

# Separable and Three-Dimensional Optical Reversible Data Hiding with Integral Imaging Cryptosystem

Liu Yiqun<sup>(✉)</sup>

Key Laboratory of CAPF for Cryptology and Information Security,  
Department of Electronic Technology, Engineering University of Chinese Armed  
Police Force, Xi'an, Shaanxi 710086, China  
wjliuyiqun@126.com

**Abstract.** Reversible data hiding in encrypted domain (RDH-ED) is an important and effective technical approach for security data management of cloud computing, big data and privacy protection. This paper proposes a three-dimensional (3D) optical reversible data hiding (RDH) with integral imaging cryptosystem. The secret data is encrypted and embedded into the cover image. The receivers can decrypt the cover image and secret data with a reversible or lossless manner, respectively. The simulation experiment and results show that the data embedding rate can be increased to one. Besides, the quality of image decryption is quite high. The technique boasts the advantages of high data embedding rate, security level and real-time capability.

**Keywords:** 3D-ORDH-InImC · Reversible data hiding in encrypted domain (RDH-ED) · Three-dimensional optical information hiding

## 1 Introduction

The security of information systems is increasingly crucial in our lives, as everything is going to be connected to the Internet [1–4]. Barton presented the concept of reversible data hiding (RDH) for the first time in his patent in 1997 [5]. He adopted the lossless compression technology to create more redundant space in image and realized reversible hiding of carrier image and secret information. After that, RDH gradually becomes a new hot spot of information hiding research field. According to the current research situations, RDH can be divided into six categories [6], i.e., RDH of spatial domain, RDH of compressed domain, semi-fragile RDH, RDH of cipher-text domain, RDH of audio and video, and RDH of contrast enhancement type. The existing reversible information methods of spatial domain mainly include RDH of difference expansion, RDH of histogram shifting, RDH of lossless image compression and RDH of contrast enhancement.

RDH-ED is an important and effective technical approach for security data management of cloud computing, big data and privacy protection. The existing methods include RDH method based on private key cipher [7–9] and RDH method based on public key cipher [10, 11]. Zhang Xinpeng et al. [7] jointed encryption and information

hiding technology, and put forward a RDH algorithm in cipher images, which owned the advantage of convenient operation and could meet the reversible requirements. However, the encryption algorithm was too simple and image decryption was required before the secret image was extracted. As a result, steganography load and steganography quality were greatly limited by cipher image. The literatures [10–12] utilized encryption carrier data of public key cipher and homomorphic encryption embedding information. The algorithm led to obvious expansion of encrypted data volume, complex computation and low embedding capacity. The literatures [7, 8, 13, 14] carried out pre-processing to compress partial data before image encryption and then hid information. It could guarantee the reversibility. However, it couldn't be regarded as a method for the encryption domain. The true information hiding of encryption domain shall be carried out completely in the encryption domain, and no characteristic should be public when the carrier data is in plaintext state. But many algorithms for the cipher-text domain fail to deal with this problem.

