Optica Applicata, Vol. LII, No. 2, 2022
DOI: 10.37190/oa220210

Asymmetric double image encryption, compression and watermarking scheme based on orthogonal-triangular decomposition with column pivoting

Savita ANJANA[1*], Pankaj RAKHEJA[2], Ak YADAV[3], Phool SINGH[4], Hukum SINGH[1]

[1]Department of Applied Sciences, The NorthCap University, Gurugram, India, 122017

[2]Department of Computer Science Engineering, The NorthCap University, Gurugram, India, 122017

[3]Department of Mathematics, Central University of Haryana, Mahendergarh, India, 123031

[4]Department of Mathematics, SoET, Central University of Haryana, Mahendergarh, India, 123031

[*]Corresponding author: savita.anjana13@gmail.com

A novel asymmetric scheme for double image encryption, compression and watermarking based on QR decomposition in the Fresnel domain has been presented. The QR decomposition provides a permutation matrix as a ciphertext, and the product of orthogonal and triangular matrix as a key. The ciphertext obtained through this process is a sparse matrix that is compressed by the CSR method to give compressed encrypted data, which when combined with a host image, gives a watermarked image. Thus, a cryptosystem that involves compression and watermarking is proposed. The proposed scheme is validated for grayscale images. To check the efficacy of the proposed scheme, histograms, statistical parameters, and key sensitivity are analyzed. The scheme is also tested against various attacks. Numerical simulations are performed to validate the security of the scheme.

Keywords: QR decomposition, Fresnel transform, sparse matrix, asymmetric cryptosystem.

1. Introduction

Worldwide commercial organizations and governments are facing ever-increasing numbers of cyber-attacks. Since image data is equally prone to such attacks, their security during transmission and in a system is equally important. One of the techniques to secure the image data is image encryption, and so far, several approaches have been proposed to encrypt images. A well-known and widely reported approach for image encryption was proposed by Refregier and Javidi [1] in 1995. They proposed an optical system of double random phases to encrypt images in the Fourier domain, which was also implemented digitally. Similarly, researchers introduced the use of other transforms in double random phase encoding [2–11]. All these systems are symmetric in nature

as the same keys are used for encryption and decryption. Later, QIN and PENG [12] introduced an asymmetric cryptosystem based on phase truncation to encrypt images in the Fourier domain. Following them, many asymmetric cryptosystems using various decomposition techniques have been proposed by researchers, like optical cryptosystem based on polar decomposition and Shearlet transform [13] *etc*. Several double image cryptosystems have also been introduced [14–21]. Double image cryptosystems allow multiple images to be sent over a channel simultaneously, thereby optimizing the use of available resources during transmission. Double image cryptosystems proposed in the recent past have used the iterative phase retrieval algorithm [15, 20], random binary encoding [18], chaotic map algorithms [16] and many more. Various studies [22–26] have shown that optical cryptosystems are vulnerable to various attacks. Just as image security, image compression has also grabbed the attention of researchers. Many image compression techniques have been introduced [27–30], and it has been observed that sparse matrix compression and storage is much easier than dense matrices. Thus, we have proposed a new encryption, compression and watermarking algorithm for double images using orthogonal-triangular decomposition (QR decomposition) with column pivoting. QR decomposition has been widely used for image watermarking and compression algorithms [31, 32]. Orthogonal-triangular decomposition with column pivoting is a matrix factorization technique in which a given matrix $M \in R^{n \times n}$ with linearly independent columns is decomposed to give an orthogonal matrix Q, an upper triangular matrix R and a permutation matrix P. Mathematically, it can be represented as

$$\begin{bmatrix} m_{11} & \cdots & m_{1n} \\ \vdots & \ddots & \vdots \\ m_{n1} & \cdots & m_{nn} \end{bmatrix} \times \begin{bmatrix} p_{11} & \cdots & p_{1n} \\ \vdots & \ddots & \vdots \\ p_{n1} & \cdots & p_{nn} \end{bmatrix} = \begin{bmatrix} q_{11} & \cdots & q_{1n} \\ \vdots & \ddots & \vdots \\ q_{n1} & \cdots & q_{nn} \end{bmatrix} \times \begin{bmatrix} r_{11} & \cdots & r_{1n} \\ \vdots & \ddots & \vdots \\ 0 & \cdots & r_{nn} \end{bmatrix} \tag{1}$$

i.e., $M \times P = Q \times R$.

The proposed algorithm produces a sparse matrix for the encrypted image, which is watermarked using a host image.

One of the main features of our algorithm is that the ciphertext obtained is in a sparse matrix form, and this enables us to store it in compressed form using any sparse matrix storage technique, such as CSR (Compressed Sparse Row) [33]. The proposed scheme is implemented using MATLAB. Strength of the scheme is assessed by computing and analyzing various statistical parameters. The scheme is also tested against various attacks. Entropy computation, along with histograms and statistical analysis, show the efficacy of the scheme.

