Optica Applicata, Vol. LII, No. 1, 2022
DOI: 10.37190/oa220102

Asymmetric double-image encryption using twin decomposition in fractional Hartley domain

JAIDEEP KUMAR[1*], PHOOL SINGH[2], AK YADAV[3]

[1]School of Engineering and Technology, K.R. Mangalam University, Gurugram-122103, India

[2]School of Engineering and Technology, Central University of Haryana-123031, India

[3]Amity School of Applied Sciences, Amity University Haryana, Gurugram-122413, India

[*]Corresponding author: jaideep.rohtak@gmail.com

Twin decomposition, consisting of equal and random modulus decompositions, not only makes a cryptosystem asymmetric but also resists special attack. A new double-image asymmetric cryptosystem using twin decomposition in fractional Hartley domain is proposed. An input grayscale image, bonded with another grayscale image as its phase mask, is transformed via fractional Hartley transform. Equal modulus decomposition is applied on the resulting image, giving us two intermediate images. One of them is subjected to another fractional Hartley transform followed by random modulus decomposition, whereas the other serves as the first private key. The application of random modulus decomposition also results in two images: encrypted image and the second private key. During the process of decryption, firstly the encrypted image is combined with second private key and thereafter it is subjected to inverse fractional Hartley transform. The resulting image is then combined with the first private key, and followed by another inverse fractional Hartley transform, thus recovering the two original images. The proposed cryptosystem is validated for pairs of grayscale images.

Keywords: double image encryption, twin decomposition, asymmetric cryptosystem, fractional Hartley transform.

1. Introduction

In modern era, when our world is increasingly becoming one platform with availability, access and sharing of personal information through public networks for professional transactions as well as personal interactions, the importance of digital security cannot be overlooked. This data can be as small as a four-digit password for performing an online banking transaction and as big as stock market reports of listed companies. One of the major concerns with this increased accessibility is, how to effectively and efficiently

secure, process, protect, share and store the abundant information thereby minimizing the risk of malicious intrusion. During the past few decades, researchers have investigated information security with optical approach to capitalize on the potential capacity of optical technologies. Optical technologies not only provide massive information capacity and high speed but also possess capabilities for parallel processing. In 1995, an optical encryption scheme based on double random phase encoding (DRPE) in Fourier transform domain in which an input image is transformed to a stationary white noise was proposed by REFREGIER and JAVIDI [1]. Researchers extended DRPE to other integral transform domains such as wavelet [2], Fresnel [3] and Hartley [4]. Later on, DRPE was found to be vulnerable to certain basic attacks [5–8], owing to its symmetric and linear nature. Further work on DRPE included its extension to fractionalized version of integral transform domains like fractional Fourier [9], fractional Hartley [10], gyrator [11], fractional Mellin [12], and fractional wavelet [13], to add more security features against the basic attacks. However, DRPE in fractional transform domains has also been shown vulnerable to known plaintext attack under certain conditions. Therefore, researchers have been continuously attempting to develop cryptosystems with ever-increasing security features, while retaining the simplicity of DRPE.

In order to overcome the security threat due to linearity of DRPE, QIN and PENG [14] proposed an asymmetric cryptosystem which was based on phase truncation operation. The technique was commonly known as phase truncated Fourier transform (PTFT). The encryption and decryption keys are different in PTFT-based techniques and therefore, basic attacks such as known plaintext attack, ciphertext attack and chosen plaintext attack are meaningless. The phase and amplitude truncation techniques have been extended to other domains [15–20] also. But later on, PTFT-based schemes were reported to be vulnerable to a special attack [21–23].

CAI *et al*. [24] presented an asymmetric encryption scheme based on coherent superposition and equal modulus decomposition (EMD) in order to solve the silhouette problem. DENG [25] and WU *et al*. [26] have shown that single EMD is vulnerable to special attack as its ciphertext provides adequate information to an intruder. WANG *et al*. [27] proposed a random modulus decomposition (RMD), as an alternative to equal modulus decomposition, in which resultant random phase masks possessed unequal moduli.

In order to strengthen the security, double and multiple image encryption schemes have been explored and investigated by researchers, due to their high efficiency towards transmission of information [28]. In 2007, TAO *et al*. [28] reported a novel method to encrypt two images into stationary white noise. In 2012, LIU *et al*. [29] used Arnold transform and discrete fractional angular transform for double image encryption. WANG and ZHAO [30] proposed a double-image encryption technique based on the phase truncated Fourier transform (PTFT) and joint transform correlator (JCT). XIONG *et al*. [31] have shown that the scheme proposed by WANG and ZHAO [30] is exposed to a special attack built on phase retrieval algorithm. In 2015, SUI *et al*. [32] used multi-parameter fractional angular transform and two coupled logistic maps to encrypt

a double image. In 2018, KUMAR *et al*. [33] proposed a double image encryption scheme by using linear canonical transform. In 2019, LIANSHENG SUI *et al*. [34] presented double image encryption by using optical interference logistic maps.

Hartley transform is a mathematical tool used in image and signal processing. It is a real valued transform whereas its fractionalized version called fractional Hartley transform is complex valued [35]. Fractional Hartley transform is optically implementable [36] and is used symmetric algorithms [37, 38], asymmetric algorithms [39, 40] and compression algorithm [41]. However, effectiveness of an asymmetric scheme using twin decomposition based on EMD and RMD in fractional Hartley domain is yet to be studied.

The present study proposes a double-image encryption scheme that uses twin (equal modulus and random modulus) decomposition in fractional Hartley domain. Random modulus decomposition and equal modulus decomposition not only make a cryptosystem asymmetric, but also resist basic as well as special attack.