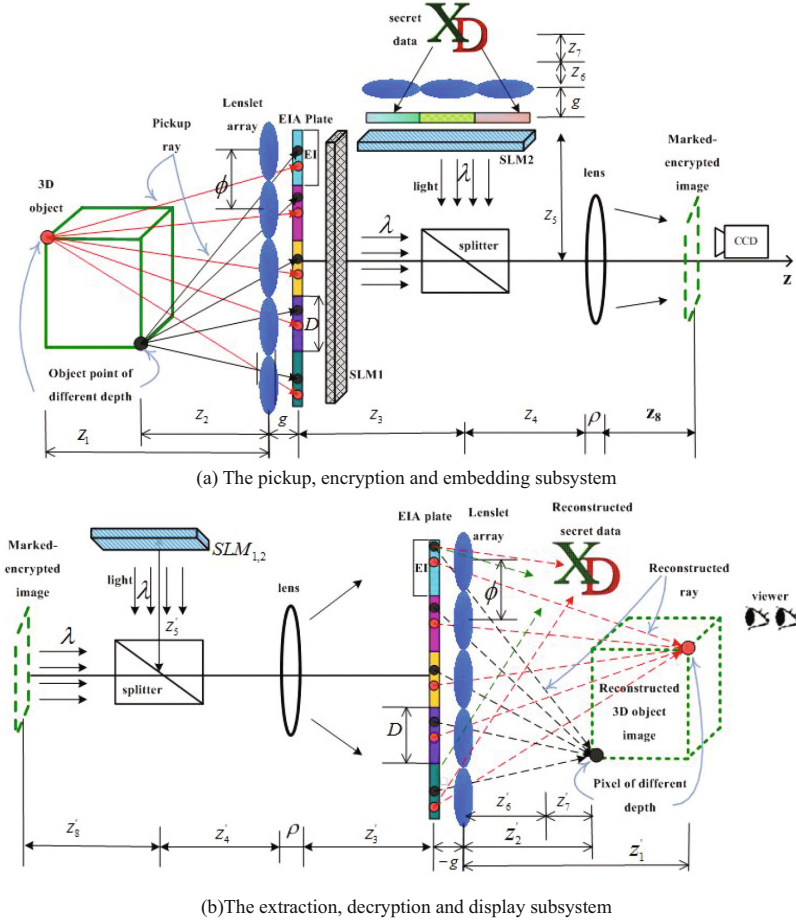
The main motivation for using optical technology of optics and photonics for information security is that optical waveforms possess many complex degrees of freedom such as amplitude, phase, polarization, nonlinear transformations, quantum properties of photons, and multiplexing that can be combined in many ways to make information encryption more secure and more difficult to attack [15, 16]. Among published research reports, patents and literatures [1–4, 6, 17–21], there are few researches on jointing optical technologies, integral imaging and RDH, not to mention three-dimensional multimedia RDH. Therefore, it's worthy taking full advantage of optical technologies for three-dimensional RDH technology based on integral imaging cryptosystem.

This paper proposes a three-dimensional optical reversible data hiding with integral imaging cryptosystem (3D-ORDH-InImC). We have researched on the technical principles, implementation algorithm and implement workflows of 3D-ORDH-InImC. They are introduced in detail. Finally, the simulation experiment was done, and the results proved that the data embedding rate could be approximately increased to 1, which was higher than that of the existing methods by about 60%. Besides, the image decryption quality was quite high. We also further analyzed influence of change in key space element on image decryption quality. The system boasts the advantages of high data embedding rate, computation efficiency, security level and real-time capability, and thus can meet the performance requirements of RDH. The current state of the arts, it is the first scheme on jointing the integral imaging and RDH in cipher-text domain.

## 2 The Principle of the Proposed Scheme

The 3D-ORDH-InImC is designed and shown in Fig. 1. It is divided into two subsystems. Figure 1 (a) is the pickup, encryption and embedding subsystem and Fig. 1 (b) is the extraction, decrypted and display subsystem.

Therein, A and B represent the two planes which separate spatially in the direction of propagation.  $s$ ,  $t$ ,  $z_{AB}$  and  $\lambda$  denote the sampling number of two adjacent orthogonal pixels, the spacing between the planes, the wavelength of incident light, respectively. We define correlation sampling lengths of the input plane along the  $x$  and  $y$  axes as  $\Delta x$



**Fig. 1.** The schematically of 3D-ORDH-InImC

and  $\Delta y$ , and the Fourier plane along the  $\xi$  and  $\eta$  axes in Fresnel transform domain (FTD) as  $\Delta\xi$  and  $\Delta\eta$ , respectively.  $C$  is a complex constant whose value may be calculated by the formula (2).

$$\begin{aligned}
 DFD[A, B, s, t; z_{AB}, \lambda] &= \frac{\exp[j2\pi z_{AB}/\lambda]}{j\lambda z_{AB}} \times \exp[j\frac{\pi}{\lambda z_{AB}}(s^2\Delta\xi^2 + t^2\Delta\eta^2)] \\
 &\times \sum_{q=0}^{N-1} \sum_{l=0}^{N-1} U_A(q, l) \exp[j\frac{\pi}{\lambda z_{AB}}(q^2\Delta x_0^2 + l^2\Delta y_0^2)] \times \exp[-j2\pi(\frac{qs}{N} + \frac{lt}{N})]
 \end{aligned} \quad (1)$$

Where

$$C = \frac{\exp[j2\pi z_{AB}/\lambda]}{j\lambda z_{AB}} \quad (2)$$

As we all know, since  $DFD[A, B, s, t; z_{AB}, \lambda]$  is complex value in Formula (1), it pickups both the amplitude and phase information of the result signal in the optical implementation described in Fig. 1.

