Asymmetric watermarking scheme in fractional Hartley domain using modified equal modulus decomposition

P. SINGH[a,*], A. K. YADAV[b], K. SINGH[c], I. SAINI[a]
[a]*Central University of Haryana, Mahendergarh 123031, India*
[b]*Amity School of Applied Sciences, Amity University Haryana, Gurugram-122413, India*
[c]*The NorthCap University, Gurugram -122017, India*

Motivated by the endurance of special attack on asymmetric cryptosystems by modified equal modulus decomposition, a new watermarking scheme for grayscale images in fractional Hartley domain is proposed in this paper. The input grayscale images, bonded with random phase mask, are transformed according to fractional Hartley transform, followed by equal modulus decomposition. One of the two images obtained by equal modulus decomposition serves as a private key, whereas the other image is further transformed with another fractional Hartley transform followed by equal modulus decomposition. Again, one of the resulting images acts as a second private key, whereas the other image is phase truncated before combining with the host image, resulting in a watermarked image. Simulation of the watermarking scheme shows that the scheme is very sensitive to private keys, fractional Hartley orders, and attenuation factor used in the watermarking process. Analysis of histograms, autocorrelation plot, and entropy also indicate that the scheme resists statistical attacks. The scheme also shows its robustness against the additive Gaussian noise attack.

(Received November 10, 2018; accepted August 20, 2019)

Keywords: Modified equal modulus decomposition, Fractional Hartley transform, Watermarking

1. Introduction

In the modern times, security of data is the uppermost need of society because of increased use of public networks (secure/unsecure channels) for data transmission. Data may be one-time password for someone's banking transaction, accounts details, salary details, shopping details, social media details, images, and many more. To restrict an intruder from gaining access to unauthorized data, encryption is one of the widely used approaches. With rapidly decreasing cost of computation, digital image encryption algorithms are prone to the attacks as they possess low degrees of freedom. On the other hand, optical cryptosystems have higher degrees of freedom in terms of wavelength, phase, orbital angular momentum, and polarization, to encode data securely [1–3]. They can process data in parallel, ensuring higher throughput rate as compared to their digital counterparts. These advantages led to development of many encryption schemes modelled on the double random phase encoding (DRPE) proposed by Refregier and Javidi [4], in various domains such as Fourier [5], fractional Fourier [6, 7], Hartley [8], fractional Hartley [9], gyrator [10], Mellin, fractional Mellin [11], and wavelet [12] etc.

Image watermarking is an effective way to employ copyright protection and guarantee the security of data transmitted over a network. An effective watermarking scheme should exhibit adjustability, robustness, imperceptibility, security, and computational complexity [13]. It may be classified in many ways. In view of imperceptibility of watermark, the schemes can be classified as invisible and visible watermarking. Normally invisible watermarking schemes are used for copyright protection. Data being hidden can be encrypted for further strengthening the watermarking scheme. Owing to additional features for security, optical encryption based watermarking schemes have been employed in the recent past. Watermarking schemes may be categorized as symmetric and asymmetric. Symmetric schemes are characterized by the use of same keys for watermarks embedding and detection as in the case of DRPE whereas in asymmetric watermarking, watermarks embedding and detection keys are different.

Qin and Peng [14] introduced an asymmetric optical cryptosystem based on phase-truncated Fourier transform (PTFT). But later on, PTFT based schemes were found to be vulnerable to a special attack [15, 16]. In 2015, Cai et al. [17] introduced asymmetric optical cryptosystem based on equal modulus decomposition (EMD). Deng [18], and Wu et al. [19] have shown that single EMD is also vulnerable to special attack as its ciphertext provides enough information to an attacker. However, Chen et al. [20] proposed pixel scrambling operator along with EMD in gyrator domain to resist special attack. Another scheme employing phase truncation operation and EMD in fractional Fourier domain is proposed by Barfungpa and Abuturab [21]. Fatima et al. [22] countered vulnerability of the special attack on EMD by using multiple diffraction imaging in the gyrator domain. In 2017, Cai and Shen [23] proposed modified equal modulus decomposition scheme where EMD is implemented twice in Fourier domain, to resist the special attack. Recently, Fatima and Nishchal [24] discussed vulnerability of EMD to the specific attack and its variants that overcome the vulnerability to the attack. Recently, Rahekja et al. [25–27] used modified equal modulus decomposition scheme in hybrid domain.

Attempts to explore the application of fractional Hartley transform (FrHT) in the area of image encryption has been made in recent years. Zhao et al. [28] proposed redefined fractional Hartley transform for image encryption as FrHT does not satisfy the additive property. They also proposed its optical implementation. Li and Zhao [9] extended their work for color images. Thereafter, FrHT based schemes are proposed with, pixel scrambling operation [29,30], for double images [31], vector operation [32], phase images [33], and structured phase masks [34]. Recently, Singh et al. [35], and Yadav and Singh [36] proposed PTFT based asymmetric cryptosystem in FrHT domain.