2. Proposed scheme

The proposed scheme starts with a pair of input images $f(x, y)$ and $g(x, y)$. One of the input grayscale images is bonded with the other input image as its phase mask, further transformed; via fractional Hartley transform of order (p, t). With the help of θ, an equal modulus decomposition (EMD) is performed on the resulting image. The EMD divides the image into P1 and P2 which have the same amplitude, and P1 has a phase equal to θ which is a public key (as shown in Fig. 1). Thus, P1 needs not be stored as it can be easily reconstructed using θ and amplitude of P2. Now P2 is further exposed to another fractional Hartley transform of order (q, r). With the help of two random functions α and β which are uniformly distributed in the interval $[0, 2\pi]$, an RMD is performed on the

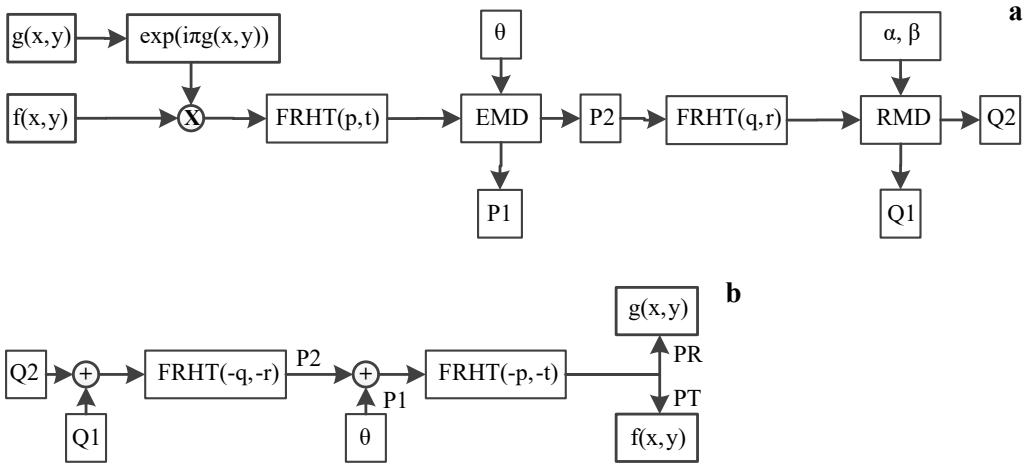

Fig. 1. Schematic diagram of (**a**) encryption, and (**b**) decryption scheme.

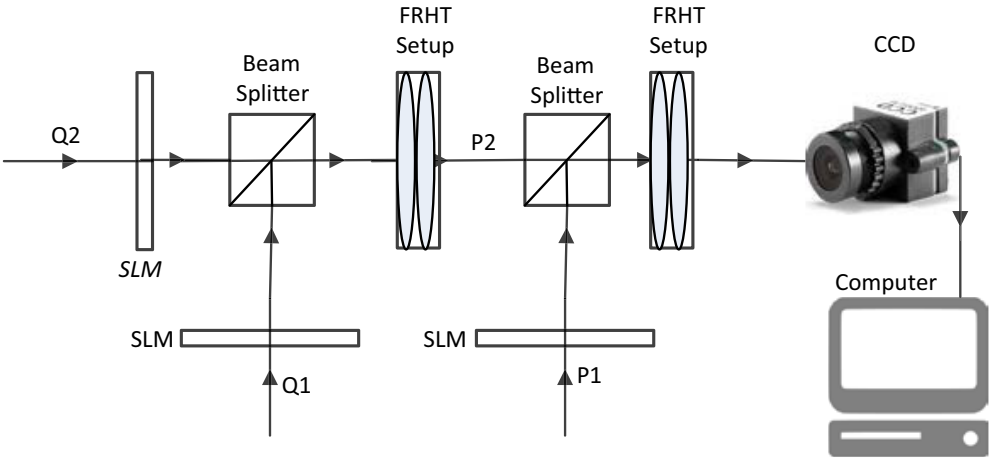

Fig. 2. Optoelectronic setup of the proposed decryption process.

image obtained from the previous step. RMD divides the image into two components Q1 and Q2. Q1 acts as a private key and Q2 is the encrypted image.

For decryption, a reverse process is followed wherein encrypted image Q2 is added with the private key Q1 and thereafter subjected to an inverse fractional Hartley transform of order $(-q, -r)$ to give P2. With the help of amplitude of P2 and public key θ, P1 can be obtained. In the next step, the images P1 and P2 are added and then another inverse fractional Hartley transform of order $(-p, -t)$ is performed, thus recovering the input double images. One is amplitude image, obtained as a result of phase truncation, and the other image as argument part of the decrypted image. The proposed scheme has four fractional Hartley transform orders and a private key Q1 as its encryption parameters.

The optoelectronic set of the decryption process of the proposed scheme is also shown in Fig. 2. Charge-coupled device (CCD), spatial light modulator (SLM) and beam splitter are used to transfer data between the computer and optical system. The encrypted image Q2 is combined with the private key Q1 in the fractional Hartley transform domain using the beam splitter. In the fractional Hartley domain, we obtained P2 which is again combined with P1, another key with the help of beam splitter. Finally, the decrypted images are recorded using the CCD and stored in the computer.

