Optica Applicata, Vol. LII, No. 3, 2022
DOI: 10.37190/oa220303

Audio and image encryption scheme based on QR decomposition and random modulus decomposition in Fresnel domain

SAVITA ANJANA[1*], AK YADAV[2], PHOOL SINGH[2], HUKUM SINGH[1]

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

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

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

In this paper, an asymmetric audio and image encryption mechanism using QR decomposition and random modulus decomposition (RD) in the Fresnel domain is proposed. The audio file is recorded as a vector and converted to a two-dimensional array to act as an image or a sound map. This sound map is encrypted using the image encryption algorithm proposed in this paper. The proposed cryptosystem is validated for both audios and grayscale images. Fresnel parameters and the two private keys obtained from QR decomposition and random modulus decomposition (RD) form the key space. Computer-based reproductions have been carried out to prove the validity and authenticity of the scheme. Simulation results authenticate that the scheme is robust and efficient against various attacks and is sensitive to input parameters.

Keywords: QR decomposition, audio encryption, random modulus decomposition.

1. Introduction

As the rate of digital media transmission increases, issues of privacy and identity theft also increase; thus, encryption plays an essential role in ensuring digital media is transmitted securely. Over the years, various audio and image encryption schemes have been developed. Each of them has its strengths and weaknesses. However, when it comes to audio encryption using conventional image encryption techniques, we still have a lot to explore. Voice data is widely used as audio evidence in courts, biometric, secret business talks and other related fields, so it becomes essential to secure it against intruders. Since we can record an audio file as a 2-D array just like an image, we can apply image encryption algorithms on audio files as well. One such approach was presented by RAJPUT and MATOBA [1], in which they recorded human voices as holograms and en-

crypted them directly using double random phase encoding (DRPE). Similarly, YANG *et al*. [2] proposed a quantum encryption scheme which was also a generalization of the DRPE scheme in quantum scenarios. Many other audio encryption schemes using chaotic baker map [3], virtual optics scheme [4], a mixture of chaos function [5], cosine number transform[6], and Arnold transform with random decomposition [7] were proposed. These schemes are generalizations of image encryption to audio files. Digital and optical image encryptions have been performed by many different algorithms like DRPE [8], which uses the same keys for encryption and decryption, fractional Fourier transform-based DRPE [9] by UNNIKRISHNAN and SINGH, asymmetric cryptosystem by QIN and PENG [10], Fresnel transform based schemes [11–17], radial Hilbert transform [18], equal modulus decomposition (EMD) and random modulus decomposition (RD) based cryptosystems [7, 12, 14, 19–21], gyrator wavelet transform [13], chaotic logistic map[22], fractional Mellin transform [23], 3D-Lorenz chaotic system [24], Lorenz-chaos and exclusive-OR [25], 3D-bit matrix [26], hyperchaotic system and RD based cryptosystems [20]. Researchers also carried out cryptoanalysis of various schemes [27–30], and one such work [21] shows that the random modulus decomposition-based image encryption has the edge over EMD based cryptosystems as the latter one was found to be vulnerable to an iteration-based attack.

Various image decomposition techniques or matrix decomposition methods such as LU and QR decomposition *etc*., are available in mathematics, and many encryption techniques have been developed using them [31–34]. One such cryptosystem was given by ABUTURAB [34] using LU decomposition in the gyrator domain for colour images. Some other cryptosystems using QR decomposition are also presented [32, 33]. These decomposition techniques give sparse matrices, which are quite space-saving. Here, we are presenting an audio and image encryption scheme based on QR and random modulus decomposition in the Fresnel domain. This cryptosystem is validated for both audio and grayscale image files and owns a large key space as there are "six" Fresnel transform parameters, "three" for each Fresnel transform. Also, "two" private keys obtained by RD and QR decomposition are essential to decrypt the data successfully. Thus, the scheme is secure enough against brute force attack. Additionally, classical attack analysis and noise attack analysis are also carried out to determine the strength of the proposed encryption scheme. The cryptosystem is analyzed by 3D graphs, histograms, and statistical parameters. All these results indicate the efficacy and strength of the proposed encryption scheme.

The rest of the paper is organized as follows; Section 2 explains the proposed scheme. Section 3 comprises simulation results obtained in MATLAB and a detailed discussion on the efficacy and robustness of the proposed scheme, and finally, Section 4 concludes the study.

2. The proposed algorithm

Figure 1 gives the stepwise depiction of the encryption process of the proposed cryptosystem. Here, the audio files is first converted into a 2-D sound map, just like an im-

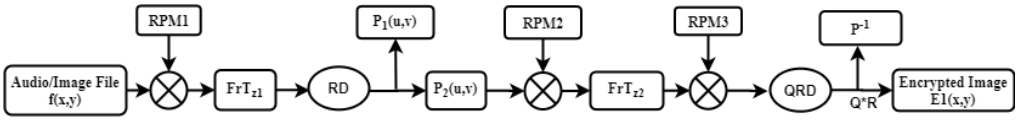

Fig. 1. Schematic flowchart of the encryption process.

age. Then, this sound map is multiplied with RPM1. Thereafter, it is subjected to Fresnel transform (FrT_{z1}) followed by random modulus decomposition (RD) to give a complex-valued private key $P_1(u, v)$ and a decomposed image $P_2(u, v)$. The decomposed image $P_2(u, v)$ is subjected to RPM2 followed by Fresnel transform (FrT_{z2}). The transformed image P_{11} is again multiplied with RPM3 and subjected to QR decomposition to give another private key and encrypted image.

2.1. Encryption process

Step-1

For audio files, the encryption process starts with the conversion of audio vector $V \times 1$ into a 2-D sound map of size $M \times N$. Then, this sound map or the input image is multiplied with a random phase mask $\mathrm{RPM1} = \exp\{2\pi i m(x, y)\}$, followed by Fresnel transform (FrT_{z1}).

$$E(x, y) = \mathrm{FrT}_{z1}(f(x, y) \times \mathrm{RPM1}) \tag{1}$$

Step-2

The Fresnel transformed image $E(x, y)$ is then subjected to random decomposition to give a private key $P_1(u, v)$, and a complex-valued decomposed image $P_2(u, v)$.

$$P_1(u, v) = \frac{M_1(u, v)\sin(b_1(u, v))}{\sin[a_1(u, v) + b_1(u, v)]} \exp\{-i[a_1(u, v) - \Phi_1(u, v)]\} \tag{2}$$

$$P_2(u, v) = \frac{M_1(u, v)\sin(a_1(u, v))}{\sin[a_1(u, v) + b_1(u, v)]} \exp\{-i[b_1(u, v) + \Phi_1(u, v)]\} \tag{3}$$

where, $a_1(u, v) = 2\pi\,\mathrm{rand}(u, v)$, $b_1(u, v) = 2\pi\,\mathrm{rand}(u, v)$, $M_1(u, v) = |E|$, $\Phi_1(u, v) = \arg\{E\}$.