This study proposes a novel watermarking scheme that uses modified equal modulus decomposition (MEMD) principle in the fractional Hartley domain. Further, it is claimed that there is no such watermarking scheme proposed in the literature till date. Modified equal modulus decomposition is used to resist the special attack. The rest of the paper is organized as follows: Section 2 gives basic definitions of fractional Hartley transform, and modified equal modulus decomposition. The proposed watermarking scheme and its validation on MATLAB are presented in Section 3. Results and discussion are reported in Section 4. Finally, Section 5 gives the main conclusions of the study.

2. The principle

Fractional Hartley transform, and modified equal modulus decomposition are the basic tools used in the proposed watermarking scheme which are briefly given as follows:

2.1. Fractional Hartley transform

Hartley transform is a real valued transform whereas fractional Hartley transform $(FrHT)$ is complex valued. The two dimensional $FrHT$ of a plaintext $f(x,y)$ is defined [28] as,

$$H^{r,s}(u,v) = \frac{\sqrt{(1-icot\phi_1)(1-icot\phi_2)}}{2\pi}$$
$$\exp\left[i\pi\left(\frac{u^2cot\phi_1}{\lambda f_{s1}}+\frac{v^2cot\phi_2}{\lambda f_{s2}}\right)\right]$$
$$\times\int_{-\infty}^{\infty}\int_{-\infty}^{\infty} exp\left(\frac{i\pi x^2cot\phi_1}{\lambda f_{s1}}+\frac{i\pi y^2cot\phi_2}{\lambda f_{s2}}\right)\left\{\frac{1-i\exp[i(\phi_1+\phi_2)/2]}{2}\right.$$
$$\times cas\left(\frac{ux\ csc\ \phi_1}{\lambda f_{s1}}+\frac{vy\ csc\ \phi_2}{\lambda f_{s2}}\right)+\frac{1+i\exp[i(\phi_1+\phi_2)/2]}{2}$$
$$\left.\times cas\left(-\frac{ux\csc\phi_1}{\lambda f_{s1}}-\frac{vy\csc\phi_2}{\lambda f_{s2}}\right)\right\}f(x,y)dxdy \tag{1}$$

where r and s are the fractional orders of $FrHT$, $\phi_1 = r\pi/2$ and $\phi_2 = s\pi/2$, $cas = cos + sin$. In optical implementation of FrHT, f_{s1} and f_{s2} are the focal lengths of lenses in the x and y directions respectively, and λ is the wavelength of the input light. Zhao et al. [28] redefined $FrHT$ in terms of fractional Fourier transform ($FrFT$), which is as follows:

$$H^{r,s}(u,v) = \frac{1+\exp\left[\frac{i(\phi_1+\phi_2)}{2}\right]}{2}FrFT^{r,s}(u,v)$$
$$+\frac{1-\ \exp[i(\phi_1+\phi_2)/2]}{2}FrFT^{r,s}(-u,-v) \tag{2}$$

Period of fractional Hartley transform is 2. In optical implementation (eq. (2)), $FrHT$ is realized in four-channel way. Two channels represent $FrFT^{r,s}(u,v)$ and $\exp[i(\phi_1+\phi_2)/2]FrFT^{r,s}(u,v)$ expressions, and the other two channels represent $FrFT^{r,s}(-u,-v)$ and $\exp[i(\phi_1+\phi_2)/2]FrFT^{r,s}(-u,-v)$. Optical implementation of $FrFT^{r,s}(u,v)$ is well-known [37,38], whereas $FrFT^{r,s}(-u,-v)$ is obtained using cube corner prism by rotating the field of $FrFT^{r,s}(u,v)$ through π.

2.2. Modified equal modulus decomposition

Cai *et al.* [17] proposed an asymmetric image encryption referred to as equal modulus decomposition. A plaintext $f(x,y)$ is first bonded with a random phase mask (RPM) and then Fourier transformed (Fig. 1).

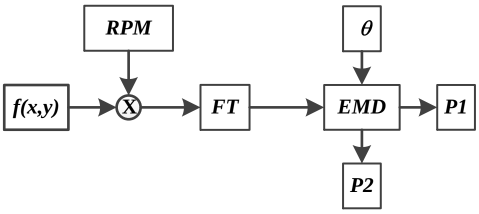


Fig. 1. Flowchart of the encryption scheme of equal modulus decomposition (Cai et al. [17]*)*

The resulting image $F(u,v)(=A(u,v)\exp(i\varphi(u,v))$, with the help of random distribution function $\theta(u,v)$ uniformly distributed in the interval $[0,2\pi]$, is decomposed into two masks $P1$ and $P2$ given by:

$$P1=\frac{A(u,v)/2}{\cos(\varphi(u,v)-\theta(u,v))}e^{i\theta(u,v)}$$

$$P2=\frac{A(u,v)/2}{\cos(\varphi(u,v)-\theta(u,v))}e^{i(2\varphi(u,v)-\theta(u,v)})$$

$P1$ is taken as ciphertext and $P2$ acts as a private key. The principle behind EMD is well-explained by Cai *et al.* [17]. From Fig. 2, $P1+P2=A(u,v)\exp(i\varphi(u,v))$, and therefore, the decryption process can be explained as $f(x,y)=|FT^{-1}(P1+P2)|$, where FT^{-1} is the inverse Fourier transform. The optical set-up of decryption process is given in Fig.3. It consists of two spatial light modulators (SLMs) to display the $P1$ and $P2$, one beam splitter, lens and charge-coupled device (CCD). The two monochromatic coherent light beams, which are placed in the Fourier plane interfere with each other and the plaintext is recorded by intensity detector.

