra, A. Fatima, N.K. Nishchal, Gyrator wavelet transform, IET Image Process. 12 (2018) 432–437, http://dx.doi.org/10.1049/iet-ipr.2017.0666.

[29] I. Mehra, N.K. Nishchal, Optical asymmetric image encryption using gyrator transform, Opt. Commun. 354 (2015) 344–352, http://dx.doi.org/10.1016/j.optcom.2015.06.015.

[30] H. Singh, Devil's vortex Fresnel lens phase masks on an asymmetric cryptosystem based on phase-truncation in gyrator wavelet transform domain, Opt. Lasers Eng. 81 (2016) 125–139, http://dx.doi.org/10.1016/j.optlaseng.2016.01.014.

[31] Q. Su, Y. Niu, G. Wang, S. Jia, J. Yue, Color image blind watermarking scheme based on QR decomposition, Sig. Process. 94 (2014) 219–235, http://dx.doi.org/10.1016/j.sigpro.2013.06.025.

[32] P. Rakheja, P. Singh, R. Vig, An asymmetric image encryption mechanism using QR decomposition in hybrid multi-resolution wavelet domain, Opt. Lasers Eng. 134 (2020) 106177, http://dx.doi.org/10.1016/j.optlaseng.2020.106177.