2. The proposed algorithm

Figure 1 shows the schematic diagram for the encryption, compression, and watermarking of double images. All the steps involved in the proposed algorithm are explained in the following subsections.

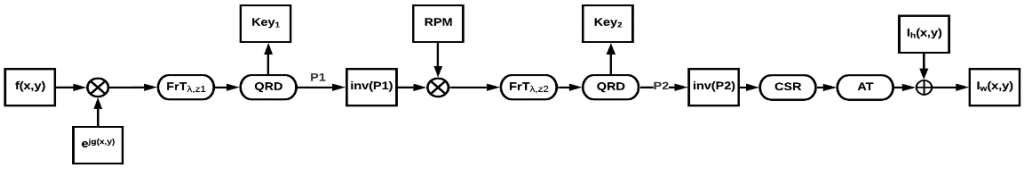

Fig. 1. Flowchart showing encryption, compression, and watermarking process.

2.1. Encryption, compression, and watermarking process

The two input images $f(x, y)$ and $g(x, y)$, one considered as an amplitude and the other as a phase, are first combined to give $H(x, y)$. Then, the following steps are implemented to give the encrypted image $E(x, y)$.

$$\left[Q_1, R_1, P_1\right] = \mathrm{QRD}\Big(\mathrm{FrT}\Big(H(x, y)\Big)\Big) \tag{2}$$

$$\mathrm{Key}_1 = Q_1 \times R_1 \tag{3}$$

The inverse of P_1, is then modulated with a random phase mask (RPM). This modulated image is again subjected to Fresnel transform, and once again QR factorized to give another private key (Key_2) and the ciphertext $E(x, y)$.

$$\left[Q_2, R_2, P_2\right] = \mathrm{QRD}\Big(\mathrm{FrT}(\mathrm{RPM} \times P_1^{-1})\Big) \tag{4}$$

$$\mathrm{Key}_2 = Q_2 \times R_2 \tag{5}$$

$$E(x, y) = P_2^{-1} \tag{6}$$

The encrypted image $E(x, y)$ is then compressed by the CSR [33] (Compressed Sparse Row) method, which is described as follows.

For a 4 × 4 sparse matrix A. CSR method will give three column vectors as follows:

$$A = [a000\ 0bc0\ 00d0\ 0000] \tag{7}$$

First column vector V contains all non-zero entries of matrix A shown as

$$V = [a\ b\ c\ d\ ] \tag{8}$$

The second column vector, RV, is obtained by the following steps:

1) RV[0] = 0; that means the first entry in the vector RV is zero.

2) RV[k] = RV[k – 1] + (number of non-zero entries in the $(k-1)^{\mathrm{th}}$ row of the matrix), if the matrix to be compressed is of order $n \times n$, then there will be $(n + 1)$ elements in the vector RV. First, n elements store the index of the non-zero elements in the rows of the matrix. The last element stores the total number of non-zero elements.

$$\mathrm{RV} = [0\ 1\ 3\ 4\ 4] \tag{9}$$

The third column vector, CV, contains the column index of non-zero entries of matrix A.

$$\mathrm{CV} = [0\ 1\ 2\ 2] \tag{10}$$

Therefore, the matrix A is now represented by the following three column vectors, which contain a total of 13 elements.

$$V = [a, b, c, d] \tag{11}$$

$$\mathrm{RV} = [0\ 1\ 3\ 4\ 4] \tag{12}$$

$$\mathrm{CV} = [0\ 1\ 2\ 2] \tag{13}$$

This method is quite useful for the present scheme, as all the non-zero elements in the ciphertext are 1. So, the vector V contains only one element, whereas RV contains 257 elements. Also, the column vector CV contains 256 elements. So, the compressed, encrypted image has a total of 1 + 257 + 256 = 514 elements, which are far less as compared to the uncompressed encrypted image having a total of 65536 elements.

To evaluate the strength of the compression algorithm used, a metric 'Space Savings' is computed. It is defined in terms of reduction in size with respect to the uncompressed image and is given by:

$$\text{Space Savings} = 1 - \frac{\text{Compressed size}}{\text{Uncompressed size}} \tag{14}$$

In the proposed scheme with input image of size 256 × 256 and compressed image of size 16 × 16, the Space Savings is

$$\text{Space Savings} = 1 - \frac{256}{65536} = 0.9961 \tag{15}$$

which indicates that the compressed image saves 99.61% memory in comparison to the uncompressed encrypted image. This shows that the scheme is suitable for the compression of double images.

After compression, the image is watermarked by first zero-padding it to the image's desired size, and then applying Arnold transform (AT) on it. The resulting image is then combined with the host image $I_{\mathrm{h}}(x, y)$, to give the watermarked image $I_{\mathrm{w}}(x, y)$.

$$I_{\mathrm{w}}(x, y) = \mathrm{AT}(\text{Compressed } E(x, y)) + I_{\mathrm{h}}(x, y) \tag{16}$$

2.2. Watermark extraction, decompression, and decryption process

Figure 2 shows the flowchart followed at the receiver end to retrieve the original image. The process involves watermark extraction followed by the decompression process and the decryption algorithm. All these steps are explained in the following text.