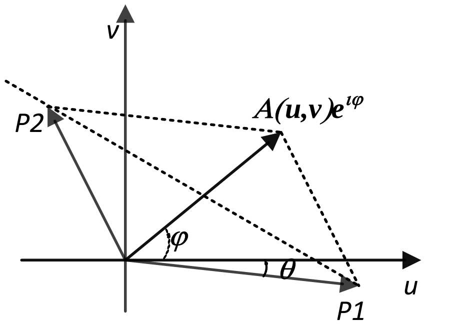


Fig. 2. Principle of equal modulus decomposition

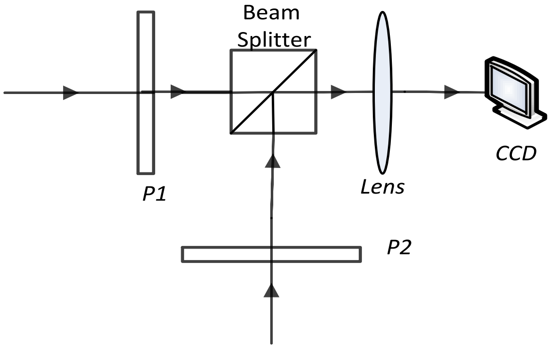


Fig. 3. Optical setup of the decryption process of the equal modulus decomposition

Deng [18], and Wu et al. [19] have shown that single EMD is vulnerable to special attack as its ciphertext reveals information such as amplitude which is the same for private key. Recently, Cai and Shen [23] modified the EMD by cascading the asymmetric unit twice (Fig.4). In this asymmetric cryptosystem, RPM, θ_1, and θ_2 act as public keys whereas $P1$ and $Q2$ are the private keys. PT and PR are respectively the phase truncation and phase reserve operations. It is worth noting that they have taken $P1$ as a private key in the first unit in place of $P2$ as in EMD. They have shown that the scheme also resists the special attack.

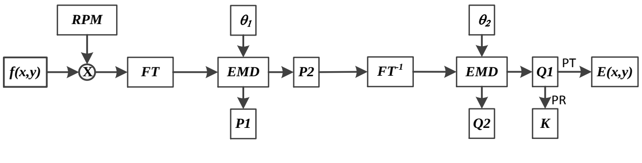


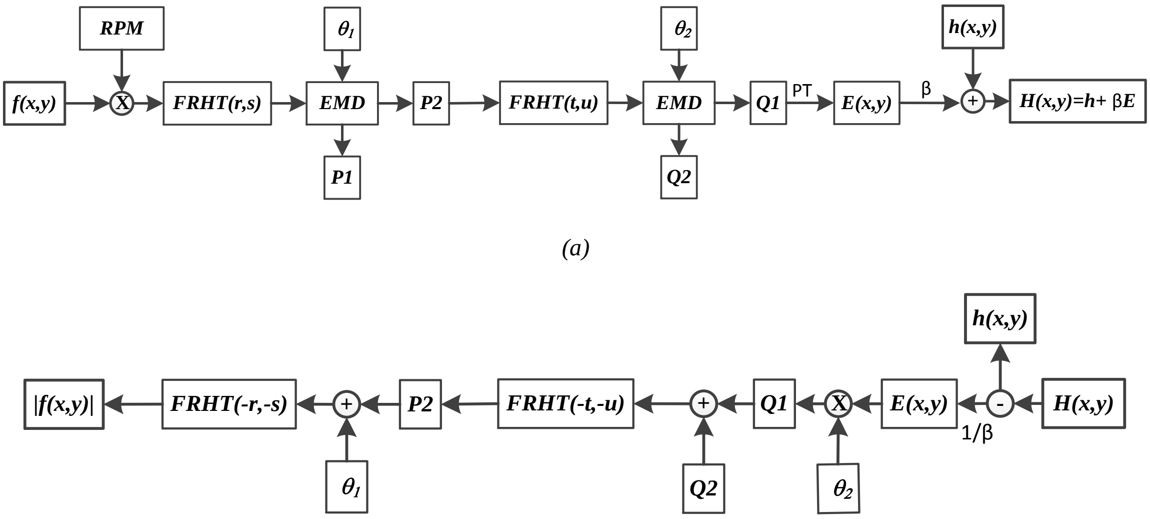
Fig. 4. Flowchart of the encryption scheme of modified equal modulus decomposition