Step-3

In the next step, $P_2(u, v)$ is multiplied with another random phase mask, $\mathrm{RPM2} = \exp\{2\pi i n(x, y)\}$ and subjected to Fresnel transform again (FrT_{z2}).

$$P_{11}(x, y) = \mathrm{FrT}_{z2}(P_2(u, v) \times \mathrm{RPM2}) \tag{4}$$

Step-4

In the final step, $P_{11}(x, y)$ is multiplied with another random phase mask $\mathrm{RPM3} = \exp\{2\pi i t(x, y)\}$ and subjected to QR decomposition to give the encrypted image $E_1(x, y)$ and another private key P^{-1}.

$$[Q\ R\ P] = \mathrm{QR}(P_{11}(x, y) \times \mathrm{RPM3}) \tag{5}$$

where the encrypted image $E_1(x, y)$ is given by $E_1(x, y) = Q \times R$ and key is given by the inverse of the permutation matrix P, *i.e.*, P^{-1}.

2.2. Decryption process

For decryption, we will follow the reverse steps of the encryption process. Figure 2 gives the schematic diagram for the decryption process, and all the steps involved in getting back the original image are explained as follows.

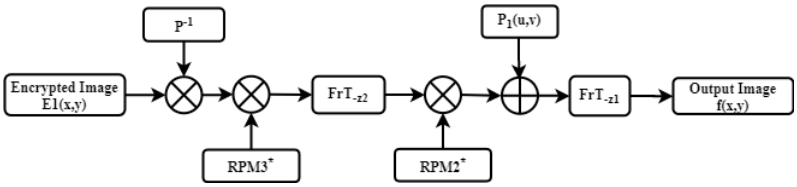

Fig. 2. Schematic flowchart of the decryption process.

Step-1
The encrypted image or encrypted audio file $E_1(x, y)$ is first multiplied with the key P^{-1} and then multiplied with the conjugate of RPM3 followed by Fresnel transform with propagation distance $-z_2$ to give $\mathrm{Pr}_{11}(x, y)$.

$$\mathrm{Pr}_{11}(x, y) = \mathrm{FrT}\{(P^{-1} \times E_1(x, y)) \times \mathrm{RPM3}^*\} \tag{6}$$

Step-2
The intermediate image $\mathrm{Pr}_{11}(x, y)$ is then multiplied with the conjugate of RPM2 and added the key $P_1(u, v)$. After that it is subjected to Fresnel transform again with propagation distance $-z_1$.

$$E_r(x, y) = \mathrm{FrT}\{P_1(u, v) + (\mathrm{Pr}_{11}(x, y) \times \mathrm{RPM2}^*)\} \tag{7}$$

Step-3
At the final step, the absolute or amplitude part is taken to get the decrypted image or decrypted sound map. This sound map is then converted back into the audio vector.

$$f(x, y) = \mathrm{abs}(E_r(x, y)) \tag{8}$$

2.3. Optical setup

The decryption process can be carried out via an optoelectronic setup, as shown in Fig. 3. The communication between a computer and the optical system will be carried out with the help of the spatial light modulator (SLM) and charge-coupled device (CCD). For decryption, the encrypted image or encrypted audio file is first multiplied with the key P^{-1} and then with the conjugate of RPM3, after that it is transferred from

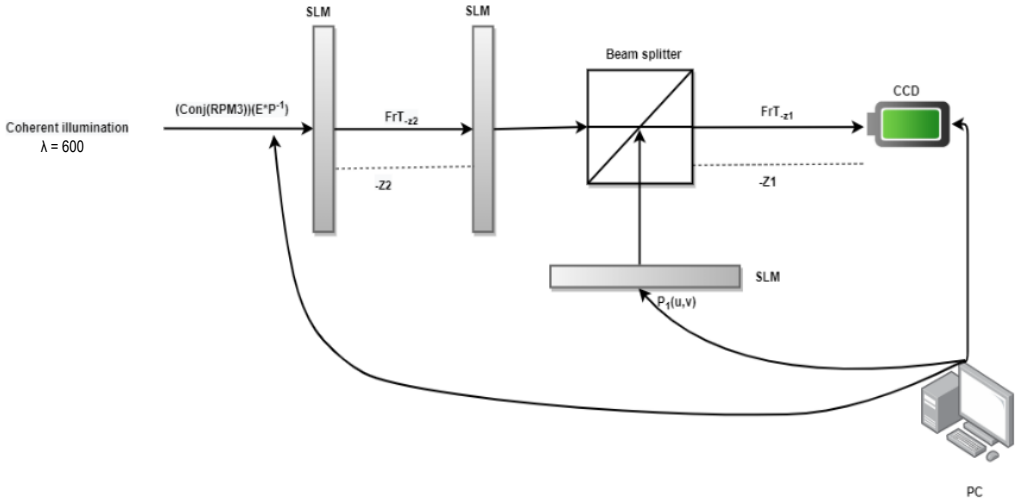

Fig. 3. Optoelectronic setup for the decryption process.

the computer to the setup as shown in the diagram. Then, it is subjected to Fresnel transform. The next steps include the multiplication with the conjugate of RPM2 and the application of beam splitter to carry out the reverse random modulus decomposition. In the final steps, the image passes through the Fresnel transform domain again. The decrypted image is then captured with the help of CCD and stored in the system.

3. Results and discussion

3.1. Validation results and key sensitivity analysis

The proposed encryption scheme is implemented on a wave file of size 65536 × 1 and an input image of size 512 × 512 pixels. Figure 4(**a**–**c**) show the input audio signal, corresponding sound map and input *Boat* image, respectively. After applying the en-

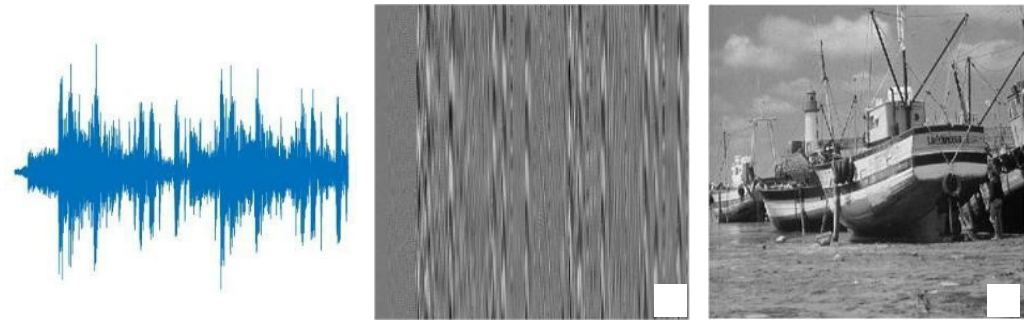

Fig. 4. Scheme validation results: (**a**–**c**) shows the input audio signal, corresponding sound map and input *Boat* image, (**d**–**e**) encrypted sound map and encrypted *Boat* image, (**f**–**h**) decrypted audio signal, decrypted sound map and decrypted *Boat* image, (**i**–**j**) shows the keys respectively.