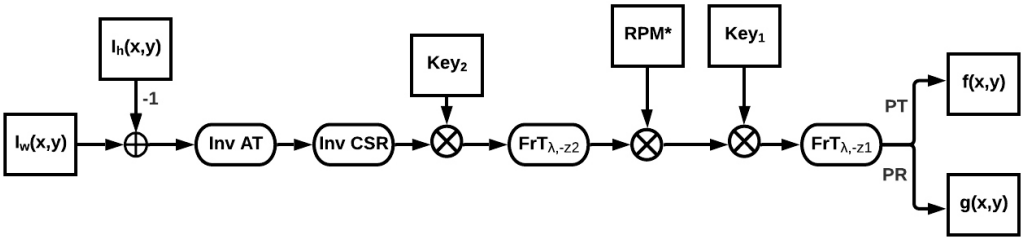

Fig. 2. Decompression and decryption process.

To recover the input image, we first need to extract the host image $I_h(x, y)$ from the watermarked image $I_w(x, y)$ using the equation

$$I(x, y) = I_w(x, y) - I_h(x, y) \tag{17}$$

to give $I(x, y)$, which is inverse Arnold transformed (Inv AT) with the correct parameter to get the compressed encrypted image. Then, it is decompressed using the following algorithm.

The decompression process for CSR format is shown using the vectors V, RV, and CV for matrix A:

$$\mathrm{V} = [a\ b\ c\ d\ ] \tag{18}$$

$$\mathrm{RV} = [0\ 1\ 3\ 4\ 4] \tag{19}$$

$$\mathrm{CV} = [0\ 1\ 2\ 2] \tag{20}$$

To decompress the vector V back into matrix A, first, allocate the rows for the non-zero entries using vector RV. As the first entry in RV is always zero and the second entry tells the number of elements in the 0 row, we will have only one element in the 0 row. The third element in RV represents the number of elements in row 0 and 1, as the 0 row has one element, so 3 indicates two elements in row 1. The next element is 4, which indicates that there is one element in row 2. So, the row allocation for elements is $\{(a), (b, c), (d\ ), (0)\}$. CV arranges values in columns, so we get the vectors $(a,0,0,0)$ $(0,b,c,0)$ $(0,0,d,0)$ $(0,0,0,0)$. These vectors give back the uncompressed encrypted image $E(x, y)$.

For decryption, the following steps are implemented on $E(x, y)$.

$$G(u, v) = \mathrm{FrT}\Big(\mathrm{Key}_2 \times E(x, y)\Big) \tag{21}$$

$$H(x, y) = \mathrm{FrT}\Big(\mathrm{Key}_1 \times \big|G(u, v)\big|\Big) \tag{22}$$

The amplitude and phase part of $H(x, y)$ gives the input images back.

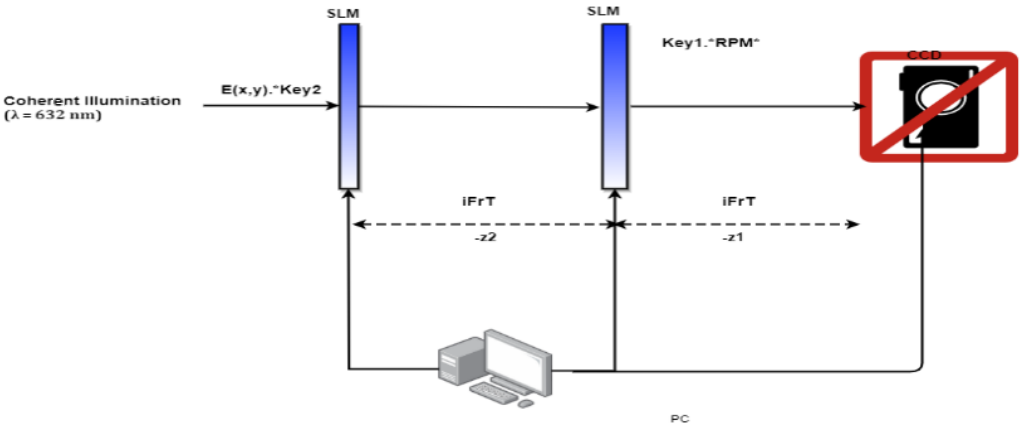

Fig. 3. Optoelectronic setup of the decryption process.

$$f(x, y) = \text{Amplitude}(H(x, y)) \tag{23}$$

$$g(x, y) = \text{Phase}(H(x, y)) \tag{24}$$

The decryption of the images can also be carried out via an optoelectronic setup shown in Fig. 3, where spatial light modulators (SLM) and charge-coupled devices (CCD) allow data transfer between computer and optical systems.