3. The scheme and its validation

A schematic diagram of the proposed watermarking scheme is presented in Fig. 5. In the encryption process (Fig.5a), an input grayscale image is first bonded with a random phase mask and then FrHT of order (r,s) is implemented on it. By using a random distribution function $\theta_1(u,v)$ which is uniformly distributed in the interval $[0,2\pi]$, first EMD decomposes the resulting image in two masks $P1$ and $P2$ as explained in previous subsection. $P2$ undergoes another $FrHT$ of order (t,u) and then EMD with the help of another random distribution function $\theta_2(x,y)$. $Q1$ and $Q2$ denote the resulting masks from the second EMD. $Q2$ serves as the private key and $Q1$ undergoes phase reservation and phase truncation operations. The phase truncated part $E(x,y)$ of $Q1$ is embedded in a host image $h(x,y)$ with an attenuation factor β, resulting in a watermarked image $H(x,y)$ in the spatial domain.

$$H(x,y) = h(x,y) + \beta\, E(x,y)$$

In the decryption process (Fig. 5 b), the host image $h(x,y)$ is extracted from the watermarked image $H(x,y)$ and the obtained image is divided by the attenuation factor β to get $E(x,y)$. A phase function with angle $\theta_2(x,y)$ which is a public key, is multiplied with $E(x,y)$ and the private key $Q2$ added to the resulting image followed by inverse $FrHT$ with orders $(-t,-u)$, to get $P2$. The first private key P1 is then added to $P2$ and subjected to inverse fractional Hartley transform with orders $(-r,-s)$. Absolute part of the resulting image is our recovered image.



(a)

(b)

Fig. 5. Flowchart of encryption (a) and decryption scheme (b)

We performed validation of the proposed scheme on MATLAB (R2017b) using grayscale images of size 256×256 pixels. Images of Lena and Cameraman are used as plaintext and host image respectively. For simplicity, $FrHT$ orders are taken as $r = s = 0.3$ and $t = u = 0.6$, and $\beta = 0.5$ in our simulation. Various steps of the watermarking scheme are shown pictorially in Fig. 6. It is worth noting that the encrypted image $E(x,y)$, shown at the last step, is a random white stationary noise, and the watermarked and the host images appear identical.

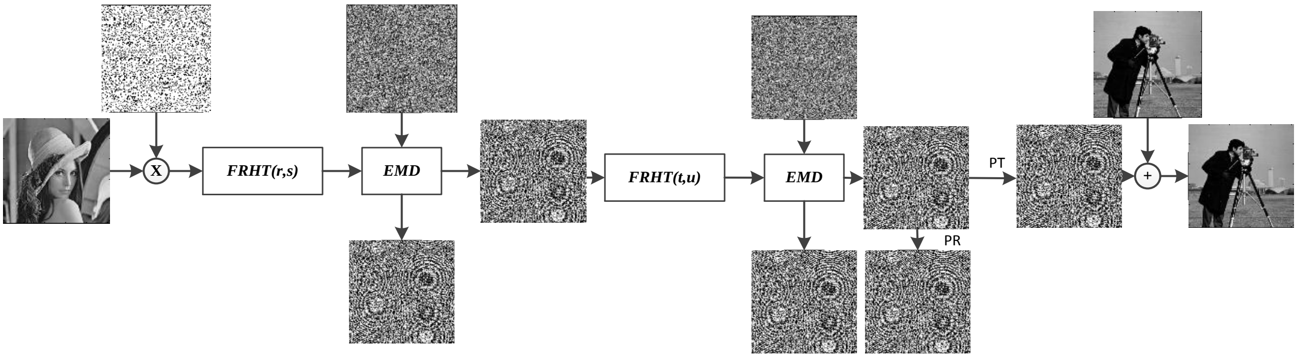


Fig. 6. Encryption scheme with input of image Lena and host image of cameraman

The recovered image of Lena is shown in Fig. 7 and correlation coefficient CC between the recovered image and the plaintext is 1. We observe that the decrypted image shows a faithful recovery of the input image, thus validating the scheme.

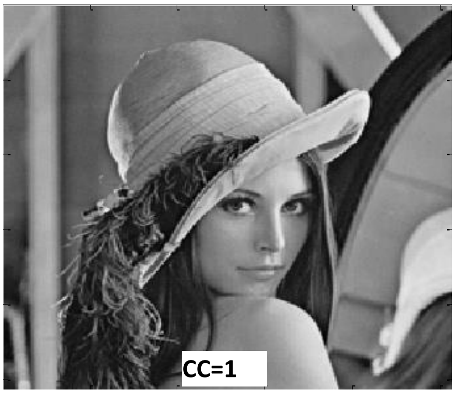


Fig. 7. Recovered image from the decryption setup

4. Results and discussion

In this section, an analysis of histogram and autocorrelation plots, entropy, keys sensitivity, and various attacks is performed on the scheme. Results are presented in terms of metrics such as mean-squared-error (MSE) and correlation coefficient (CC) which are defined as follows:

$$MSE = \frac{1}{N\times N}\sum_{x=1}^{N}\sum_{y=1}^{N}|I_o(x,\ y)\ -\ I_r(x,\ y)|^2 \quad (3)$$

$$CC = \frac{cov(I_O,I_r)}{\sigma(I_O)\sigma(I_r)} \quad (4)$$

where 〖 I〗 _o (x,y) and $\mathrm{I_r}(x,y)$ denote respectively the pixel values of the plaintext and the recovered image of size N × N pixels. Here, cov is covariance and σ is the standard deviation.