3. Results and discussion

For validating the feasibility and testing the performance of the proposed double image encryption scheme, computer based numerical simulations have been performed. Figure 3 shows scheme validation results for grayscale images of "The Girl" and "The Boy" of size 256×256 pixels. The encrypted image (Fig. 3**c**) corresponding to the grayscale input images (Figs. 3**a** and 3**b**), is quite random and resembles stationary white noise. Figures 3**d** and 3**e** shows the decrypted images obtained from the scheme and has pixel

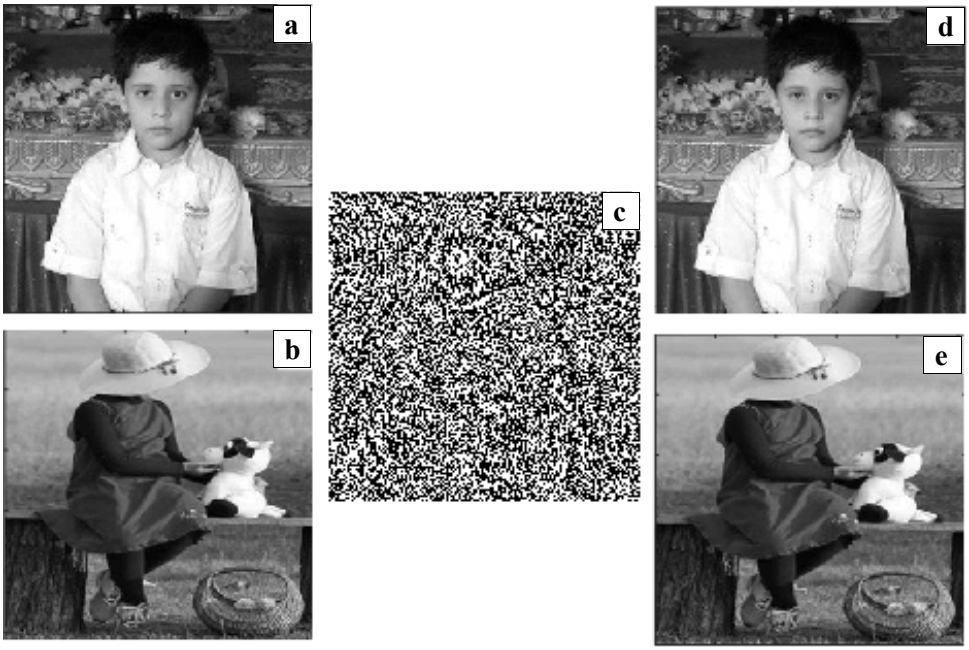

Fig. 3. Verification of the proposed scheme with grayscale input images of "The Boy" (as amplitude part) and "The Girl" (as phase part).

distribution identical to that of the input images, having corresponding correlation coefficient (CC) which equals 1.

3.1. Statistical attack

Statistical attack is initially performed using histograms in order to establish correlation between input image and the resultant encrypted image. Correlation distribution of pixels is a method for evaluating the quality of encryption of an image. Figure 4 gives histograms of the input images, encrypted image and the corresponding decrypted im-

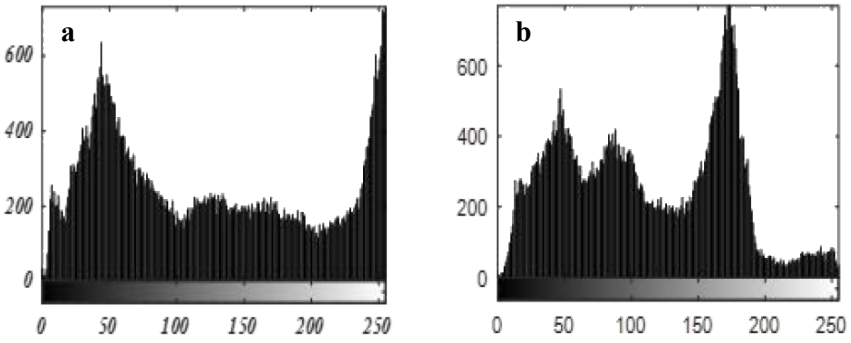

Fig. 4. Histogram plots of (**a**, **b**) input images; (**c**) encrypted image; (**d**, **e**) decrypted images.

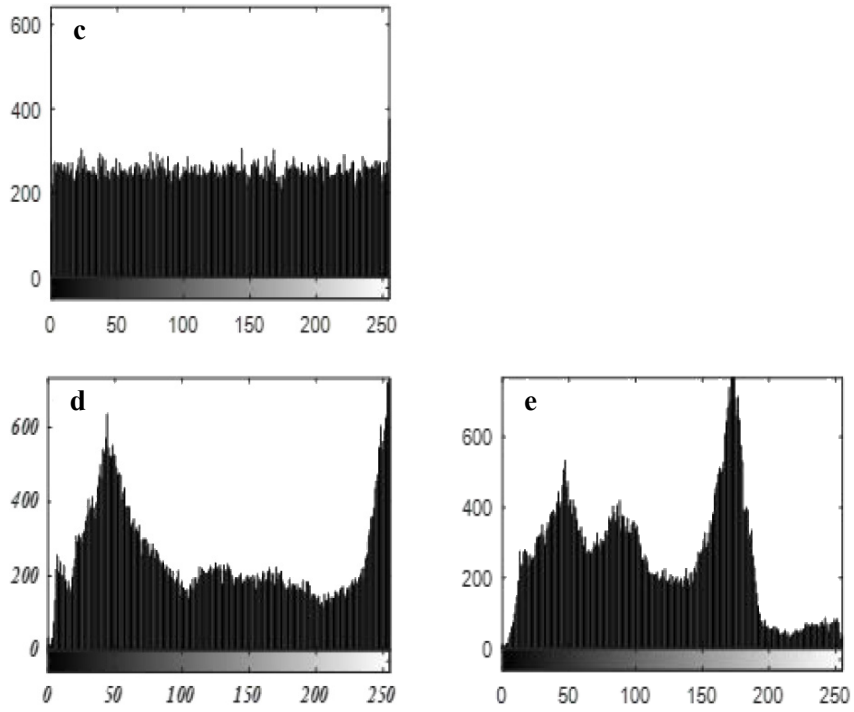

Fig. 4. Continued.

ages. Histogram of the encrypted image turns out to be completely different from those of the input images and does not show natural variation. Also, the histograms of the recovered images appear almost the same as the histograms of the input images.