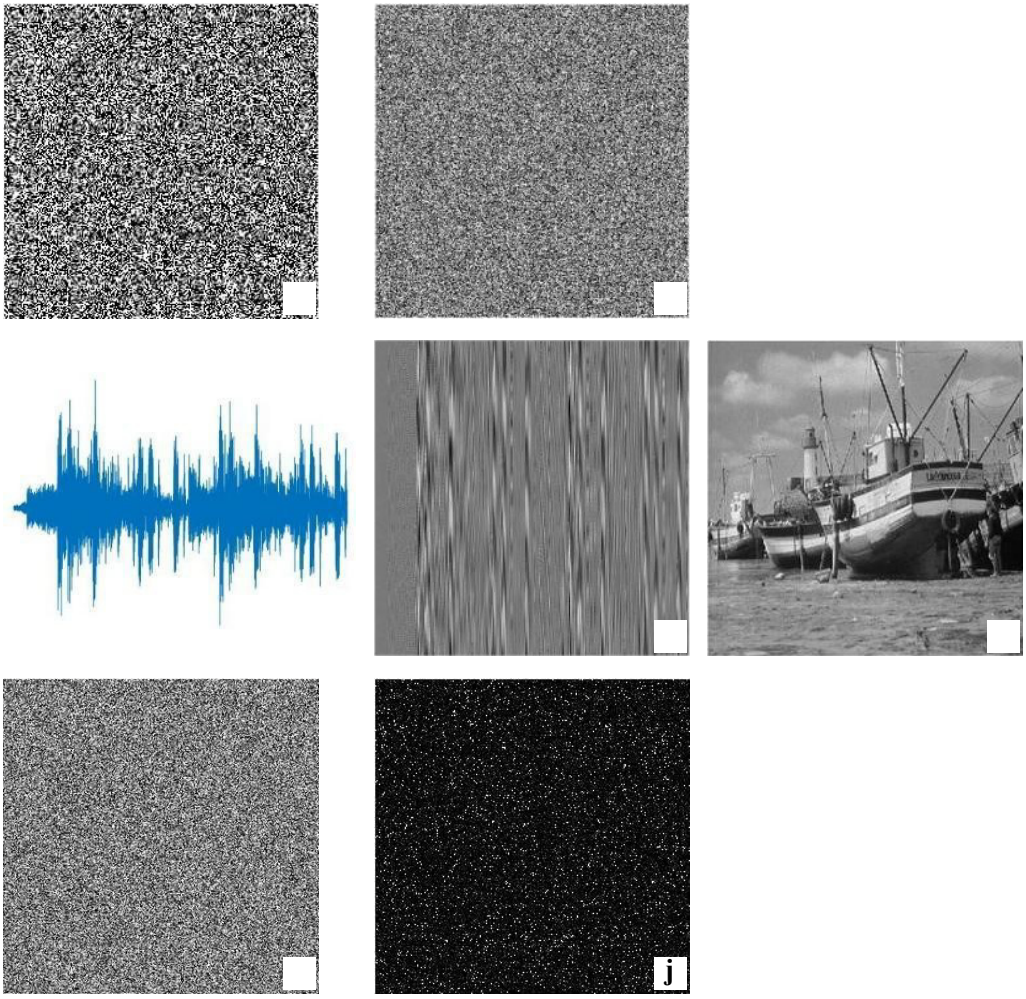

Fig. 4. Continued.

cryption algorithm, we obtained the encrypted sound map and encrypted image in Fig. 4(**d**–**e**). Figure 4(**f**–**h**) show the decrypted audio signal, decrypted sound map and decrypted *Boat* image, respectively. Figure 4(**i**–**j**) give the keys $P_1(u, v)$ and P^{-1}, respectively. The quality of the retrieved images and the audio signal have validated the proposed encryption scheme. The order in which keys are multiplied with the images matters as all matrices do not follow the commutative property. Thus, the order of multiplication of P^{-1} with the image should be correct in order to get the desired output.

3.2. Key sensitivity analysis

The key sensitivity of an algorithm determines its strength. Higher the sensitivity displayed by an algorithm for a small change in the key, the more secure it is against var-

ious attacks. In a secure cryptosystem, a small variation in parameter values yields major deviations from the correct results. So, to test the key sensitivity, we have obtained results with some incorrect parameters of Fresnel transform and incorrect keys,