4.1. Statistical attack

Statistical analysis based on histograms and autocorrelation peak plot has been performed to test the efficacy of the proposed scheme. For a good watermarking scheme, histogram of the host image should be same as that of the watermarked image. Fig. 8 a-c show the histograms of respectively the input, host image, and watermarked images. It is clearly visible that the histograms of the host image, and the watermarked image are the same. Another criterion used for evaluation of a scheme is the autocorrelation peak. Information hidden in the proposed invisible watermarking scheme is the encrypted image $E(x,y)$. Fig. 8 d gives autocorrelation peaks for the encrypted image $E(x,y)$. These peaks are very weak, and therefore the encryption scheme has strong decorrelation power and can resist the statistical attacks [21].

4.2. Entropy analysis

Information entropy serves as an effective statistical measure of randomness to characterize the texture of an image. Entropy of a grayscale image lies in the range (0-8). Higher entropy indicates greater randomness in an image. Information entropy H(m) of a source m is defined as

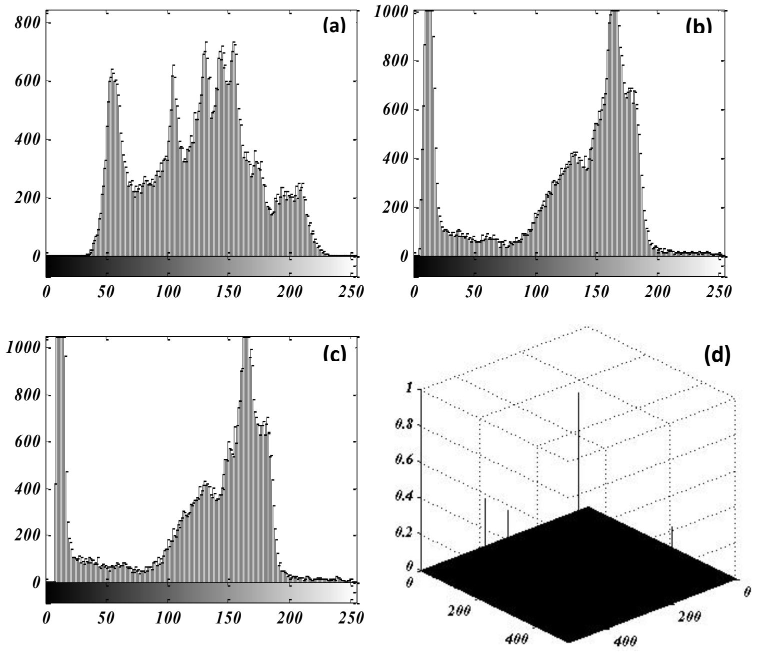


Fig. 8 Histograms of (a) input image, (b) host image, (c) watermarked image. (d) Autocorrelation of the encrypted image E

$$\mathrm{H(m)} \ = \ \sum_{\mathrm{k=1}}^{256} \mathrm{P(m_k)log_2} \frac{1}{\mathrm{P(m_k)}} \qquad (5)$$

The scheme consists of the private key $Q2$, the attenuation factor β, and the four fractional Hartley orders $\mathrm{r, s, t, u}$. Fig. 9 shows the decrypted images corresponding to minimal changes in these parameters. Correlation coefficients CC between the plaintext and the recovered image are also depicted on each picture. It is observed from the figure that with a slight change in any one of the parameters of the scheme, the recovered image is unrecognizable and corresponding CC values are close to zero. If all correct parameters of the scheme are provided, we get a faithful recovery (Fig. 9 f). Sensitivity plots of attenuation factor β, and FrHT orders $\mathrm{r, t}$ are presented in Fig. 10. Fig. 10 a shows the CC values on ordinate with respect to β on the abscissa varying with 10^{-4}. It is observed from the figure that the proposed scheme is very sensitive to the attenuation factor. *MSE* plots of *FrHT* orders t and r are shown in Fig. 10 b, c. Results indicate that the scheme is also sensitive to *FrHT* orders.