In order to improve security of the cryptosystem, the EIA images are encrypted by Discrete 2D-logistic [22] algorithm. The most important characteristics of chaos encryption algorithm are efficiency and high speed in encryption. It is especially applicable to real-time communication [22]. Therefore, the plain-text images are encrypted with Discrete 2D-logistic algorithm and these cipher-text images are marked as  $W_1(x, y)$ ,  $W_2(x, y)$ .

$$\begin{aligned} G_{RDH}(\omega, \gamma) = & \{ \alpha_1 DFD[W_1(x, y), L(x, y), s, t; z_{W_1}, \lambda] \\ & + \alpha_2 DFD[W_2(x, y), L(x, y), s, t; z_{W_2}, \lambda] + \alpha_3 DFD[R_1(x, y), L(x, y), s, t; z_{R_1}, \lambda] \\ & + \alpha_4 DFD[R_2(x, y), L(x, y), s, t; z_{R_2}, \lambda] \} \times T(s, t; f) \end{aligned} \quad (3)$$

Assume that  $W_1(x, y)$ ,  $W_2(x, y)$ ,  $R_1(x, y)$ ,  $R_2(x, y)$ ,  $L(x, y)$  represent planes in different position, respectively.  $s, t$  are the number of pixel samples.  $z_j$  represents the distance between the different planes, where  $j = 1, 2, \dots, 9$ ,  $W_1, W_2, R_1, R_2$ . These symbols  $z_{W_1} = z_{R_1} = z_3 + z_4$ ,  $z_{W_2} = z_{R_2} = z_5 + z_4$  and  $g$  represent the distance between the lenslet array and elemental image plane.  $D$  represents the size of elemental images.  $\phi$  represents lenslet spacing. The focal length of the imaging lens  $\rho$  is  $f$ ,  $\alpha_1, \alpha_2, \alpha_3, \alpha_4$  are encryption weighting factors, where  $\alpha_1 + \alpha_2 + \alpha_3 + \alpha_4 = 1$ . They are used to adjust the energy ratio among the DFD transforms of the cover image, 3D digital secret image and RPMP. The optical transfer function is  $T(s, t; f)$ .  $G_{RDH}(\omega, \gamma)$  is marked encrypted image that is encrypted cover images containing secret data or additional bits.

The three-dimensional decryption, extraction and display subsystem is shown in Fig. 1(b). The legal user can receive these marked encrypted images transmitted by the secure communication network, implement subtraction through contribution in embedding of RDH of two random phase mask plates, and then obtain cipher-text image according to Fourier transform and inverse Fresnel diffraction transformation theory, as shown in Eq. (5). The mathematical model of decryption can be represented with Eqs. (4)–(6). Implement decryption of EIA images of carrier image and secret image with the original value set by Discrete 2D-logistic. Finally, three-dimensional images can be displayed by the 3D-ORDH-InImC.

$$\begin{aligned} EW' = & G_{RDH}(\omega, \gamma) - DFD\{ \alpha_3 DFD[R_1(x, y), L(x, y), s, t; z_{R_1}, \lambda] \times T(s, t; f) \} \\ & - DFD\{ \alpha_4 DFD[R_2(x, y), L(x, y), s, t; z_{R_2}, \lambda] \times T(s, t; f) \} \end{aligned} \quad (4)$$

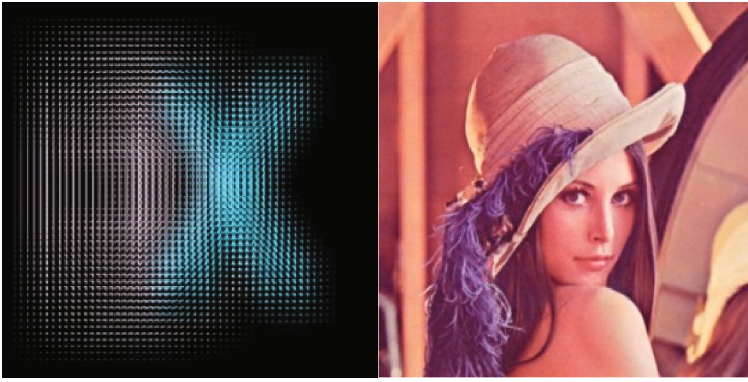
$$W' = IDFD[EW']|_{z=z'_{w_{1,2}}} \quad (5)$$

Among them, the diffraction distance  $z'_{W_{1,2}}$  can be calculated by the following formula:

$$\frac{1}{z_{W_{1,2}}} + \frac{1}{z'_{W_{1,2}}} = \frac{1}{f} \quad (6)$$

### 3 Experimental Results and Discussions

As shown in Fig. 2, Lena image and XD EIAs are chosen as the cover images and secrete images. Their sizes are all in  $512 \times 512$  pixels. Joint Photographic Experts Group (JPEG) is the image format.