3.2. Information entropy

Only information entropy reveals the level of randomness in an image, which in turn describes the quality of encryption of the image. Information entropy is defined by

$$H(m) = -\sum_{k=1}^{256} P(m_k)\log_2(P(m_k)) \tag{1}$$

where $P(m_k)$ refers to the probability of m_k. For grayscale images, the entropy value should be in the range of 0 to 8. The entropy of the encrypted image obtained in this study is 7.9962, which is very close to the ideal value. Thus, the proposed scheme resists entropy attack in the absence of adequate information leakage.

3.3. Correlation distribution

It is a general phenomenon that in an original image, all pixels adjacent to each other are closely related. An effective encryption scheme should be able to reduce the correlation amongst the adjacent pixels of the encrypted image to a bare minimum. Figure 5

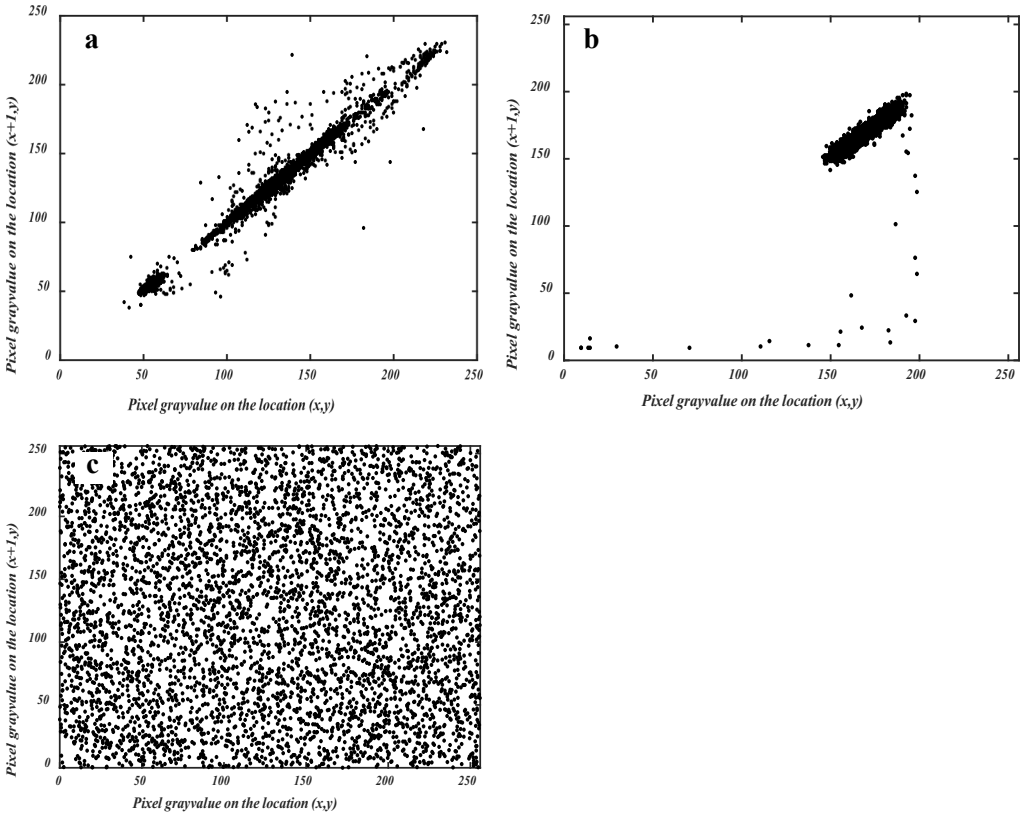

Fig. 5. Correlation distribution for input images of (**a**) "The Boy", (**b**) "The Girl" and for (**c**) encrypted image.

depicts the correlation distribution of horizontally adjacent pixels for input images and the encrypted image.

At random, 5 000 pixels of input images are selected and plotted against their neighbouring pixels in horizontal direction in Figs. 5**a** and 5**b**. The corresponding plot for the encrypted image is shown in Fig. 5**c**. It is observed that the neighbouring pixels in the input images show high correlation whereas the correlation distribution of the encrypted image shows no correlation at all.

3.4. Key sensitivity

A scheme is considered highly secure in case it is sensitive to its input parameters which implies that even a slight change in the secret key will give an entirely wrong result. Figures 6**a** and 6**b** show the decrypted images with one incorrect parameter, $q = 0.6005$ instead of $q = 0.6$ of fractional Hartley transform, while Figs. 6**c** and 6**d** show the decrypted images with correct keys. It can be observed that a slight change of the parameters of the secret key produced completely wrong results. Figures 7**a**, 7**b** and Figs. 7**c**, 7**d**

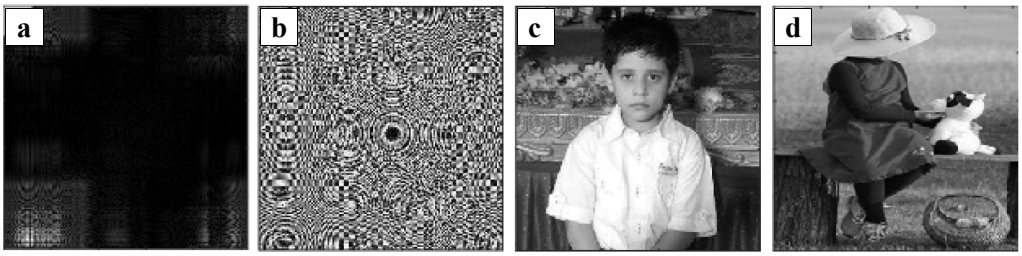

Fig. 6. Recovered images when wrongs keys are used in the decryption process (**a**, **b**) $q = 0.6005$ is used instead of $q = 0.6$, whereas (**c**, **d**) are with correct parameters.