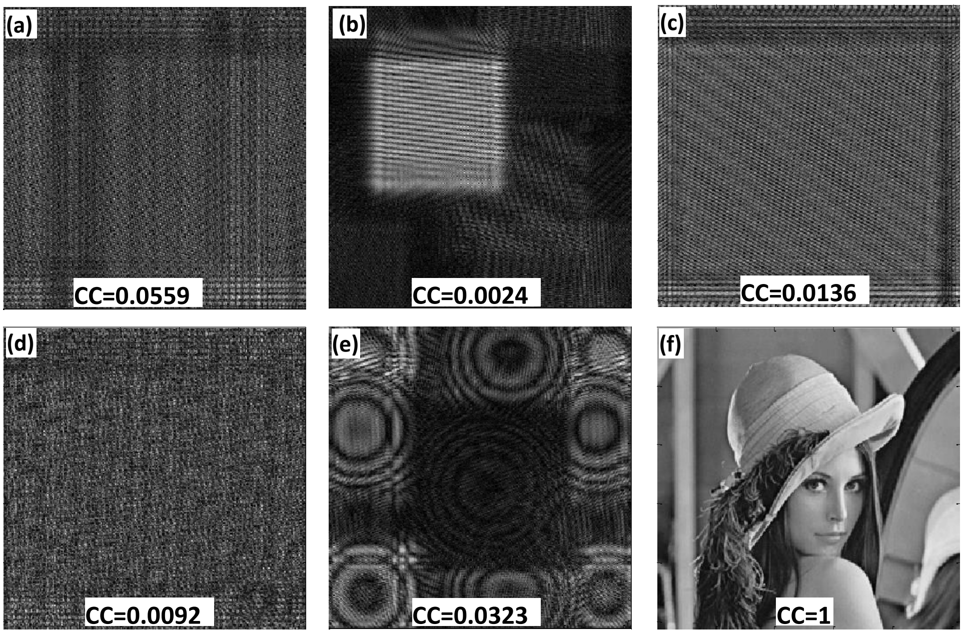


Fig. 9 Decrypted images when (a) wrong β ($\beta = 0.5001$ in place of correct $\beta = 0.5$); (b) wrong $P1$ ($P2$ is used in place of $P1$); (c) wrong private key $Q2$ ($Q1$ is used in place of $Q2$); (d) wrong phase θ_2 ($random\ matrix$ is used in place of θ_2); (e) wrong $FRHT$ order t ($t = t + 0.01$ is used); (f) all correct keys

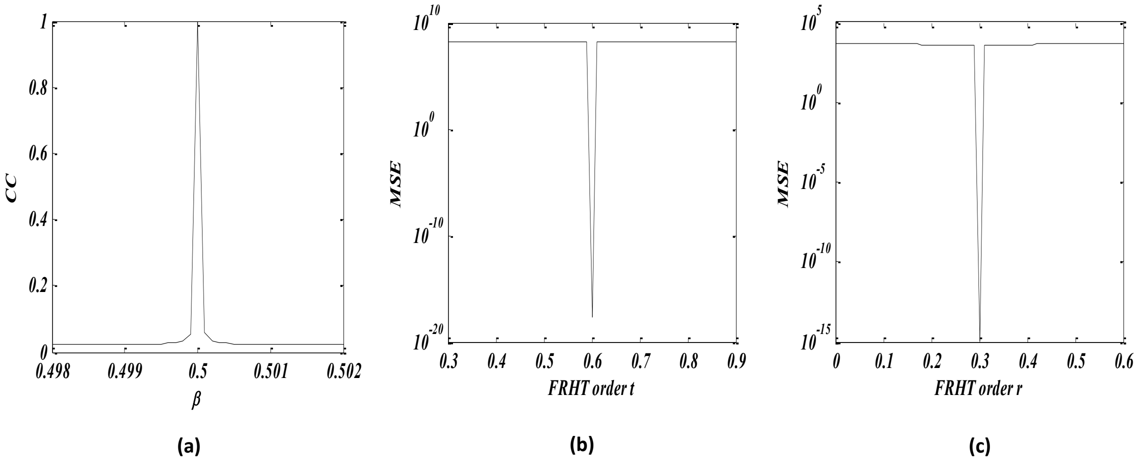


Fig. 10. Sensitivity plots of (a) attenuation factor β and (b,c) fractional Hartley orders t, r

4.4. Attack analysis

A scheme is said to be secure if it can endure basic attacks like brute-force attack, noise attack, known-plaintext attack, and ciphertext-only attack etc. Since the proposed watermarking scheme is asymmetric in nature, it must resist the special attack also. Singh *et al.* [33] have shown that a scheme consisting of $FrHT$ can endure brute-force attack for a reasonable time. Also, this scheme consist of attenuation factor which is very sensitive (Fig.10 a) to its value. Therefore, the proposed watermarking scheme endures the brute-force attack. Fig. 11 shows the results of noise attack on the scheme. It is worth noting that the normal random noise N with mean 0 and standard deviation 1 is added to the encrypted image $E(x, y)$ with strength α agiven by the equation as follows:

$$E^* = E + \alpha N \tag{6}$$

where E^* is noise-effected encrypted image. Fig. 11 (a-d) give the recovered images with noise strength 10, 30, 50, and 70 respectively. It is clearly evident that the input image of Lena is recognizable even in presence of high noise ($\alpha = 70$). A correlation coefficient CC versus noise strength α plot is given in Fig. 11e. From these results, we can easily infer that the proposed watermarking scheme endures the noise attack.