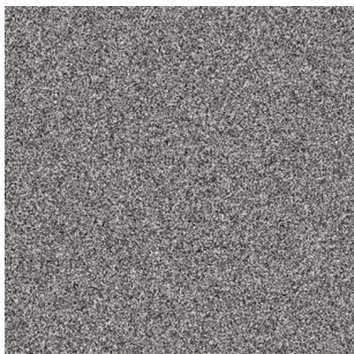
(a) XD EIA

(b) Lena

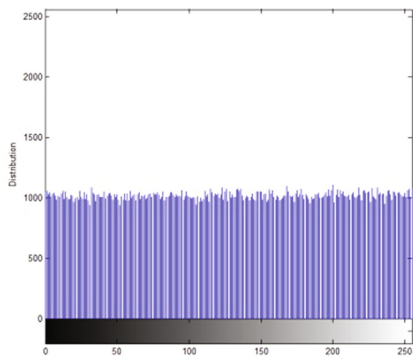
**Fig. 2.** Sample images of the experiments

XD EIAs are encrypted by discrete 2D-logistic algorithm. For analyzing the correlation of neighboring pixels, we chose scatter diagrams in the horizontal and vertical directions to characterize the correlation. Figure 3 shows correlation between neighboring pixels of plaintext images and cipher-text images. According to the above figures, neighboring pixels of plaintext images have large correlation, and distribution diagrams of cipher-text images are relatively uniform. They indicate the correlations of neighboring pixels in two directions are relatively small. Therefore, the encryption algorithm can greatly reduce pixel correlation of cipher-text images, improve the capability to resist the statistical analysis attacks, and meet the cipher-text image evaluation index requirements of histogram statistics and neighboring pixel correlation.

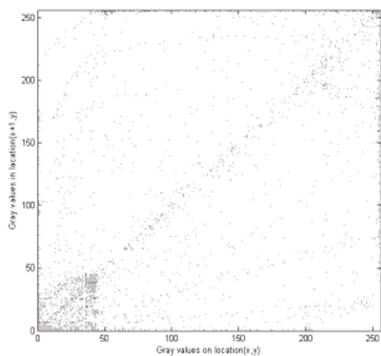
The security and robustness are improved by the proposed method. The linear characteristics of the  $4f$  system are enhanced with these techniques such as discrete 2D-logistic, DFD and double random phase coding, etc. That is to say, Plain images can be encrypted by scrambling the pixel position or pixel value replacement. Thus the integral security of the optical cryptosystem is improved. Discrete 2D-logistic



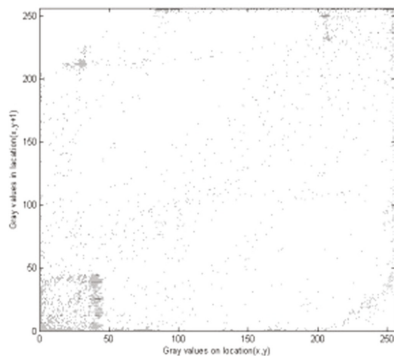
(a) single channel diagram of XD



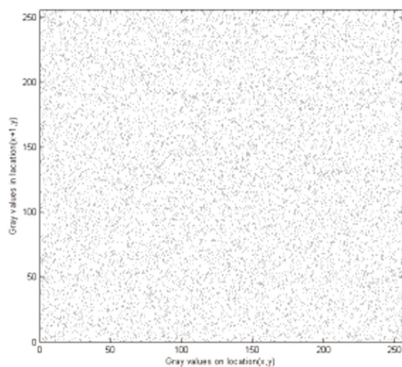
(b) histogram of XD



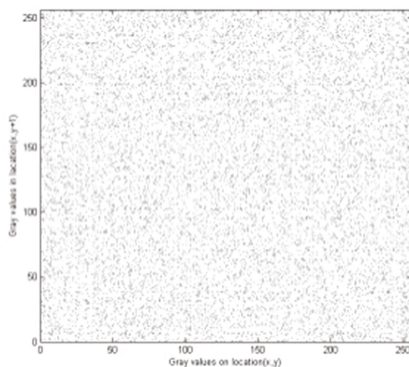
(c) horizontal correlation diagram of XD