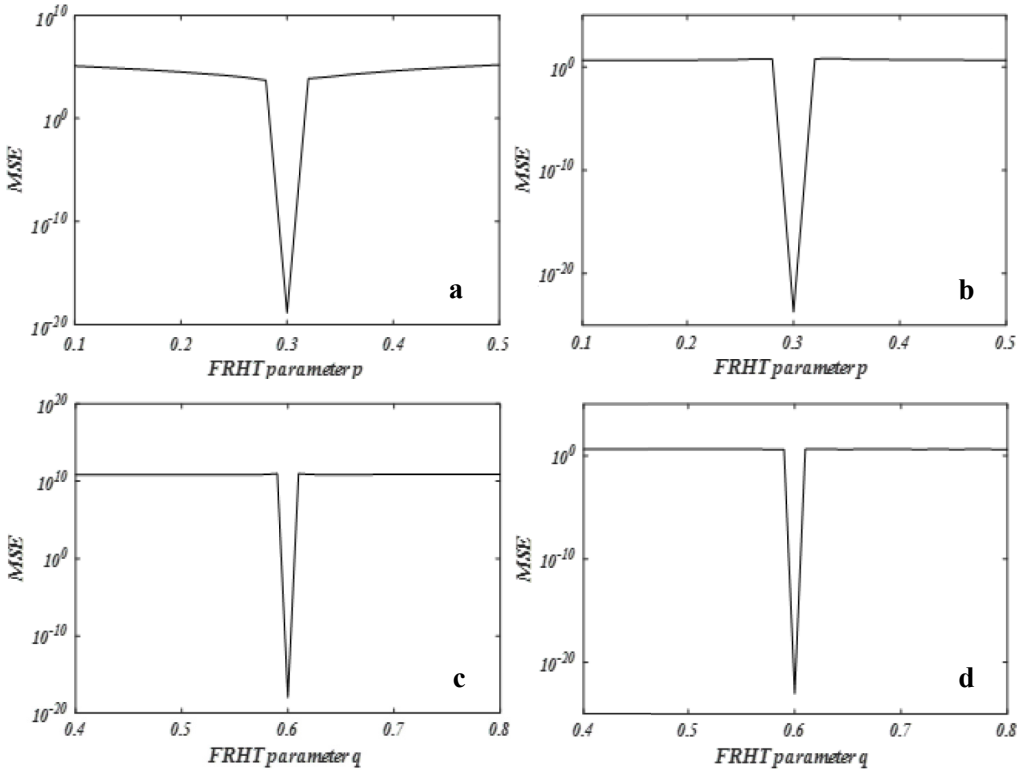

Fig. 7. Sensitivity plots showing mean-squared error (MSE) *versus* order of fractional Hartley transform for recovered images of (**a**, **c**) "The Boy" and (**b**, **d**) "The Girl".

show the sensitivity plots for input images of "The Boy" and "The Girl" with respect to orders of fractional Hartley transform, respectively.

3.5. Noise attack analysis

During the transmission of encrypted images, we often encounter loss due to noise attack. Here, we test immunity of the proposed scheme to these transmission influences.

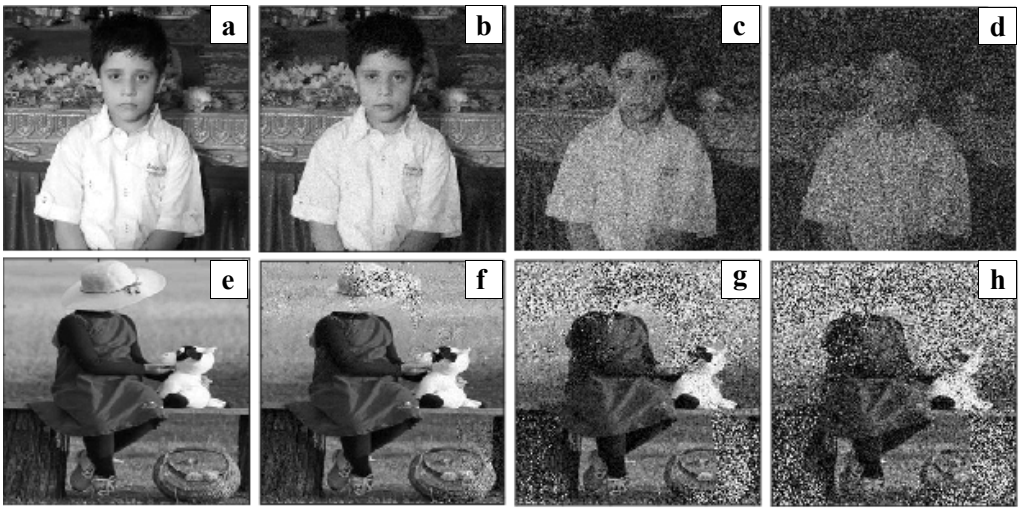

Fig. 8. Decrypted images when the encrypted image is attacked with varying noise strength (**a**, **e**) $k = 0.1$, (**b**, **f**) $k = 0.3$, (**c**, **g**) $k = 0.5$, and (**d**, **h**) $k = 1$.