In the present scheme, public keys $\{RPM, \theta_1$ and $\theta_2\}$ would be same for any input image, whereas private keys $\{Q2, \beta$ and $FrHT$ orders$\}$ vary with input images. Therefore, extracting private keys using a given set of plaintext-ciphertext is meaningless for an asymmetric scheme and as a result, known-plaintext attack and chosen-ciphertext attacks are not applicable on the scheme. Deng [18] showed that with the help of ciphertext and public key, single EMD can be breached by the special attack. With a guess of private key whose modulus is same as that of the ciphertext, and using iterative method, plaintext is successfully recovered. Later Wu *et al.* [19] also performed cryptanalysis on a single EMD scheme and shown that it is vulnerable to the special attack. Cai and Shen [23] modified EMD by cascading EMD twice and changing the private key for the first EMD. They have shown that their scheme endured the special attack. Since our scheme uses modified EMD in fractional Hartley domain, it also resists the special attack. The computation time has been obtained on a personal computer with the following configuration: i7-8700 processor, 8 GB RAM, 3.19 GHz, MATLAB2017b, Window 10 etc. We have compared the computation time of Singh et al. [33], Cai and Shen [23] with the present results in Table 1.

Table 1. Comparison of computation time (sec) of the present scheme with the existing literature.

Time for	Singh et al. [33] (without watermarking)	Cai and Shen [23] (without watermarking)	Present Scheme
Encryption	1.38	0.35	0.92
Decryption	1.13	0.03	0.37

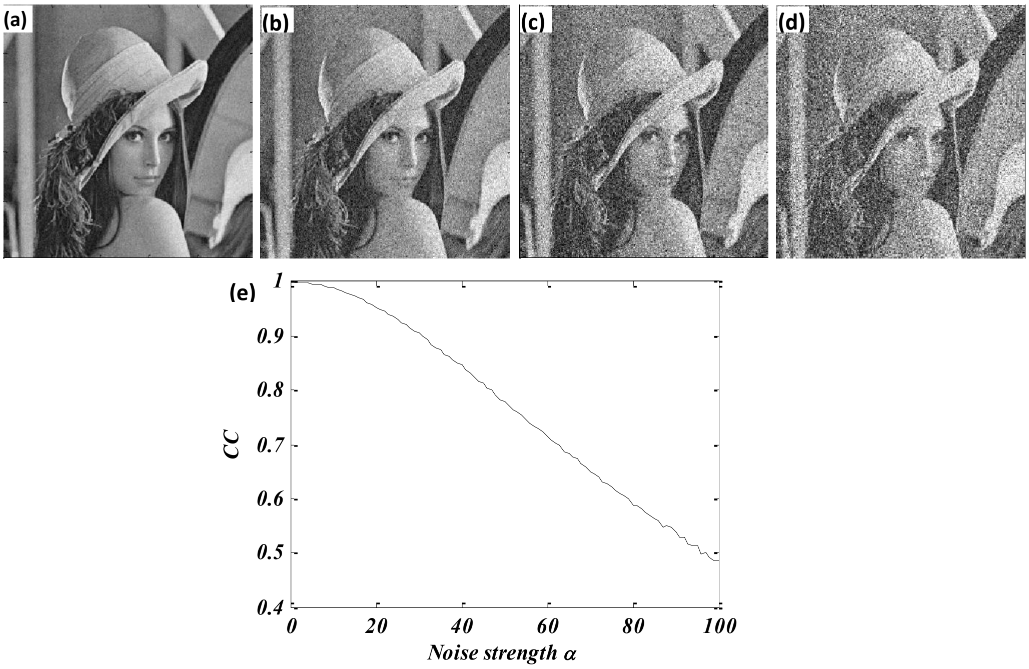


Fig. 11. Decrypted images when encrypted image is attacked with noise strengths α: 10, 30, 50 and 70 respectively in (a-d). Plot of CC versus noise strength is presented in (e)

5. Conclusions

A new asymmetric invisible watermarking scheme in fractional Hartley domain is presented in this paper. Modified equal modulus decomposition is used to resist the special attack. The scheme is validated for grayscale images through experiments performed on MATLAB (R2017b). Results show that the scheme is very sensitive to the private keys, attenuation factor, and orders of fractional Hartley transform. Entropy of the encrypted image is 7.9953, very near to its perfect value of 8. Histograms and autocorrelation plot establish that the scheme resists the statistical attack. The present scheme is also tested for its robustness to the noise attack. Results shown in terms of the recovered image and correlation coefficient plot indicate that the scheme resists a high level of noise in the encrypted image. Brute-force attack, known-plaintext attack, ciphertext-only attack, and the special attack are also discussed in the paper. Endurance to all these attacks establishes that the proposed watermarking scheme is secure.

References

[1] W. Chen, B. Javidi, X. Chen, Adv. Opt. Photonics **6**, 120 (2014).