(d) vertical correlation diagram of XD



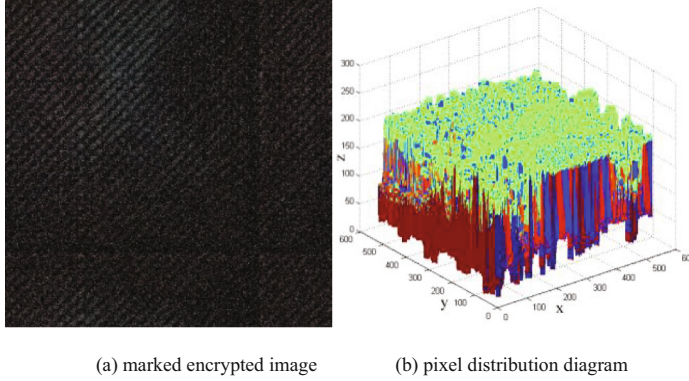
(e) horizontal correlation diagrams of encrypted XD



(f) vertical correlation diagrams of encrypted XD

**Fig. 3.** The correlation diagrams of XD and encrypted XD





**Fig. 4.** The pixel distribution diagram of the marked encrypted image

algorithm is a kind of digital image encryption technology based on the chaos theory, and it can enhance the system security. First, the higher the sensitivity of the original value of chaotic mapping, the smaller the correlation between neighboring pixels will be. After these images are scrambled, the better ergodic property, the larger randomness of scrambling image will be. Therefore, during the pixel scrambling, the sensitivity of the original value of chaotic mapping and ergodic property determine the scrambling intensity. Second, during the pixel scrambling and the pixel replacement, the more number of iterations, the higher the encryption intensity will be. At the same time, the exhaustion become more difficult than additional technologies and computing complexity is higher. It's necessary to trade off the security and computing complexity when users decide the number of iterations. Finally, the key sensitivity is determined by the parameter sensitivity when mapping parameters are used as the scrambling key. While key sensitivity will resolve security of the whole system. 3D-ORDH-InImC can improve the encryption performance and practicability. Figure 4(a) and (b) are marked encrypted image and pixel distribution diagram.

In the new method, the optical device parameters and functionality parameters of integral imaging system can be used as keys. These modulation parameters for secrete data embedding coefficient can also be used as keys. Multiple keys synthesizing the above mentioned keys will enhance security. It could be more difficult to crack. By redistributing signal energy and diffusing hidden signal energy embedded into transformation coefficients in spatial and temporal domains, the DFD embedding and extraction algorithm applied in the new method effectively resolves the contradiction between imperceptibility and robustness of information hiding. Thus, the new method can meet robustness and security requirements.

## 4 Conclusion

A three-dimensional (3D) optical reversible data hiding (RDH) with integral imaging cryptosystem is proposed. The secret data is encrypted and embedded into the cover image that is encrypted by 3D-ORDH-InImC. The receivers can decrypt the cover

image and secret data with a reversible or lossless manner, respectively. The simulation experiment and results prove that the data embedding rate can be increased to one. The technique boasts the advantages of high data embedding rate, security level and real-time capability. The proposed method can be used in such fields as three-dimensional new media information hiding and multimedia information security. This paper is a powerful new example for optical information security theory. In the future work, we'll research on characteristics of three-dimensional image cryptosystem from the perspectives of cryptanalysis and information theory, and then improve strategies for the system security. To the best of our knowledge, three-dimensional multimedia information security is developing forward from scientific theoretical research to engineering technology in spite of many challenges.