3. Results and discussion

3.1. Validation results and key sensitivity analysis

Scheme validation results are demonstrated in Fig. 4. Results of the decryption show quality of the retrieved images.

Key-sensitivity for an algorithm is a very important aspect of security analysis. The extent of variation in the results, due to changes in the key, determines the key -sensitivity. Thus, to analyze the key-sensitivity, we have obtained decryption results with some incorrect keys. Figure 5 illustrates the retrieved images of *Lena* and *Cam-*

Fig. 4. Scheme validation results: (**a**) input image $g(x, y)$: *Lena*, (**b**) input image $f(x, y)$: *Cameraman*, (**c**) host image $I_h(x, y)$: *Barabara*, (**d**) encrypted image $E(x, y)$, (**e**) compressed encrypted image $I_{ce}(x, y)$, (**f**) watermarked image $I_w(x, y)$, corresponding recovered image $I_{r1}(x, y)$, and (**c**) recovered image $I_{r2}(x, y)$.

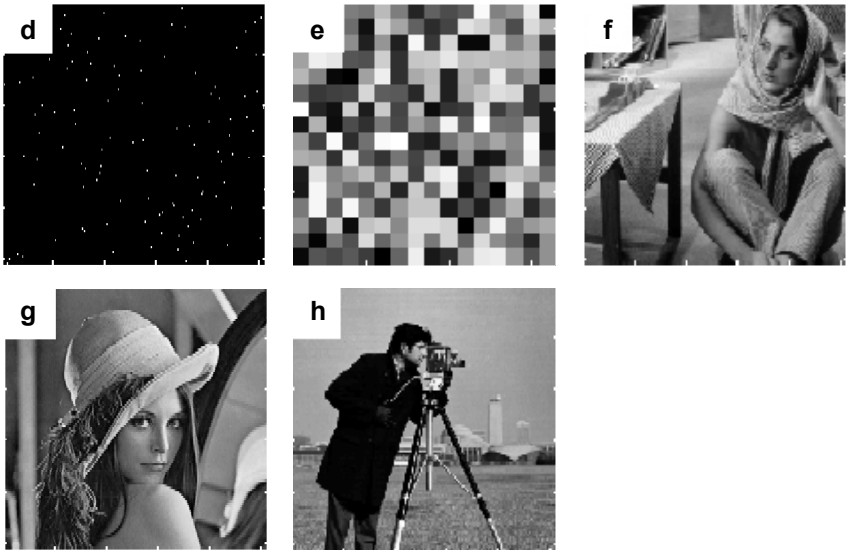

Fig. 4. Continued.

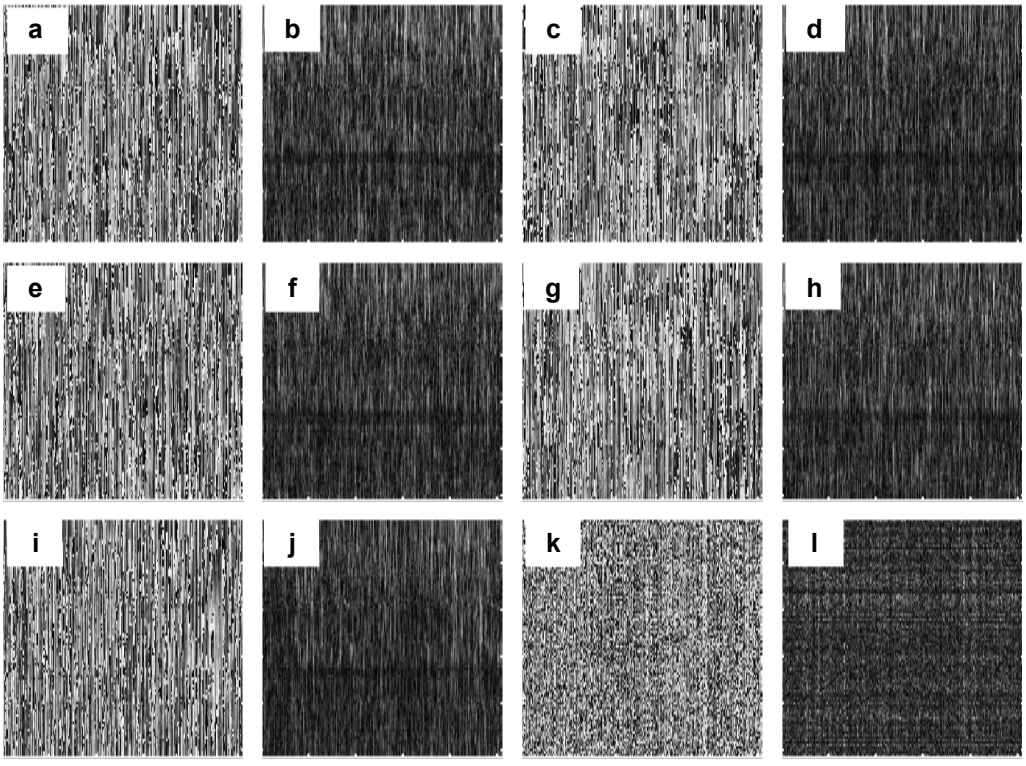

Fig. 5. Key-sensitivity analysis: retrieved images of *Lena* $g_r(x, y)$ and *Cameraman* $f_r(x, y)$ with wrong values of (**a**, **b**) Key_2, (**c**, **d**) L_1, (**e**, **f**) λ, (**g**, **h**) z_2, (**i**, **j**) RPM, and (**k**, **l**) Key_1.