[2] B. Javidi, A. Carnicer, M. Yamaguchi, T. Nomura, E. Pérez-Cabré, M. S. Millán, N. K. Nishchal, R. Torroba, J. F. Barrera, W. He, X. Peng, A. Stern, Y. Rivenson, A. Alfalou, C. Brosseau, C. Guo, J. T. Sheridan, G. Situ, M. Naruse, T. Matsumoto, I. Juvells, E. Tajahuerce, J. Lancis, W. Chen, X. Chen, P. W. H. Pinkse, A. P. Mosk, A. Markman, J. Opt. **18**, 083001 (2016).

[3] P. Kumar, J. Joseph, K. Singh, in Linear Canonical Transforms, Edited by J. J. Healy, M. Alper Kutay, H. M. Ozaktas, J. T. Sheridan, New York, NY, Springer New York (2016), p. 367.

[4] P. Refregier, B. Javidi, Opt. Lett. **20**, 767 (1995).

[5] N. Towghi, B. Javidi, Z. Luo, J. Opt. Soc. Am. A **16**, 1915 (1999).

[6] B. M. Hennelly, J. T. Sheridan, Opt. - Int. J. Light Electron Opt. **114**, 251 (2003).

[7] G. Unnikrishnan, J. Joseph, K. Singh, Opt. Lett. **25**, 887 (2000).

[8] L. Chen, D. Zhao, Opt. Lett. **31**, 3438 (2006).

[9] X. Li, D. Zhao, Optik - Int. J. Light Electron Opt. **121**, 673 (2010).

[10] Z. Liu, Q. Guo, L. Xu, M. A. Ahmad, S. Liu, Opt. Express **18**, 12033 (2010).

[11] N. Zhou, Y. Wang, L. Gong, Opt. Commun. **284**, 3234 (2011).

[12] I. Mehra, N. K. Nishchal, Opt. Express **22**, 5474 (2014).

[13] A. K. Yadav, S. Vashisth, H. Singh, K. Singh, Opt. Commun. **344**, 172 (2015).

[14] W. Qin, X. Peng, Opt. Lett. **35**, 118 (2010).

[15] X. Wang, D. Zhao, Opt. Commun. **285**, 1078 (2012).

[16] X. Wang, Y. Chen, C. Dai, D. Zhao, Appl. Opt. **53**, 208 (2014).

[17] J. Cai, X. Shen, M. Lei, C. Lin, S. Dou, Opt. Lett. **40**, 475 (2015).

[18] X. Deng, Opt. Lett. **40**, 3913 (2015).

[19] J. Wu, W. Liu, Z. Liu, S. Liu, Appl. Opt. **54**, 8921 (2015).

[20] H. Chen, C. Tanougast, Z. Liu, L. Sieler, Opt. Lasers Eng. **93**, 1 (2017).

[21] S. P. Barfungpa, M. R. Abuturab, Opt. Quantum Electron. **48**, 520 (2016).

[22] A. Fatima, I. Mehra, N. K. Nishchal, J. Opt. **18**, 085701 (2016).

[23] J. Cai, X. Shen, Opt. Laser Technol. **95**, 105 (2017).

[24] A. Fatima, Naveen K. Nishchal, in *A*dvanced Secure Optical Image Processing for Communications, Edited by A. Al Falou, IOP Publishing, 5 (2018).

[25] P. Rakheja, R. Vig, P. Singh, Optik **176**, 425 (2019).

[26] P. Rakheja, R. Vig, P. Singh, R. Kumar, Opt. Quantum Electron. **51**, 204 (2019).

[27] P. Rakheja, R. Vig, P. Singh, J. Mod. Opt. **66**, 799 (2019).

[28] D. Zhao, X. Li, L. Chen, Opt. Commun. **281**, 5326 (2008).

[29] P. Singh, A. K. Yadav, K. Singh, I. Saini, AIP Conf. Proc. **1802**, 020017 (2017).

[30] P. Singh, A. K. Yadav, K. Singh, Opt. Appl. **47**, 421 (2017).

[31] J. M. Vilardy, C. O. Torres, C. J. Jimenez, in Proc. SPIE 8785, 8th Iberoamer. Opt. Meet. 11th Lat.Amer. Meet. Opt. Las. Appl. **8785,** 87851R (2013).

[32] Y. Liu, J. Du, J. Fan, L. Gong, Multimed. Tools Appl. **74**, 3171 (2015).

[33] P. Singh, A. K. Yadav, K. Singh, Opt. Lasers Eng. **91**, 187 (2017).

[34] A. K. Yadav, P. Singh, K. Singh, J. Opt. **47**, 208 (2018).

[35] A. K. Yadav, P. Singh, I. Saini, K. Singh, J. Mod. Opt. **66**, 629 (2019).

[36] P. L. Yadav, H. Singh, 3D Res. **9**, 1 (2018).

[37] D. Mendlovic, H. M. Ozaktas, J. Opt. Soc. Am. A **10**, 1875 (1993).

[38] H. M. Ozaktas, D. Mendlovic, J. Opt. Soc. Am. A **10**, 2522 (1993).

*Corresponding author: phoolsingh@cuh.ac.in