The following publication Y. Xiao, L. Zhou and W. Chen, "Single-Pixel Imaging Authentication Using Sparse Hadamard Spectrum Coefficients," in IEEE Photonics Technology Letters, vol. 31, no. 24, pp. 1975-1978, 15 Dec.15, 2019 is available at https://doi.org/10.1109/LPT.2019.2952177.

Single-pixel imaging authentication using sparse Hadamard spectrum coefficients

Yin Xiao, Lina Zhou, and Wen Chen

***Abstract*—We experimentally present optical authentication using a small number of Hadamard spectrum coefficients in single-pixel imaging (SPI). A method is applied to generate sparse Hadamard spectrum coefficients in the SPI. By randomly selecting and using a small number of Hadamard spectrum coefficients (e.g., less than 8.0% of Nyquist limit), information of an object (i.e., plaintext) can be effectively hidden in the decrypted object. Although the decrypted object cannot visually render information about the plaintext, it can be effectively authenticated. Optical experiment is conducted to verify feasibility and effectiveness of the proposed optical authentication method. It is expected that the proposed method can provide a promising insight for single-pixel optical authentication.**

***Index Terms*—Optical security, optical authentication, Hadamard transform, single-pixel imaging.**

I. Introduction

RECENTLY, single-pixel imaging (SPI), also called ghost imaging [1–7], has been studied and applied for optical encryption and authentication [9–12]. In single-pixel optical encryption schemes, plaintext can be encoded into a series of single-pixel intensity values instead of a complex-valued matrix or 2D intensity patterns. There are two significant advantages of the SPI in optical security: (1) 1D ciphertext is beneficial to storage and transmission, and (2) the reduction in dimension of ciphertext enhances system security. In conventional work using the SPI for optical security, random phase or amplitude-only masks are usually used as illumination patterns, and the number of measurements is still large. When Hadamard pattern is applied in the SPI, sparse property of Hadamard spectrum is utilized, which means that only a few significant components can represent the main information of an object [13]. Compared with other transform patterns, Hadamard transform pattern consisting of only binary values is easier to be generated by using spatial light modulator (SLM), or can be better displayed by using the digital micro-mirror devices [14–18]. However, differential Hadamard method is usually used to generate Hadamard spectrum coefficients in the SPI, and it is concerned that this could lead to the low sampling efficiency. In addition, applying Hadamard spectrum in the SPI for optical encryption-based authentication has not been explored before.

In this Letter, we experimentally present optical authentication using a small number of Hadamard spectrum coefficients in the SPI. A method is applied to generate sparse Hadamard spectrum coefficients in the SPI. By randomly selecting and using a small number of Hadamard spectrum coefficients, information of an object (i.e., plaintext) can be effectively hidden in the decrypted object. Although the decrypted object does not visually render information about the plaintext, nonlinear correlation conducted between the decrypted object and original object can effectively verify the decrypted object and the receiver. Optical experiment is conducted to verify feasibility and effectiveness of the proposed method.

II. Theories

The Hadamard transform of a target object $O(x,y)$, i.e., plaintext used in this study, can be described by

$$\mathbf{F}=\mathbf{HO}, \tag{1}$$

where $\mathbf{O}$ denotes the vectorized form of object $O(x,y)$, $\mathbf{H}$ denotes the fixed and standard Hadamard matrix, and $\mathbf{F}$ denotes the vectorized form of Hadamard spectrum coefficients. Since the Hadamard matrix $\mathbf{H}$ consists of full orthogonal bases, object reconstruction can be implemented by using inverse Hadamard transform.

$$\mathbf{O}=\mathbf{H}^{-1}\mathbf{F}. \tag{2}$$

The experimental setup used to realize Hadamard transform in the SPI is shown in Fig. 1, and the SPI process be described by

$$B=\sum_{x=0}^{N-1}\sum_{y=0}^{N-1}O(x,y)P'(x,y), \tag{3}$$

where B denotes the intensity value (i.e., ciphertext) detected by using a single-pixel bucket detector in optical experiment, N denotes dimension size of the horizontal or vertical direction of the object, and $P'(x,y)$ represents illumination pattern used in optical experiment. In optical experiment, the used illumination pattern is described by

$$P'(x,y)=\frac{1+P(x,y)}{\alpha}, \tag{4}$$

where $P(x,y)$ denotes a basic Hadamard pattern consisting of 1 and -1 extracted from the standard Hadamard matrix $\mathbf{H}$, and

This work was supported by the National Natural Science Foundation of China (NSFC) (61605165), The Hong Kong Polytechnic University (G-YBVU), and Hong Kong Research Grants Council (25201416).

Yin Xiao is with the Department of Electronic and Information Engineering, The Hong Kong Polytechnic University, Hong Kong, China.

Lina Zhou is with the Department of Electronic and Information Engineering, The Hong Kong Polytechnic University, Hong Kong, China.

Wen Chen is with the Department of Electronic and Information Engineering, The Hong Kong Polytechnic University, Hong Kong, China, and also with the Hong Kong Polytechnic University Shenzhen Research Institute, Shenzhen 518057, China (corresponding author: owen.chen@polyu.edu.hk).

α denotes a scaling constant which can be controlled precisely by using the computer.

During the decryption, each Hadamard spectrum coefficient $F(u,v)$ can be obtained by [19]

$$F(u,v)=\alpha B-F(0,0), \tag{5}$$

where $F(0,0)$ denotes the first Hadamard spectrum coefficient.