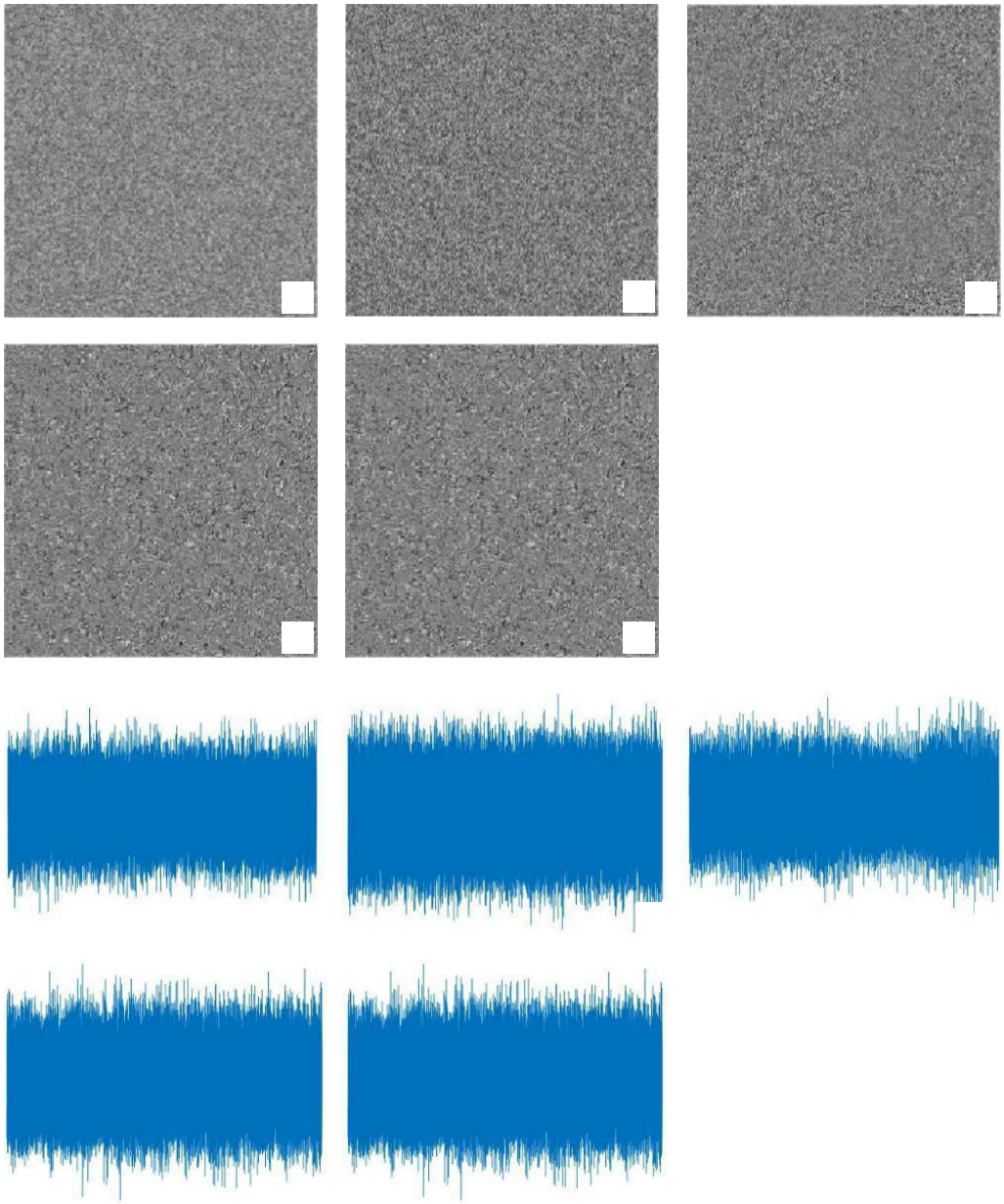

Fig. 5. Decryption results with the wrong values of (**a**–**e**) $P_1(u, v)$, P^{-1}, λ, z_1 and z_2, respectively for sound map, (**f**–**j**) wrong values of $P_1(u, v)$, P^{-1}, λ, z_1 and z_2, respectively for Audio file, (**k**–**o**) wrong values of $P_1(u, v)$, P^{-1}, λ, z_1 and z_2, respectively for *Boat* image.

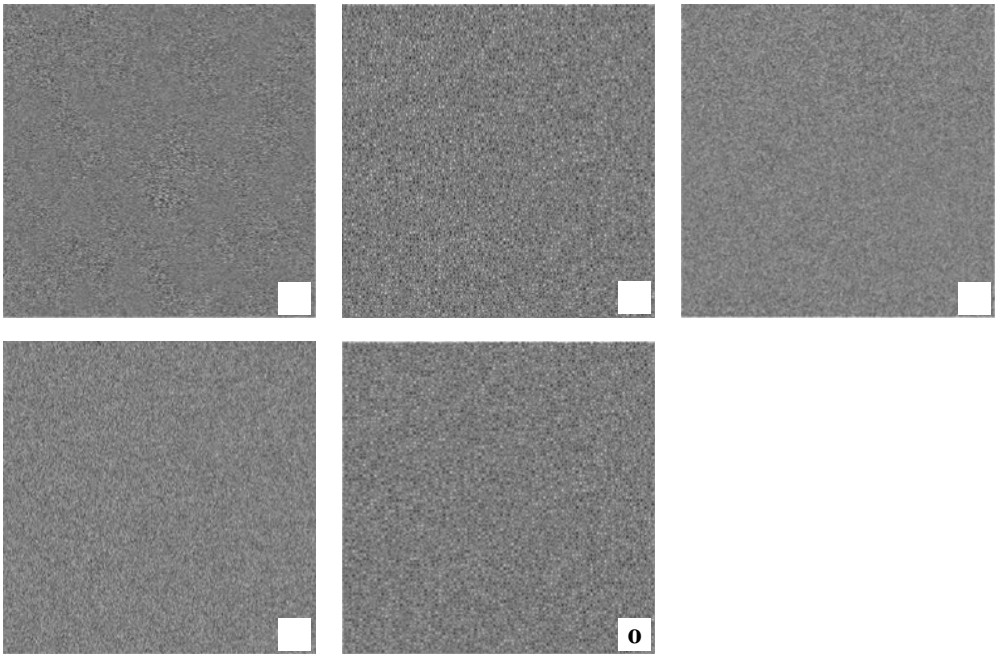

Fig. 5. Continued.

$P_1(u, v)$ and P^{-1}. The correct values of the Fresnel parameter are $\lambda = 600$ nm, $z_1 = 20$ cm, $z_2 = 30$ cm. The incorrect values of these parameters taken for analysis are $\lambda = 610$ nm, $z_1 = 25$ cm, $z_2 = 25$ cm. Figure 5(**a**–**e**) shows the decrypted audio image or sound map with the wrong values of $P_1(u, v)$, P^{-1}, λ, z_1 and z_2, respectively. Figure 5(**f**–**j**) shows the output results for an audio signal with incorrect values of $P_1(u, v)$, P^{-1}, λ, z_1 and z_2, respectively. Figure 5(**k**–**o**) shows the output results for *Boat* image with incorrect values of $P_1(u, v)$, P^{-1}, λ, z_1 and z_2, respectively. It can be easily seen that both the keys

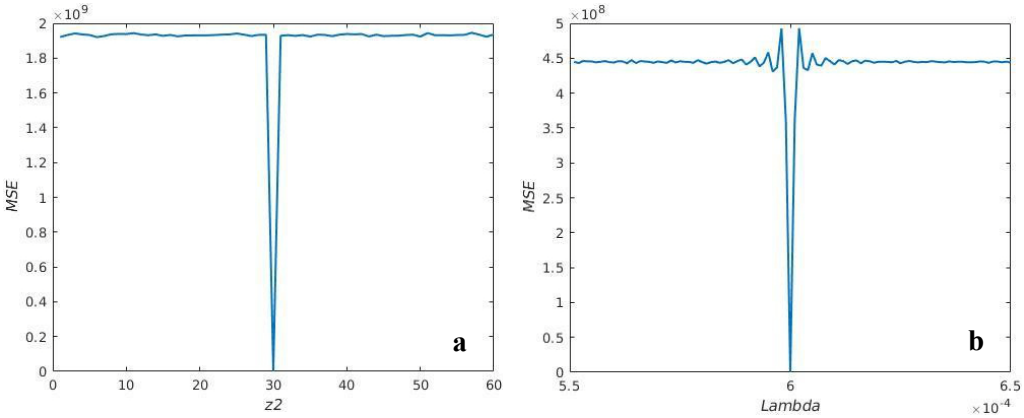

Fig. 6. Plots of MSE *versus* Fresnel transform parameters z_2 (**a**) and λ (**b**).

and the Fresnel parameters should be correct to retrieve the original image or audio file. Thus, the proposed enciphering scheme is sensitive to the decryption keys. The sensitivity is further displayed in Fig. 6(**a**–**b**), which shows the plots of MSE *versus* Fresnel parameters.