eraman with wrong values of (**a**, **b**) Key_2, (**c**, **d**) L_1, (**e**, **f**) λ, (**g**, **h**) z_2, (**i**, **j**) RPM, and (**k**, **l**) Key_1. As can be seen, both the secret keys and Fresnel parameters should be accurate to retrieve the original images successfully.

3.2. Statistical and robustness analysis

For statistical analysis of the proposed algorithm, a few commonly used metrics such as correlation coefficient (CC), mean-squared-error (MSE) and peak signal-to-noise ratio (PSNR) have been computed between input and recovered images. The computed values of the statistical measures are given in Table 1, and it clearly shows that the scheme is statistically stable.

T a b l e 1. Statistical measures for the input and the recovered images.

Statistical measure	Image *Lena*	Image *Cameraman*
Correlation coefficient	1	1
Mean-squared-error	0	3.7128×10^{-26}
Peak signal-to-noise ratio	634 dB	254.3030 dB

In addition, entropy evaluation and histogram analysis of images are also carried out. Figure 6 shows the histograms for input, encrypted and output images, which clearly indicate robustness of the encryption algorithm. The compressed encrypted image's entropy is 7.9922, which also validates the strength and efficiency of the encryption process deployed.

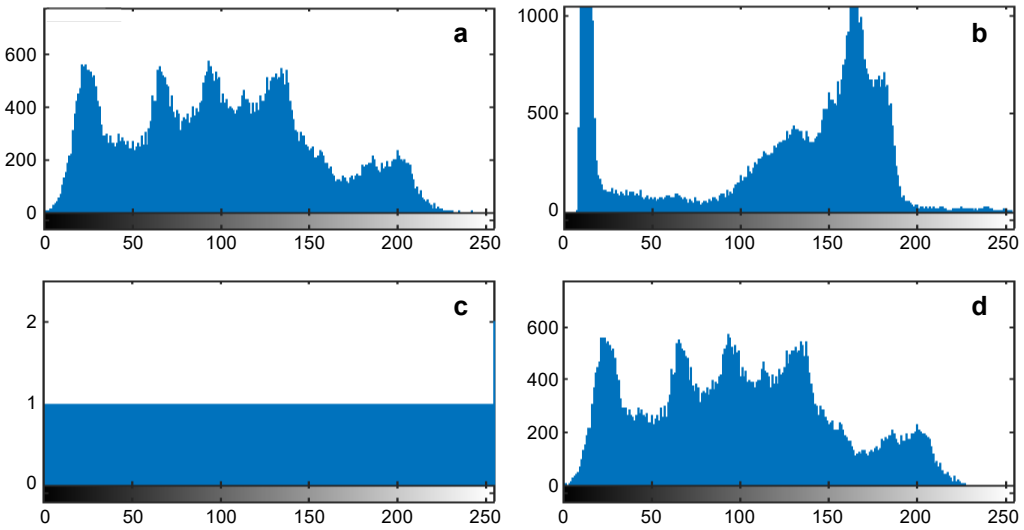

Fig. 6. Histogram plots for (**a**) input image $g(x, y)$: *Lena*, (**b**) input image $f(x, y)$: *Cameraman*, (**c**) compressed encrypted image $I_{ce}(x, y)$, and (**d**) recovered image of *Lena*.

3.3. Occlusion attack analysis

Occlusion attack analysis is also performed on the proposed scheme. To check the firmness of the scheme against occlusion attack, the encrypted image is occluded to 25%, and the corresponding output results are shown in Fig. 7. CC plot against the percentage occluded area for both the images is shown in Fig. 8. The results clearly show the robustness of the scheme against such obstruction attacks as the output images are sufficiently recognizable even after 25% occlusion.

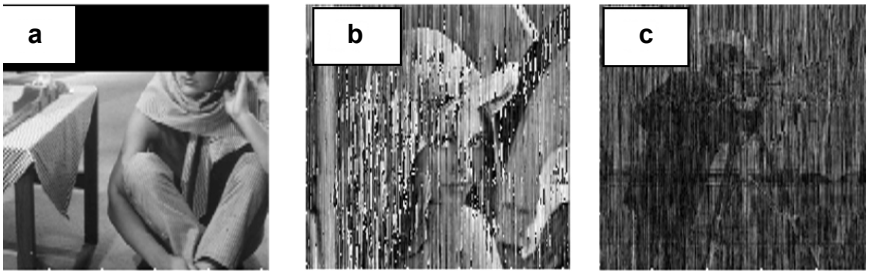

Fig. 7. Occlusion attack analysis: (**a**) occluded watermarked image, (**b**) corresponding recovered image $I_{r1}(x, y)$, and (**c**) recovered image $I_{r2}(x, y)$ with 25% occlusion.