## References

1. Liu, Y., Wang, X., Zhang, J., Zhang, M., Luo, P., Wang, X.A.: An improved security 3D watermarking method using computational integral imaging cryptosystem. *Int. J. Technol. Hum. Interact. (IJTHI)* **12**, 1–12 (2016)
2. Pereira, R., Pereira, E.G.: Future internet: trends and challenges. *Int. J. Space-Based Situated Comput. (IJSSC)* **5**, 159–167 (2015)
3. Akase, R., Okada, Y.: WebGL-based 3D furniture layout system using interactive evolutionary computation and its user evaluations. *Int. J. Space-Based Situated Comput. (IJSSC)* **4**, 143–164 (2014)
4. Moore, P., Thomas, A., Tadros, G., et al.: Detection of the onset of agitation in patients with dementia: real-time monitoring and the application of big-data solutions. *Int. J. Space-Based Situated Comput. (IJSSC)* **3**, 136–154 (2013)
5. Barton, J.M.: Method and apparatus for embedding authentication information within digital data. In: US Patent. US: 1997
6. Shi, Y.-Q., Li, X., Zhang, X., et al.: Reversible data hiding: advances in the past two decades. *IEEE Access* 3210–3237 (2016)
7. Zhang, X.: Reversible data hiding in encrypted image. *IEEE Signal Process. Lett.* **18**, 255–258 (2011)
8. Lian, S., Liu, Z., Ren, Z., Wang, H.: Commutative encryption and watermarking in video compression. *IEEE Trans. Circuits Syst. Video Technol.* **17**, 774–778 (2007)
9. Cancellaro, M., Battisti, F., Carli, M., et al.: A commutative digital image watermarking and encryption method in the tree structured Haar transform domain. *Signal Process. Image Commun.* **26**, 1–12 (2011)
10. Memon, N., Wong, P.W.: A buyer-seller watermarking protocol. *IEEE Trans. Image Process.* **10**, 643–649 (2001)
11. Kuribayashi, M., Tanaka, H.: Fingerprinting protocol for images based on additive homomorphic property. *IEEE Trans. Image Process.* **14**, 2129–2139 (2005)
12. Jiayong, C., et al.: A secure image steganographic method in encrypted domain. *J. Electron. Inf. Technol.* **34**, 1721–1726 (2012)
13. Zhang, X., Long, J., Wang, Z., Cheng, H.: Lossless and reversible data hiding in encrypted images with public key cryptography. *IEEE Trans. Circuits Syst. Video Technol.* **26**, 1622–1631 (2015). 1
14. Ma, K., Zhang, W., Zhao, X., et al.: Reversible data hiding in encrypted images by reserving room before encryption. *IEEE Trans. Inf. Forensics Secur.* **8**, 553–562 (2013)



15. Markman, A., Carnicer, A., Javidi, B.: Security authentication with a three-dimensional optical phase code using random forest classifier. *J. Opt. Soc. Am. A* **33**, 1160–1165 (2016)
16. Javidi, B., Carnicer, A., Yamaguchi, M., et al.: Roadmap on optical security. *J. Opt.* **18**, 1–39 (2016)
17. Wang, Y., Du, J., Cheng, X., Lin, Z.L.K.: Degradation and encryption for outsourced PNG images in cloud storage. *Int. J. Grid Util. Comput.* **7**, 22–28 (2016)
18. Honarvar, A.R., Sami, A.: Extracting usage patterns from power usage data of homes' appliances in smart home using big data platform. *Int. J. Inf. Technol. Web Eng. (IJITWE)* **11**, 39–50 (2016)
19. Alamareen, A., Al-Jarrah, O., Aljarrah, I.A.: Image mosaicing using binary edge detection algorithm in a cloud-computing environment. *Int. J. Inf. Technol. Web Eng. (IJITWE)* **11**, 1–14 (2016)
20. Mola, L., Rossignoli, C., Carugati, A., Giangreco, A.: Business Intelligence System Design and its Consequences for Knowledge Sharing, Collaboration, and Decision-Making: An Exploratory Study. *Int. J. Technol. Hum. Interact. (IJTHI)* **11**, 1–25 (2015)
21. Balusamy, B., Krishna, P.V.: Collective advancements on access control scheme for multi-authority cloud storage system. *Int. J. Grid Util. Comput.* **6**, 133–142 (2015). Special Issue on Intelligent Grid and Cloud Computing
22. Sun, F., Liu, S.: Cryptographic pseudo-random sequence from the spatial chaotic map. *Chaos, Solitons Fractals* **41**, 2216–2219 (2009)

Advances in Internetworking, Data & Web Technologies  
The 5th International Conference on Emerging  
Internetworking, Data & Web Technologies  
(EIDWT-2017)

Barolli, L.; Zhang, M.; Wang, X.A. (Eds.)

2018, XXIX, 779 p. 291 illus., Softcover

ISBN: 978-3-319-59462-0