We add random noise to the cipher image with varying strength k. Figure 8 shows the results of the noise attack on the proposed scheme. Thus, the normal random noise R with mean 0 and standard deviation 1 multiplied by a strength parameter k is added to the encrypted image $E_n(x, y)$, according to the equation

$$E_{\mathrm{n}}^{*} = E_{\mathrm{n}} + kR \tag{2}$$

where E_{n}^{*} is the noise affected encrypted image. Figures 8**a**–8**d** and Figs. 8**e**–8**h** give the recovered images of "The Boy" and "The Girl" corresponding to the noise strength $k = 0.1$, 0.3, 0.5 and 1, respectively. It is clearly evident that the input images of "The Boy" and "The Girl" are recognizable even in the presence of high noise strength

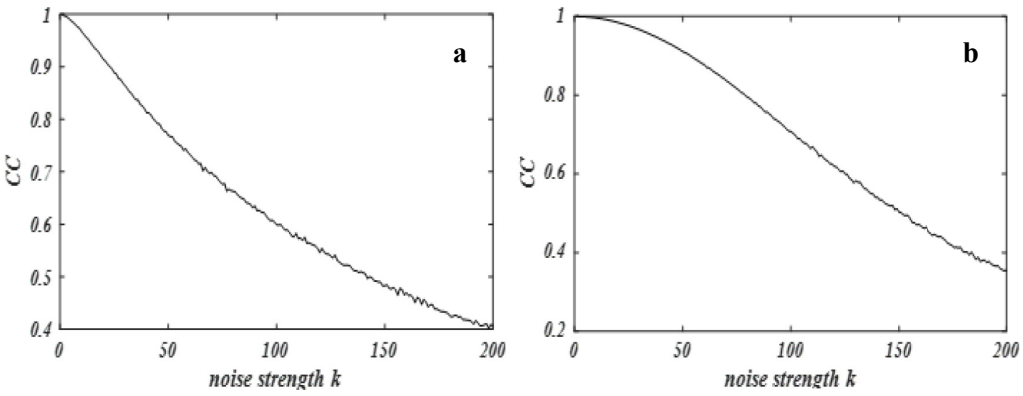

Fig. 9. Plot of correlation coefficient against noise strength for (**a**) "The Boy", and (**b**) "The Girl".

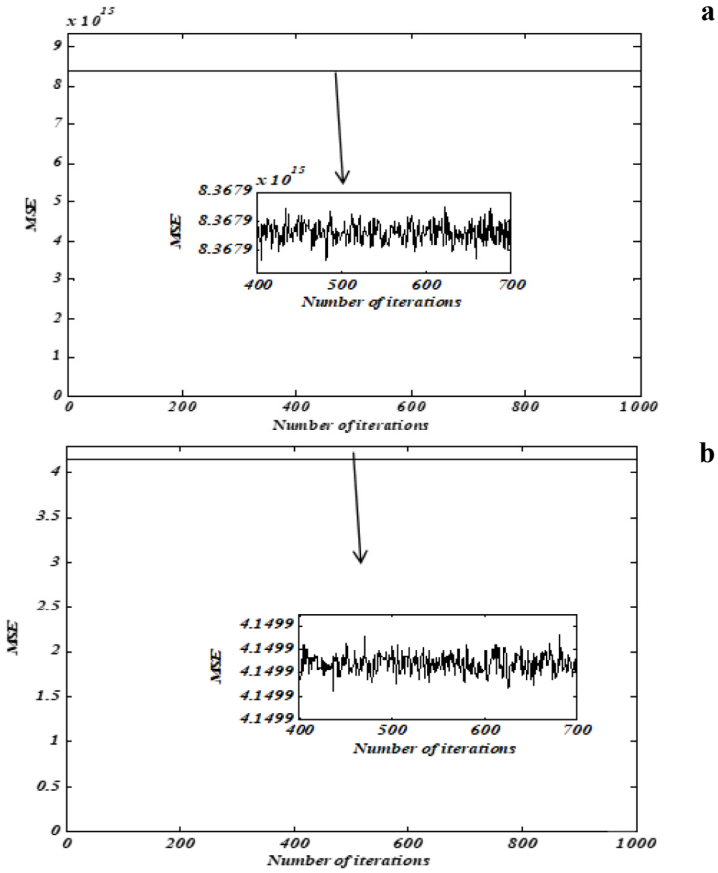

Fig. 10. Results of special attack mounted on the proposed scheme (**a**) "The Boy" image, and (**b**) "The Girl" image.

($k = 1$). A plot of correlation coefficient CC *versus* noise strength k is given in Fig. 9. These results clearly indicate that the proposed scheme endures the noise attack. The proposed scheme is asymmetric, and its strength lies in the private key which varies with the input image. Therefore, given a plaintext-ciphertext pair, attempting a private key is futile as it is a one-time padding. Therefore, chosen plaintext and known plaintext attacks are not applicable on the proposed scheme.

We have also mounted a special attack on the proposed scheme. Results of this attack are shown in Fig. 10 by plotting mean-squared error (MSE) computed for the input images and their respective recovered images for 1 000 iterations for "The Boy" and "The Girl" images, respectively. MSE between images of size $R \times S$ pixels is defined as

$$\mathrm{MSE} = \frac{1}{R \times S} \sum_{x=1}^{R} \sum_{y=1}^{S} \left| \mathrm{input\_image}(x, y) - \mathrm{decrypted\_image}(x, y) \right|^2 \qquad (3)$$

T a b l e. Comparison of the present scheme with some existing asymmetric schemes.