3.3. Statistical and robustness analysis

In order to statistically analyse the performance of the given algorithm, correlation coefficient (CC) [35], mean-squared-error (MSE) and peak signal-to-noise ratio (PSNR) [36] have been calculated between the input and the corresponding output images. Entropy is calculated for the encrypted image to check the randomness. The results obtained show that the encryption scheme is secure and efficient for audio and image encryption. Mathematical expressions for these statistical parameters are as follows:

$$\mathrm{CC} = \frac{\mathrm{cov}(E, E_1)}{\sigma(E)\,\sigma(E_1)} \tag{9}$$

$$\mathrm{MSE} = \frac{1}{M \times N} \sum_{x=1}^{M} \sum_{y=1}^{N} \left| E(x, y) - E_1(x, y) \right|^2 \tag{10}$$

$$\mathrm{PSNR} = 10 \log_{10} \frac{255^2}{\mathrm{MSE}} \tag{11}$$

For source m,

$$\mathrm{Entropy} = \sum_{l=1}^{256} P(m_l) \log_2 \frac{1}{P(m_l)} \tag{12}$$

where cov denotes covariance, σ is the standard deviation, E and E_1 represent input and retrieved images of size $M \times N$, respectively. $P(m_l)$ denotes the probability of m_l. The values of CC, MSE, PSNR and entropy for both audio signal and *Boat* image are shown in Table 1. These values depict the strength of the cryptosystem. In addition to these metrics, Figs. 7 and 8 show histograms and 3D plots, respectively, of the input, encrypted and output audio and images. Uniform distribution as seen in histograms and 3D plots of the encrypted image and encrypted sound map indicates that the encryption is carried out efficiently. On the other hand, histograms and 3D plots of the

T a b l e 1. Values of CC, MSE, PSNR and entropy.

Statistical parameter	Audio signal/sound map	Image *Boat*
Correlation coefficient	1	1
Mean squared error	1.5414×10^{-28}	2.3885×10^{-21}
Peak signal-to-noise ratio	278.1208	206.2188
Entropy of encrypted file	4.6373	7.9979

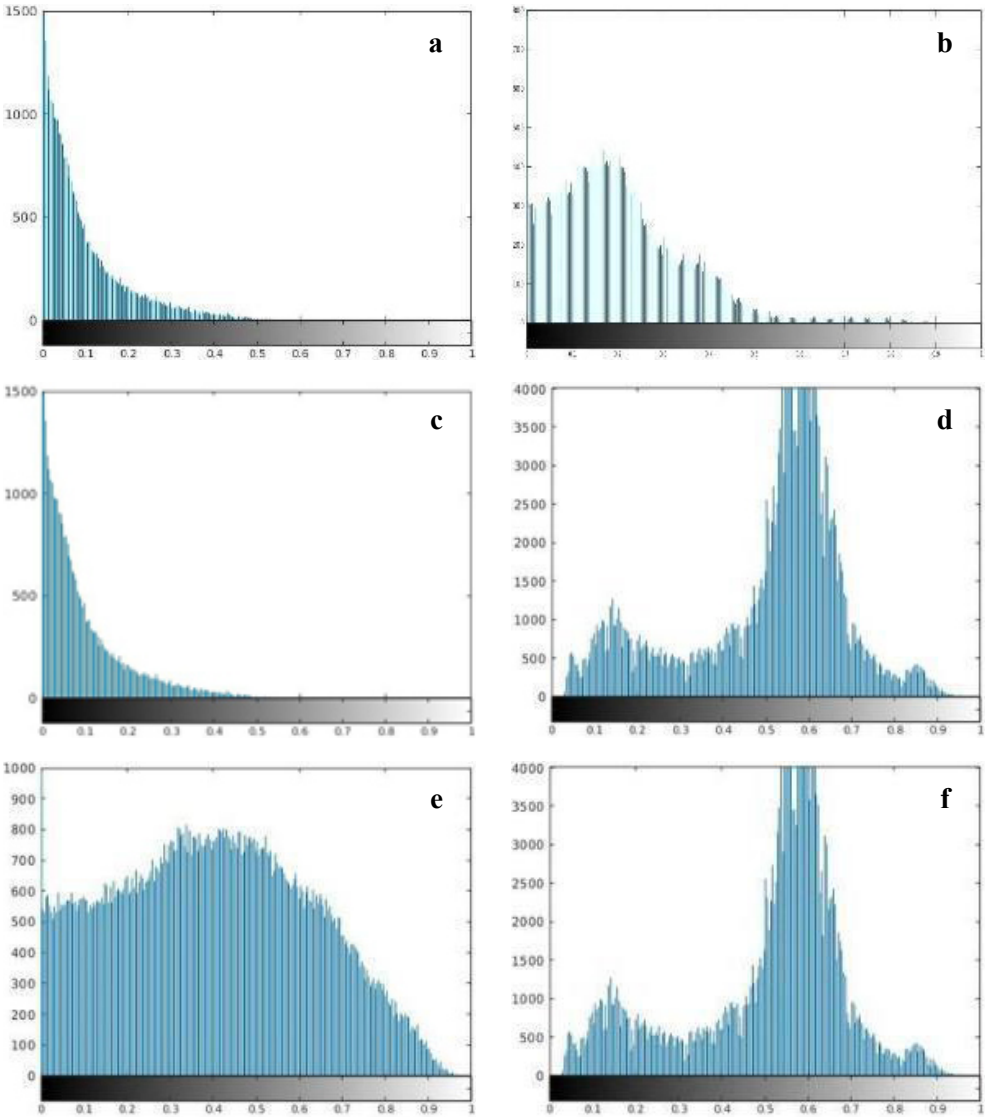

Fig. 7. Histograms of (**a**–**c**) input, encrypted and decrypted sound map and (**d**–**e**) input, encrypted and decrypted *Boat* image respectively.

decrypted files show that the original image and the sound map are faithfully recovered as they resemble completely with the histograms and 3D plots of the corresponding input files.

3.4. Classical attack analysis

The security of a cryptosystem is determined by its resistance against four basic attacks, which are ciphertext only attack, known plaintext attack, chosen plaintext attack, cho-