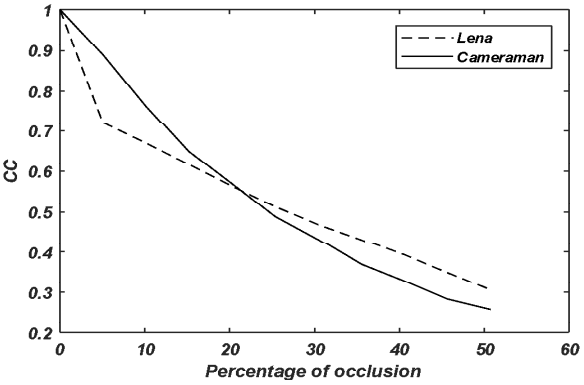

Fig. 8. Plot CC *versus* percentage of occlusion for the recovered images of *Lena* and *Cameraman*.

3.4. Classical attack analysis

Generally, in cryptanalysis, the algorithm and the key domain are public and thus accessible to attackers. This implies that the overall security and robustness of any scheme lie in the strength of the secret key. The proposed mechanism also is not an exception to the above criterion. It should also exhibit resistance to classical attacks like known plaintext, ciphertext only, chosen-plaintext and chosen-ciphertext attacks. Seemingly cho-

T a b l e 1. Comparison analysis of different encryption schemes.

Parameters	GONG *et al.* [29]	SINGH [19]	XU *et al.* [34]	GONG *et al.* [30]	YANG *et al.* [28]	ZHOU *et al.* [35]	Proposed scheme
Transform domain utilized	Discrete fractional random transform	Gyrator	Discrete wavelet domain	Spatial	Spatial	Fourier domain	Fresnel transform
Applied approach	Symmetric	Asymmetric	Symmetric	Symmetric	Symmetric	Asymmetric	Asymmetric
Execution	Digital	Optical or digital	Digital	Digital	Digital	Optoelectronic	Optoelectronic
Substitution techniques	√	√	√	√	√	√	√
Permutation techniques	Hyper chaotic system	×	2D-SLIM hyperchaotic map	Arnold transform & chaotic system	Fractional-order hyper-chaotic system	2D Henon map	×
Compression procedure	DCT	×	Compressive sensing	Compressive sensing	2D compressed sensing	Compressive sensing	Compressed sparse row
Compression ratio/ Space savings ratio	CR = 4	×	CR = 0.75	CR = 1.33	CR = 87.5	–	CR = 256 SSR = 0.9961
Encryption period	–	–	0.05116 for CR = 0.75	>6 secs for image size 256 × 256 (increases with image size)	–	–	0.435884 sec for encryption 0.528438375 sec for compression
PSNR of decrypted image	76.56 dB	310.9292 dB	29 dB	>30 dB	35.8548 dB	33.7034 dB	634 dB
Performance against attacks	Robust against noise attack but can withstand a small degree of occlusion	Robust against occlusion and noise attack to some degree	Robust against known/chosen plaintext, low-intensity noise and minor occlusion	Robust against noise attack but can withstand a small degree of occlusion	Robust against noise attack and occlusion attack	Robust against statistical and differential attack along with noise attack and occlusion attack to some degree	Robust encryption and resistant against occlusion attack

sen-plaintext attack appears to be the most powerful amongst them, and if any cryptosystem can resist this, it will be robust to all. The proposed mechanism is sensitive to the secret keys, and parameters of Fresnel transform and Arnold transform, as demonstrated in scheme validation and key-sensitivity analysis carried out earlier. The ciphertext also shows great sensitivity to the public keys; a random phase mask deployed along with private keys and the mask employed is also arbitrary in nature. All these characteristics make the scheme resistant to known-plaintext attacks.

3.5. Comparison analysis

Comparison analysis of the proposed scheme against similar schemes is done to show its strength and merit in the field of encryption. Table 2 shows a comparative analysis of the proposed scheme by Gong *et al*. [29], Singh [19], Xu *et al*. [34], Gong *et al*. [30], Yang *et al*. [28] and Zhou *et al*. [35]. The comparison is based on transform domain utilized, applied approach, execution, substitution and permutation techniques, compression procedure, compression ratio/space savings, encryption period, PSNR of decrypted image and performance against attacks.

Table 2 demonstrates that the proposed scheme not only extends work in the new domain but also is robust against occlusion as compared to previous schemes. The time taken for encryption is just 0.44 sec whereas for compression it is only 0.53 sec. Moreover, the compression ratio it offers, and the PSNR value of the decrypted image, show its superiority over the existing schemes.