Parameters	Schemes				
	CAI *et al*. [24]	CAI and SHEN [42]	WANG *et al*. [27]	RAKHEJA *et al*. [43]	Present paper
Methodology	EMD, grayscale image	Modified EMD, grayscale image	Random decomposition, grayscale image	Random decomposition, grayscale image	Double image, twin decomposition
Transform domain	Fourier transform	Fourier transform	Fourier transform	Hybrid transform	Fractional Hartley transform
Key length	Private key	Private keys	Private keys	Private keys + hybrid transform order	Private keys + fractional Hartley orders
Strength(s)	Public key cryptosystem, immune to basic attacks	Public key cryptosystem, immune to basic attacks, special attack	Public key cryptosystem, immune to basic attacks	Public key cryptosystem, immune to basic attacks, special attack	Public key cryptosystem, immune to basic attacks, special attack
Weakness(es)	Complex cipher, vulnerable to special attack	Simple transform is used	Complex cipher, vulnerable to special attack	Complex cipher	Complex cipher
Entropy	7.9950	7.9952	7.9956	7.9830	7.9963
Encryption time [sec]	0.74	0.93	0.69	1.44	1.92
PSNR [db]	234	182	168	252	196

It is observed from Figs. 10**a** and 10**b** that although a straight line appears about MSE value 8.3679×10^{15} for "The Boy" image and 4.15 for "The Girl" image in the graphs but when it is zoomed out, a nonlinear pattern appears. The MSE for "The Girl" is relatively much less due to normalization, required for it to be used as a phase mask. With this high value of MSE, no information about the original input images is traceable, which demonstrates that the presented scheme is resistant to special attack.

3.6. Comparison analysis

Here, we have carried out a comparison analysis of the proposed scheme with some existing similar asymmetric schemes reported in the literature. The proposed cryptosystem is compared with CAI *et al*. [24], CAI and SHEN [42], WANG *et al*. [27] and RAKHEJA *et al*. [43], based on various parameters such as type of encryption, transform domain, applied methodology, strengths and weaknesses, key length, computational time, entropy, and peak-signal-to-noise-ratio. The Table clearly shows that the proposed scheme has an advantage in terms of entropy, larger key space, and capability to perform double-image encryption. Being asymmetric and nonlinear in nature, it resists the basic attacks as well as the special attack.

4. Conclusion

In this paper, an asymmetric double-image encryption scheme using twin decomposition in fractional Hartley domain is investigated. One of the input grayscale images is bonded with the other input image as its phase mask. It is transformed via fractional Hartley transform and followed by twin (equal and random modulus) decomposition to get the encrypted image. Numerical simulations have been performed for validating the feasibility and testing the performance of the proposed scheme. It has been successfully shown that both the original images can be faithfully recovered only when all keys used are correct. We have also mounted special attack on the scheme and found the scheme to resist the special attack. Comparison analysis with similar schemes reveals that the proposed scheme performed well in terms of entropy and also has a larger key space. Further, it is found to resist the basic attacks as well as the special attack, due to its asymmetric and nonlinear structure.

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] 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.

[3] SITU G., ZHANG J., *Double random-phase encoding in the Fresnel domain*, Optics Letters **29**(14), 2004, pp. 1584–1586, DOI: 10.1364/OL.29.001584.

[4] CHEN L., ZHAO D., *Optical image encryption with Hartley transforms*, Optics Letters **31**(23), 2006, pp. 3438–3440, DOI: 10.1364/OL.31.003438.

[5] 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.

[6] GOPINATHAN U., MONAGHAN D.S., NAUGHTON T.J., SHERIDAN J.T., *A known-plaintext heuristic attack on the Fourier plane encryption algorithm*, Optics Express **14**(8), 2006, pp. 3181–3186, DOI: 10.1364/OE.14.003181.

[7] PENG X., WEI H., ZHANG P., *Chosen-plaintext attack on lensless double-random phase encoding in the Fresnel domain*, Optics Letters **31**(22), 2006, pp. 3261–3263, DOI: 10.1364/OL.31.003261.

[8] 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.

[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] SINGH P., YADAV A.K., SINGH K., *Phase image encryption in the fractional Hartley domain using Arnold transform and singular value decomposition*, Optics and Lasers in Engineering **91**, 2017, pp. 187–195, DOI: 10.1016/j.optlaseng.2016.11.022.

[11] LIU Z., GUO Q., XU L., AHMAD M.A., 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.

[12] 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.

[13] CHEN L., ZHAO D., *Optical image encryption based on fractional wavelet transform*, Optics Communications **254**(4–6), 2005, pp. 361–367, DOI: 10.1016/j.optcom.2005.05.052.

[14] 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.

[15] ABUTURAB M.R., *Color information cryptosystem based on optical superposition principle and phase-truncated gyrator transform*, Applied Optics **51**(33), 2012, pp. 7994–8002, DOI: 10.1364/AO.51.007994.

[16] WANG J., SONG L., LIANG X., LIU Y., LIU P., *Secure and noise-free nonlinear optical cryptosystem based on phase-truncated Fresnel diffraction and QR code*, Optical and Quantum Electronics **48**(11), 2016, article 523, DOI: 10.1007/s11082-016-0796-3.

[17] WANG X., ZHAO D., *Simultaneous nonlinear encryption of grayscale and color images based on phase-truncated fractional Fourier transform and optical superposition principle*, Applied Optics **52**(25), 2013, pp. 6170–6178, DOI: 10.1364/AO.52.006170.