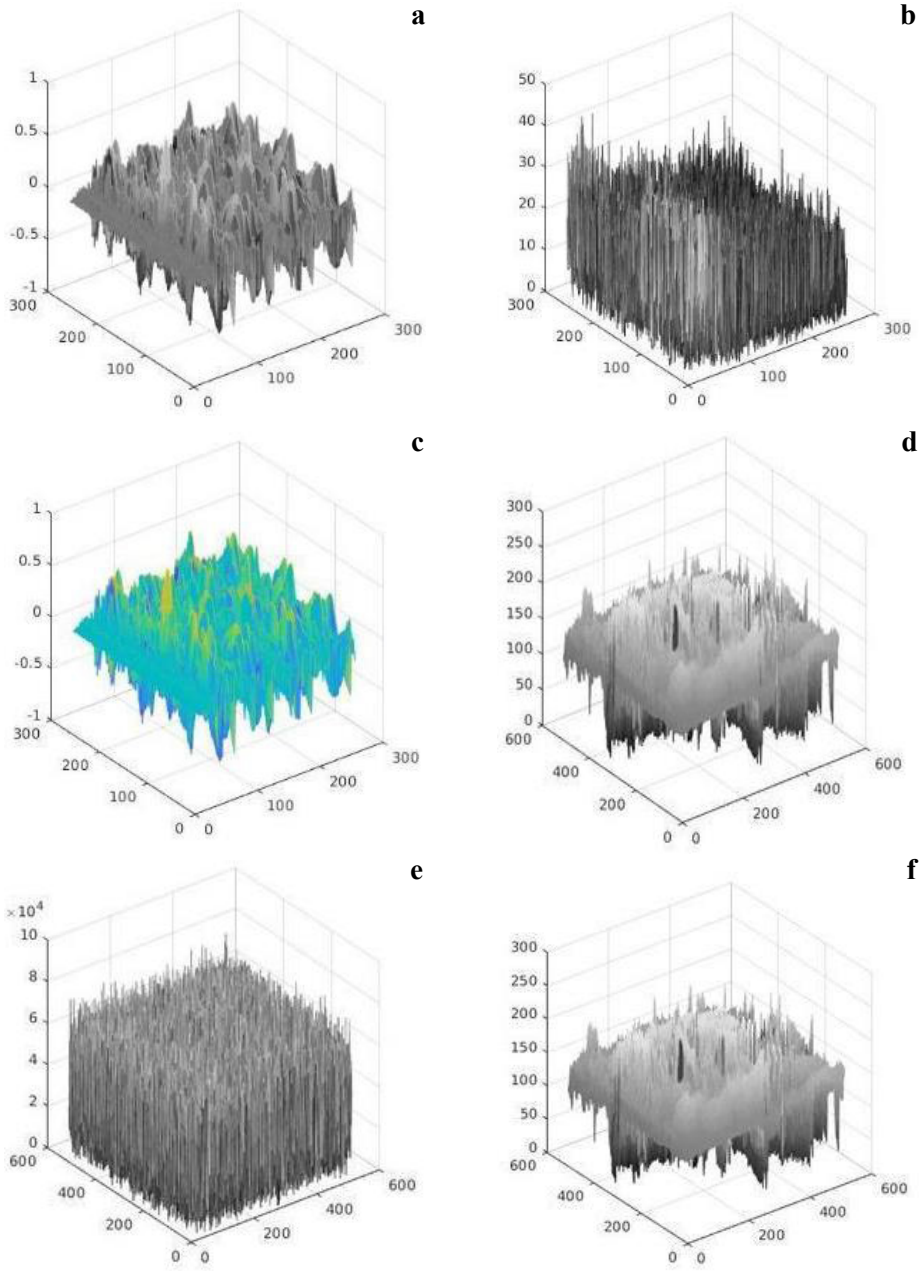

Fig. 8. 3-D plots of (**a**–**c**) input, encrypted and decrypted sound map and (**d**–**e**) input, encrypted and decrypted *Boat* image respectively.

sen ciphertext attack. Among these, chosen plaintext attack is the most powerful one. If a cryptosystem is secure against this attack, it is secure against the other three attacks also. The proposed scheme has six keys, one from random decomposition (RD), one

from QR decomposition and four from two Fresnel transforms implemented in the proposed algorithm. The scheme is highly sensitive to all these parameters. If a small change is made in these parameters, the results would be completely different. Also, QR and random decomposition (RD) of a different image would be different, and thus the key would not be the same. So, the proposed scheme is secure enough against chosen plaintext attack and hence against other classical attacks, too.

3.5. Noise attack analysis

An encryption scheme must be resistant to different noises, which may alter the data during transmission or recording. To check the resistance of the proposed algorithm against noise, Gaussian noise G with mean value zero, standard deviation 1 and strength a is added to the encrypted data E.

$$E' = E + aG \tag{13}$$

The values of a are taken to be different for the audio file and *Boat* image because, in the image, pixel values range from 0 to 255, and the values for the audio vector vary from –0.7522 to 0.8195. The decrypted audio file and sound map corresponding to a = 0.1, 0.2 and 0.25, respectively, are shown in Fig. 9(**a**–**c**, **d**–**f**). Similarly, for a = 25,

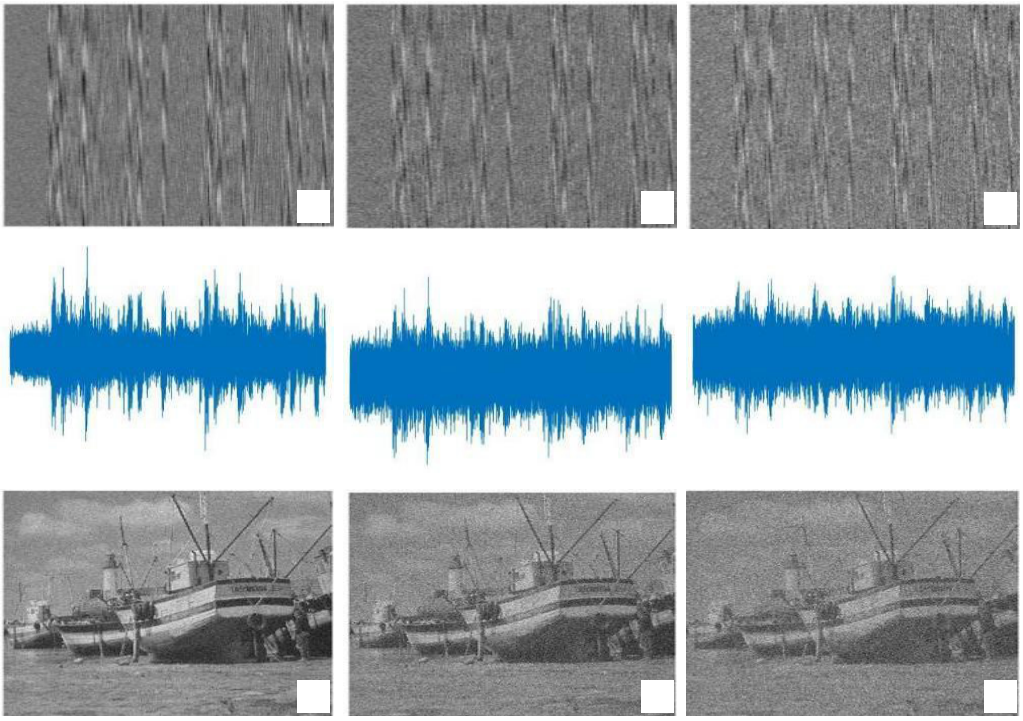

Fig. 9. (**a**–**f**) Noise results with intensities a = 0.1, 0.2, 0.25 for sound map and audio file, respectively (**g**–**i**) decrypted *Boat* image with noise intensities a = 25, 50, 75, respectively.