4. Conclusions

A new scheme for encryption, compression, and watermarking based on QR decomposition with column pivoting is introduced in this study. The private keys are obtained by taking the product of orthogonal and triangular matrices resulting from QR factorization. The scheme is sensitive to the Fresnel transform parameters and Arnold transform parameter. We have also shown that the proposed encryption and compression scheme can also be used as a watermarking scheme. The proposed encryption scheme is robust against various attacks. Histogram and key-sensitivity analysis also show strength of the encryption scheme.

References

[1] Refregier P., Javidi B., *Optical image encryption based on input plane and Fourier plane random encoding*, Optics Letters **20**(7), 1995, pp. 767–769, DOI: 10.1364/OL.20.000767.

[2] Chen W., Chen X., *Optical color image encryption based on an asymmetric cryptosystem in the Fresnel domain*, Optics Communications **284**(16–17), 2011, pp. 3913–3917, DOI: 10.1016/j.optcom.2011.04.005.

[3] Joshi M., Shakher C., Singh K., *Image encryption and decryption using fractional Fourier transform and radial Hilbert transform*, Optics and Lasers in Engineering **46**(7), 2008, pp. 522–526, DOI: 10.1016/j.optlaseng.2008.03.001.

[4] Unnikrishnan G., Joseph J., Singh K., *Optical encryption by double-random phase encoding in the fractional Fourier domain*, Optics Letters **25**(12), 2000, pp. 887–889, DOI: 10.1364/OL.25.000887.

[5] HENNELLY B., SHERIDAN J.T., *Optical image encryption by random shifting in fractional Fourier domains*, Optics Letters **28**(4), 2003, pp. 269–271, DOI: 10.1364/OL.28.000269.
[6] LIU Z., CHEN H., LIU T., LI P., XU L., DAI J., LIU S., *Image encryption by using gyrator transform and Arnold transform*, Journal of Electronic Imaging **20**(1), 2011, article 013020, DOI: 10.1117/1.3557790.
[7] ZHOU N., WANG Y., GONG L., *Novel optical image encryption scheme based on fractional Mellin transform*, Optics Communications **284**(13), 2011, pp. 3234–3242, DOI: 10.1016/j.optcom.2011.02.065.
[8] CHEN L., ZHAO D., *Optical image encryption with Hartley transforms*, Optics Letters **31**(23), 2006, pp. 3438–3440, DOI: 10.1364/OL.31.003438.
[9] SINGH P., YADAV A.K., SINGH K., SAINI I., *Optical image encryption in the fractional Hartley domain, using Arnold transform and singular value decomposition*, AIP Conference Proceedings **1802**, 2017, article 020017, DOI: 10.1063/1.4973267.
[10] MEHRA I., NISHCHAL N.K., *Image fusion using wavelet transform and its application to asymmetric cryptosystem and hiding*, Optics Express **22**(5), 2014, pp. 5474–5482, DOI: 10.1364/OE.22.005474.
[11] ABUTURAB M.R., *Group multiple-image encoding and watermarking using coupled logistic maps and gyrator wavelet transform*, Journal of the Optical Society of America A **32**(10), 2015, pp. 1811–1820, DOI: 10.1364/JOSAA.32.001811.
[12] QIN W., PENG X., *Asymmetric cryptosystem based on phase-truncated Fourier transforms*, Optics Letters **35**(2), 2010, pp. 118–120, DOI: 10.1364/OL.35.000118.
[13] KUMAR R., QUAN C., *Asymmetric multi-user optical cryptosystem based on polar decomposition and Shearlet transform*, Optics Communications **120**, 2019, pp. 118–126, DOI: 10.1016/j.optlaseng.2019.03.024.
[14] CHEN J., ZHU Z., LIU Z., FU C., ZHANG L., YU H., *A novel double-image encryption scheme based on cross-image pixel scrambling in gyrator domains*, Optics Express **22**(6), 2014, pp. 7349–7361, DOI: 10.1364/OE.22.007349.
[15] KUMAR R., SHERIDAN J.T., BHADURI B., *Nonlinear double image encryption using 2D non-separable linear canonical transform and phase retrieval algorithm*, Optics & Laser Technology **107**, 2018, pp. 353–360, DOI: 10.1016/j.optlastec.2018.06.014.
[16] LI H., WANG Y., *Double-image encryption based on discrete fractional random transform and chaotic maps*, Optics and Lasers in Engineering **49**(7), 2011, pp. 753–757, DOI: 10.1016/j.optlaseng.2011.03.017.
[17] LIU Z., GONG M., DOU Y., LIU F., LIN S., ASHFAQ AHMAD M., DAI J., LIU S., *Double image encryption by using Arnold transform and discrete fractional angular transform*, Optics and Lasers in Engineering **50**(2), 2012, pp. 248–255, DOI: 10.1016/j.optlaseng.2011.08.006.
[18] LIU Z., GUO Q., XU L., ASHFAQ AHMAD M., LIU S., *Double image encryption by using iterative random binary encoding in gyrator domains*, Optics Express **18**(11), 2010, pp. 12033–12043, DOI: 10.1364/OE.18.012033.
[19] SINGH H., *Hybrid structured phase mask in frequency plane for optical double image encryption in gyrator transform domain*, Journal of Modern Optics **65**(18), 2018, pp. 2065–2078, DOI: 10.1080/09500340.2018.1496286.
[20] SUI L., LU H., WANG Z., SUN Q., *Double-image encryption using discrete fractional random transform and logistic maps*, Optics and Lasers in Engineering **56**, 2014, pp. 1–12, DOI: 10.1016/j.optlaseng.2013.12.001.
[21] TAO R., XIN Y., WANG Y., *Double image encryption based on random phase encoding in the fractional Fourier domain*, Optics Express **15**(24), 2007, pp. 16067–16079, DOI: 10.1364/OE.15.016067.
[22] CARNICER A., MONTES-USATEGUI M., ARCOS S., JUVELLS I., *Vulnerability to chosen-cyphertext attacks of optical encryption schemes based on double random phase keys*, Optics Letters **30**(13), 2005, pp. 1644–1646, DOI: 10.1364/OL.30.001644.
[23] SINGH P., KUMAR R., YADAV A.K., SINGH K., *Security analysis and modified attack algorithms for a nonlinear optical cryptosystem based on DRPE*, Optics and Lasers in Engineering **139**, 2021, article 106509, DOI: 10.1016/j.optlaseng.2020.106501.