[18] WANG Y., QUAN C., TAY C.J., *Optical color image encryption without information disclosure using phase-truncated Fresnel transform and a random amplitude mask*, Optics Communications **344**, 2015, pp. 147–155, DOI: 10.1016/j.optcom.2015.01.045.

[19] YADAV A.K., SINGH P., SINGH K., *Cryptosystem based on devil's vortex Fresnel lens in the fractional Hartley domain*, Journal of Optics **47**(2), 2018, pp. 208–219, DOI: 10.1007/s12596-017-0435-9.

[20] YU S.-S., ZHOU N.-R., GONG L.-H., NIE Z., *Optical image encryption algorithm based on phase-truncated short-time fractional Fourier transform and hyper-chaotic system*, Optics and Lasers in Engineering **124**, 2020, article 105816, DOI: 10.1016/j.optlaseng.2019.105816.

[21] RAJPUT S.K., NISHCHAL N.K., *Known-plaintext attack-based optical cryptosystem using phase-truncated Fresnel transform*, Applied Optics **52**(4), 2013, pp. 871–878, DOI: 10.1364/AO.52.000871.

[22] WANG X., CHEN Y., DAI C., ZHAO D., *Discussion and a new attack of the optical asymmetric cryptosystem based on phase-truncated Fourier transform*, Applied Optics **53**(2), 2014, pp. 208–213, DOI: 10.1364/AO.53.000208.

[23] 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.

[24] CAI J., SHEN X., LEI M., LIN C., DOU S., *Asymmetric optical cryptosystem based on coherent superposition and equal modulus decomposition*, Optics Letters **40**(4), 2015, pp. 475–478, DOI: 10.1364/OL.40.000475.

[25] DENG X., *Asymmetric optical cryptosystem based on coherent superposition and equal modulus decomposition: comment*, Optics Letters **40**(16), 2015, p. 3913, DOI: 10.1364/OL.40.003913.

[26] WU J., LIU W., LIU Z., LIU S., *Cryptanalysis of an "asymmetric optical cryptosystem based on coherent superposition and equal modulus decomposition"*, Applied Optics **54**(30), 2015, pp. 8921–8924, DOI: 10.1364/AO.54.008921.

[27] 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.

[28] 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.

[29] LIU Z., GONG M., DOU Y., LIU F., LIN S., AHMAD M.A., 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.

[30] WANG X., ZHAO D., *Double images encryption method with resistance against the specific attack based on an asymmetric algorithm*, Optics Express **20**(11), 2012, pp. 11994–12003, DOI: 10.1364/OE.20.011994.

[31] XIONG Y., HE A., QUAN C., *Security analysis of a double-image encryption technique based on an asymmetric algorithm*, Journal of the Optical Society of America A **35**(2), 2018, pp. 320–326, DOI: 10.1364/JOSAA.35.000320.

[32] SUI L., DUAN K., LIANG J., *Double-image encryption based on discrete multiple-parameter fractional angular transform and two-coupled logistic maps*, Optics Communications **343**, 2015, pp. 140–149, DOI: 10.1016/j.optcom.2015.01.021.

[33] 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.

[34] LIANSHENG SUI, CONG DU, XIAO ZHANG, AILING TIAN, ANAND A., *Double-image encryption based on interference and logistic map under the framework of double random phase encoding*, Optics and Lasers in Engineering **122**, 2019, pp. 113–122, DOI: 10.1016/j.optlaseng.2019.06.005.

[35] SINGH P., YADAV A., SINGH K., *Color image encryption using affine transform in fractional Hartley domain*, Optica Applicata **47**(3), 2017, pp. 421–433, DOI: 10.5277/oa170308.

[36] ZHAO D., LI X., CHEN L., *Optical image encryption with redefined fractional Hartley transform*, Optics Communications **281**(21), 2008, pp. 5326–5329, DOI: 10.1016/j.optcom.2008.07.049.

[37] LI X., ZHAO D., *Optical color image encryption with redefined fractional Hartley transform*, Optik **121**(7), 2010, pp. 673–677, DOI: 10.1016/j.ijleo.2008.10.008.

[38] LIU Y., DU J., FAN J., GONG L., *Single-channel color image encryption algorithm based on fractional Hartley transform and vector operation*, Multimedia Tools and Applications **74**(9), 2015, pp. 3171–3182, DOI: 10.1007/s11042-013-1778-0.

[39] SINGH P., YADAV A.K., SINGH K., SAINI I., *Asymmetric watermarking scheme in fractional Hartley domain using modified equal modulus decomposition*, Journal of Optoelectronics and Advanced Materials **21**(7–8), 2019, pp. 484–491.

[40] YADAV A.K., SINGH P., SAINI I., SINGH K., *Asymmetric encryption algorithm for colour images based on fractional Hartley transform*, Journal of Modern Optics **66**(6), 2019, pp. 629–642, DOI: 10.1080/09500340.2018.1559951.

[41] YE H.-S., ZHOU N.-R., GONG L.-H., *Multi-image compression-encryption scheme based on quaternion discrete fractional Hartley transform and improved pixel adaptive diffusion*, Signal Processing **175**, 2020, article 107652, DOI: 10.1016/j.sigpro.2020.107652.

[42] CAI J., SHEN X., *Modified optical asymmetric image cryptosystem based on coherent superposition and equal modulus decomposition*, Optics & Laser Technology **95**, 2017, pp. 105–112, DOI: 10.1016/j.optlastec.2017.04.018.

[43] 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**, 2019, pp. 20809–20834, DOI: 10.1007/s11042-019-7406-x.

Received November 12, 2020
in revised form March 24, 2021