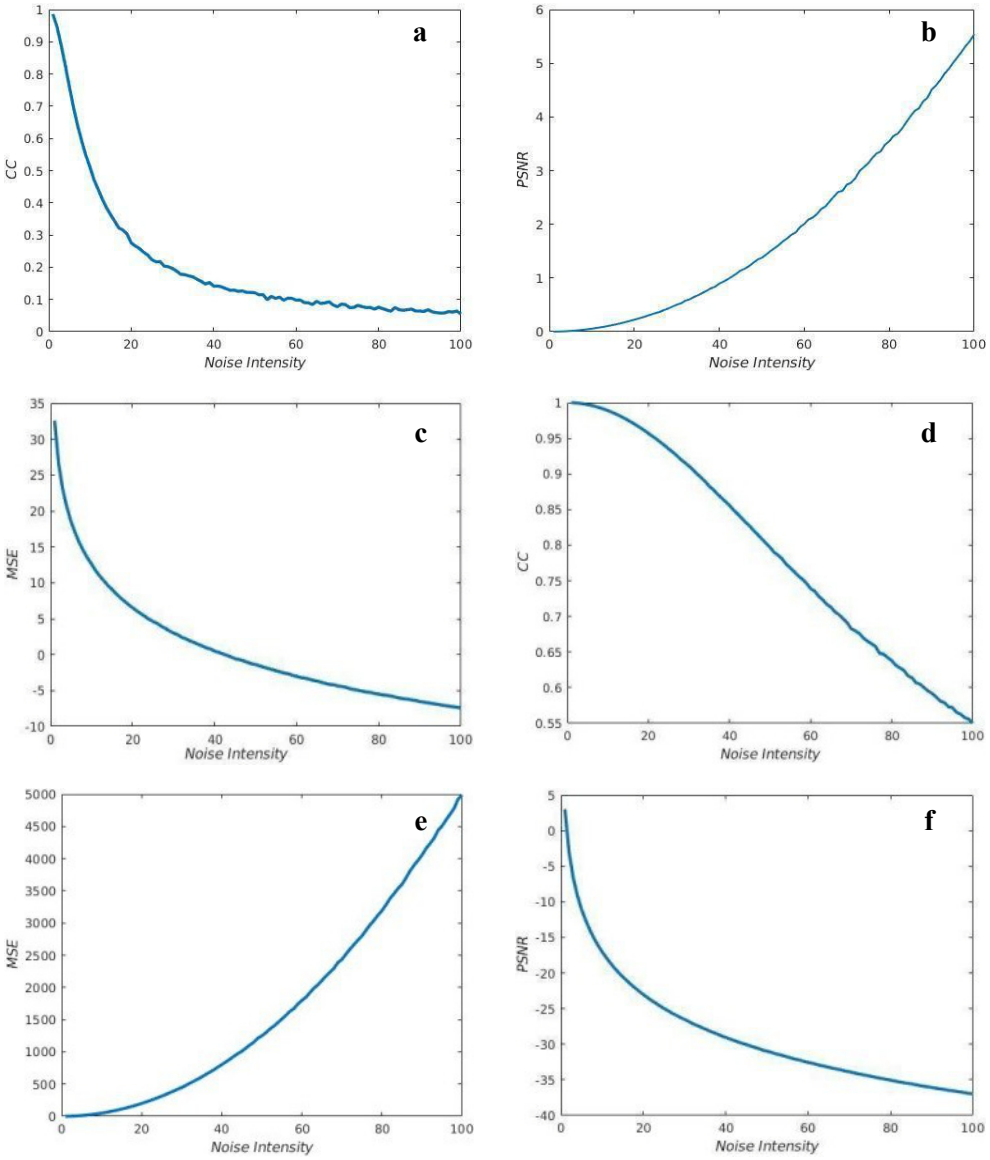

Fig. 10. Plots of CC, MSE and PSNR against noise intensity. (**a**) CC *versus* noise curve for audio, (**b**) MSE *versus* noise curve for audio, (**c**) PSNR *versus* noise curve for audio, (**d**) CC *versus* noise curve for image, (**e**) MSE *versus* noise curve for image, (**f**) PSNR *versus* noise curve for image.

50 and 75, the decrypted *Boat* image is given in Fig. 9(**g**–**i**). As can be seen, the images recovered after a noise attack can easily be identified. Figure 10 shows the plots of CC, MSE, and PSNR against noise intensity, and it indicates that the proposed scheme is resistant to additive noise attacks.

3.6. Quantitative comparison analysis

The proposed scheme is quantitatively compared with various recent schemes in terms of entropy, execution time and key space. Table 2 gives the key space, time execution and entropy of ciphertext of various schemes. As can be seen from Table 2, the proposed scheme has the least execution time of 1.615843 seconds with a key space of 3 RPM and six keys. The ciphertext entropy value is 7.9979, which indicates the randomness in the encrypted image. All these parameters demonstrate the strength and quality of the proposed encryption scheme.

T a b l e 2. Quantitative comparison analysis of the present scheme against 3D Lorenz chaotic system and DRPE based scheme [24], Lorenz-chaos and exclusive-OR based scheme [25], iterative fractional Fourier transform and chaos-based scheme [37], 3D-biomatrix and chaotic map with Markov properties based scheme [26], and hyperchaotic and RD based scheme [20] with Lena as the input image.

Parameters	3D Lorenz chaotic system and DRPE based scheme [24]	Lorenz -chaos and exclusive-OR based scheme [25]	Iterative fractional Fourier transform and chaos -based scheme [37]	3D-biomatrix and chaotic map with Markov properties based scheme [26]	Hyperchaotic and RD based scheme [20]	Present scheme
Element in key space	9	RPM+9	6	6	RPM+20	RPM+6
Entropy of the encrypted image	7.452	7.750	7.530	7.991	7.981	7.9979
Execution time	3.80553 s	3.8371 s	–	–	1.447 s	1.615843 s

4. Conclusions

A secure audio and image encryption scheme using random and QR decomposition in the Fresnel transform domain has been proposed. The Fresnel transform parameters and the keys obtained from RD and QR decomposition form the key space. Validation of the scheme is carried out on actual audio files and standard test images, along with its sensitivity by disturbing the parameters and the decryption keys. It has been observed that a single wrong parameter gives ambiguous results. Furthermore, 3D graphs, histograms and statistical measures show the efficacy of the algorithm. Noise and other attacks analysis establish the strength of the scheme. A quantitative comparison analysis of the present scheme against various recent encryption schemes has been done to bring out its advantages. Thus, this work demonstrates that we can encrypt an audio file efficiently using image encryption methods. Additionally, it also opens a field for researchers to work on audio files using image encryption schemes.

References

[1] Rajput S.K., Matoba O., *Optical voice encryption based on digital holography*, Optics Letters **42**(22), 2017, pp. 4619–4622, DOI: 10.1364/OL.42.004619.

[2] Yang Y.-G., Tian J., Sun S.-J., Xu P., *Quantum-assisted encryption for digital audio signals*, Optik **126**(21), 2015, pp. 3221–3226, DOI: 10.1016/j.ijleo.2015.07.082.

[3] Mosa E., Messiha N.W., Zahran O., Abd El-Samie F.E., *Chaotic encryption of speech signals*, International Journal of Speech Technology **14**(4), 2011, 285, DOI: 10.1007/s10772-011-9103-7.

[4] Peng X., Cui Z., Cai L., Yu L., *Digital audio signal encryption with a virtual optics scheme*, Optik **114**(2), 2003, pp. 69–75, DOI: 10.1078/0030-4026-00224.