[24] JIAO S., LI G., ZHOU C., ZOU W., LI X., *Special ciphertext-only attack to double random phase encryption by plaintext shifting with speckle correlation*, Journal of the Optical Society of America A **35**(1), 2018, pp. A1–A6, DOI: 10.1364/JOSAA.35.0000A1.

[25] PENG X., ZHANG P., WEI H., YU B., *Known-plaintext attack on optical encryption based on double random phase keys*, Optics Letters **31**(8), 2006, pp. 1044–1046, DOI: 10.1364/OL.31.001044.

[26] WANG X., ZHAO D., *A special attack on the asymmetric cryptosystem based on phase-truncated Fourier transforms*, Optics Communications **285**(6), 2012, pp. 1078–1081, DOI: 10.1016/j.optcom.2011.12.017.

[27] KUMARI E., MUKHERJEE S., SINGH P., KUMAR R., *Asymmetric color image encryption and compression based on discrete cosine transform in Fresnel domain*, Results in Optics **1**, 2020, article 100005, DOI: 10.1016/j.rio.2020.100005.

[28] YANG Y.-G., GUAN B.-W., LI J., LI D., ZHOU Y.-H., SHI W.-M., *Image compression-encryption scheme based on fractional order hyper-chaotic systems combined with 2D compressed sensing and DNA encoding*, Optics & Laser Technology **119**, 2019, article 105661, DOI: 10.1016/j.optlastec.2019.105661.

[29] GONG L., DENG C., PAN S., ZHOU N., *Image compression-encryption algorithms by combining hyper-chaotic system with discrete fractional random transform*, Optics & Laser Technology **103**, 2018, pp. 48–58, DOI: 10.1016/j.optlastec.2018.01.007.

[30] GONG L., QIU K., DENG C., ZHOU N., *An image compression and encryption algorithm based on chaotic system and compressive sensing*, Optics & Laser Technology **115**, 2019, pp. 257–267, DOI: 10.1016/j.optlastec.2019.01.039.

[31] BOUKARAM W.H., TURKIYYAH G., LTAIEF H., KEYES D.E., *Batched QR and SVD algorithms on GPUs with applications in hierarchical matrix compression*, Parallel Computing **74**, 2018, pp. 19–33, DOI: 10.1016/j.parco.2017.09.001.

[32] SU Q., NIU Y., WANG G., JIA S., YUE J., *Color image blind watermarking scheme based on QR decomposition*, Signal Processing **94**, 2014, pp. 219–235, DOI: 10.1016/j.sigpro.2013.06.025.

[33] BULUC A., FINEMAN J.T., FRIGO M., GILBERT J.R., LEISERSON C.E., *Parallel sparse matrix-vector and matrix-transpose-vector multiplication using compressed sparse blocks*, SPAA, 2009, pp. 233–244, DOI: 10.1145/1583991.1584053.

[34] XU Q., SUN K., CAO C., ZHU C., *A fast image encryption algorithm based on compressive sensing and hyperchaotic map*, Optics and Lasers in Engineering **121**, 2019, pp. 203–214, DOI: 10.1016/j.optlaseng.2019.04.011.

[35] ZHOU K., FAN J., FAN H., LI M., *Secure image encryption scheme using double random-phase encoding and compressed sensing*, Optics & Laser Technology **121**, 2020, article 105769, DOI: 10.1016/j.optlastec.2019.105769.

Received January 6, 2021
in revised form March 13, 2021