[5] Ghasemzadeh A., Esmaeili E., *A novel method in audio message encryption based on a mixture of chaos function*, International Journal of Speech Technology **20**(4), 2017, pp. 829–837, DOI: 10.1007/s10772-017-9452-y.

[6] Lima J.B., Da Silva Neto E.F., *Audio encryption based on the cosine number transform*, Multimedia Tools and Applications **75**(14), 2016, pp. 8403–8418, DOI: 10.1007/s11042-015-2755-6.

[7] Savita A., Singh P., Yadav A.K., Singh K., *Asymmetric audio encryption system based on Arnold transform and random decomposition*, Asian Journal of Physics **27**(9–12), 2018, pp. 711–719.

[8] 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.

[9] Unnikrishnan G., Singh K., *Double random fractional Fourier domain encoding for optical security*, Optical Engineering **39**(11), 2000, pp. 2853–2859, DOI: 10.1117/1.1313498.

[10] 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.

[11] Kumar R., Bhaduri B., *Double image encryption in Fresnel domain using wavelet transform, gyrator transform and spiral phase masks*, Proc. SPIE 10449, Fifth International Conference on Optical and Photonics Engineering, 2017, 104490O, DOI: 10.1117/12.2269897.

[12] Xu H., Xu W., Wang S., Wu S., *Asymmetric optical cryptosystem based on modulus decomposition in Fresnel domain*, Optics Communications **402**, 2017, pp. 302–310, DOI: 10.1016/j.optcom.2017.05.035.

[13] Singh H., *Devil's vortex Fresnel lens phase masks on an asymmetric cryptosystem based on phase-truncation in gyrator wavelet transform domain*, Optics and Lasers in Engineering **81**, 2016, pp. 125–139, DOI: 10.1016/j.optlaseng.2016.01.014.

[14] Kumar R., Bhaduri B., Nishchal N.K., *Nonlinear QR code based optical image encryption using spiral phase transform, equal modulus decomposition and singular value decomposition*, Journal of Optics **20**(1), 2017, 015701, DOI: 10.1088/2040-8986/aa9943.

[15] Yadav A.K., Vashisth S., Singh H., Singh K., *Optical cryptography and watermarking using some fractional canonical transforms, and structured masks*, [In] V. Lakshminarayanan, I. Bhattacharya [Eds], *Advances in Optical Science and Engineering*, Springer Proceedings in Physics, Vol. 166, Springer, New Delhi, 2015, pp. 25–36, DOI: 10.1007/978-81-322-2367-2_5.

[16] 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, DOI: 10.1155/2015/926135.

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

[18] 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.

[19] Fatima A., Mehra I., Nishchal N.K., *Optical image encryption using equal modulus decomposition and multiple diffractive imaging*, Journal of Optics **18**(8), 2016, 085701, DOI: 10.1088/2040-8978/18/8/085701.

[20] RAKHEJA P., VIG R., SINGH P., *An asymmetric hybrid cryptosystem using hyperchaotic system and random decomposition in hybrid multi resolution wavelet domain*, Multimedia Tools and Applications **78**(15), 2019, pp. 20809–20834, DOI: 10.1007/s11042-019-7406-x.

[21] 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, pp. 679–686, DOI: 10.1364/AO.55.000679.

[22] PAREEK N.K., PATIDAR V., SUD K.K., *Image encryption using chaotic logistic map*, Image and Vision Computing **24**, 2006, pp. 926–934, DOI: 10.1016/j.imavis.2006.02.021.

[23] VASHISTH S., SINGH H., YADAV A.K., SINGH K., *Devil's vortex phase structure as frequency plane mask for image encryption using the fractional Mellin transform*, International Journal of Optics, Vol. 2014, 2014, 728056, DOI: 10.1155/2014/728056.

[24] SHARMA N., SAINI I., YADAV A.K., SINGH P., *Phase-image encryption based on 3D-Lorenz chaotic system and double random phase encoding*, 3D Research **8**(4), 2017, p. 39, DOI: 10.1007/s13319-017-0149-4.

[25] SAINI I., SINGH P., YADAV A.K., *Analysis of Lorenz-chaos and exclusive-OR based image encryption scheme*, International Journal of Social Computing and Cyber-Physical Systems **2**(1), 2017, pp. 59–72, DOI: 10.1504/IJSCCPS.2017.088769.

[26] GE M., YE R., *A novel image encryption scheme based on 3D bit matrix and chaotic map with Markov properties*, Egyptian Informatics Journal **20**(1), 2019, pp. 45–54, DOI: 10.1016/j.eij.2018.10.001.

[27] KUMAR P., JOSEPH J., SINGH K., *Known-plaintext attack-free double random phase-amplitude optical encryption: vulnerability to impulse function attack*, Journal of Optics **14**(4), 2012, 045401, DOI: 10.1088/2040-8978/14/4/045401.

[28] QIN W., PENG X., *Vulnerability to known-plaintext attack of optical encryption schemes based on two fractional Fourier transform order keys and double random phase keys*, Journal of Optics A: Pure and Applied Optics **11**(7), 2009, 075402, DOI: 10.1088/1464-4258/11/7/075402.

[29] 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.

[30] LIU Y., ZHANG L.Y., WANG J., ZHANG Y., WONG K., *Chosen-plaintext attack of an image encryption scheme based on modified permutation–diffusion structure*, Nonlinear Dynamics **84**(4), 2016, pp. 2241–2250, DOI: 10.1007/s11071-016-2642-3.

[31] XIONG Y., QUAN C., *Hybrid attack free optical cryptosystem based on two random masks and lower upper decomposition with partial pivoting*, Optics & Laser Technology **109**, 2019, pp. 456–464, DOI: 10.1016/j.optlastec.2018.08.033.

[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] QAYUM A., KUMAR P., *QR decomposition-based cryptography: Via image generation* (*QR-CRYPT*), 2012 International Conference for Internet Technology and Secured Transactions, IEEE, 2012, https://ieeexplore.ieee.org/document/6470939 (accessed April 23, 2020).

[34] ABUTURAB M.R., *Single-channel color information security system using LU decomposition in gyrator transform domains*, Optics Communications **323**, 2014, pp. 100–109, DOI: 10.1016/j.optcom.2014.02.061.

[35] BENESTY J., CHEN J., HUANG Y., COHEN I., *Pearson correlation coefficient*, [In] *Noise Reduction in Speech Processing*, [Eds.] I. Cohen, Y. Huang, J. Chen, J. Benesty, Vol. 2, Springer, Berlin, Heidelberg, 2009, DOI: 10.1007/978-3-642-00296-0_5.

[36] HORÉ A., ZIOU D., *Image quality metrics: PSNR vs. SSIM*, [In] *2010 20th International Conference on Pattern Recognition*, 2010, pp. 2366–2369, DOI: 10.1109/ICPR.2010.579.

[37] SUI L., GAO B., *Single-channel color image encryption based on iterative fractional Fourier transform and chaos*, Optics & Laser Technology **48**, 2013, pp. 117–127, DOI: 10.1016/j.optlastec.2012.10.016.

Received May 14, 2021
in revised form August 8, 2021