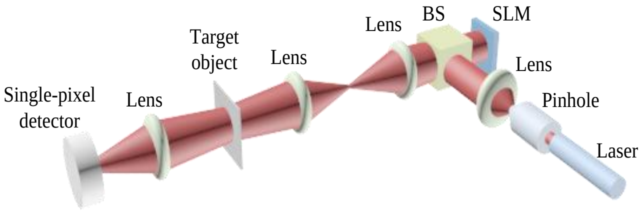


Fig. 1. The SPI experimental setup: SLM, spatial light modulator; BS, beam splitter cube.

The method based on Eq. (5) uses single step to retrieve each Hadamard spectrum coefficient in the SPI, which can achieve high sampling efficiency. We found that by randomly selecting and using a small number of Hadamard spectrum coefficients in the SPI, information of the object, i.e., plaintext, can be effectively hidden in the decrypted object. It provides a practical and effective strategy for optical encryption-based authentication which has not been exploited before.

Here, the data is processed in Hadamard domain. A small number of randomly-selected Hadamard spectrum coefficients are used for the decryption, which means that only a small number of single-pixel intensity values (i.e., ciphertext) are used. The decrypted object cannot visually render plaintext information, and can be further authenticated by using a nonlinear correlation algorithm [20–24] which is described by

$$NC=\left|IFT\left(|\Phi|^{k}\times\frac{\Phi}{|\Phi|}\right)\right|^{2}, \tag{6}$$

where NC denotes a generated nonlinear correlation map, $\Phi=FT[O]\{FT[\mathrm{Dec}]\}^{*}$, $|\ |$ denotes a modulus operation, asterisk denotes complex conjugate, FT and IFT respectively represent Fourier transform and inverse Fourier transform, Dec denotes a decrypted object, and k denotes a nonlinear strength. Nonlinear correlation is used here due to its better correlation peak, better peak-to-sidelobe ratio and narrower correlation width compared with other conventional linear correlations [13,20].

Figure 2 shows a flow chart to clearly illustrate the proposed method. As shown in Fig. 2, 300 points (i.e., the lower limit in this study) can be randomly pre-selected to form a sparse location map in this study as a typical example to illustrate the proposed method. According to this location map, plaintext is encoded into an intensity vector using a single-pixel detector in the SPI. Here, the recorded single-pixel intensity values serve as ciphertext for the proposed method. During the decryption, the ciphertext is sequentially processed to retrieve the corresponding sparse Hadamard spectrum coefficients. It is worth noting that parameters used in the optical setup, e.g., value α in Eq. (4) and sparse-coefficient location map, can serve as keys. Using the keys and ciphertext, sparse Hadamard spectrum coefficients can be correspondingly generated. Subsequently, a decrypted object can be further obtained by using Eq. (2), however it cannot visually render information about the plaintext. We found that nonlinear correlation map obtained between the decrypted object and original object (pre-recovered and stored in a database) can be further used for the authentication.

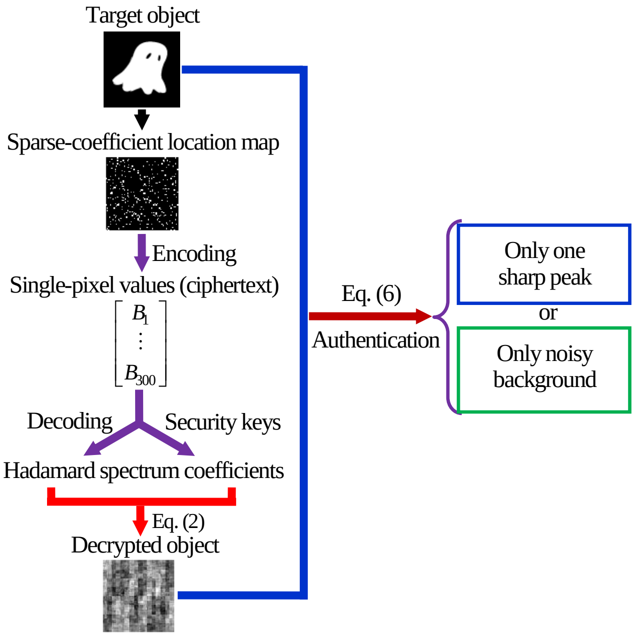


Fig. 2. Flow chart for the proposed method. An image with 64×64 pixels (i.e., Nyquist limit) is used as plaintext in this study. The white points in sparse-coefficient location map represent locations of coefficients in Hadamard domain. 300 points (i.e., about 7.32% of Nyquist limit) are randomly selected in this study as a typical example (i.e., the lower limit in this study) to illustrate the proposed method.

III. Experimental Results and Discussion

Optical experiment is conducted to verify feasibility and effectiveness of the proposed method. The experimental setup is schematically shown in Fig. 1. The He-Ne laser with wavelength of 632.8 nm is expanded by using a pinhole and collimated by a lens with focal length of 50.0 mm. A reflective SLM (Holoeye, LC-R 720) is used to display the Hadamard bases, and performs amplitude-only modulation to the illumination beam. The Hadamard patterns can be sequentially projected onto a target object (i.e., negative 1951 USAF target) through a 4*f* system with focal length of 100.0 mm, and a single-pixel bucket detector (Newport, 918D-UV-OD3R) without spatial resolution is used to sequentially collect the light intensity transmitting through the target object. A power meter connected to single-pixel detector is used to obtain experimental data, i.e., single-pixel intensity sequence to be used as ciphertext. It is worth noting that the imaging setup can also be simplified to be a lensless one, and a digital projector [14–16] can also be directly applied. The noise can be effectively eliminated or suppressed by using different methods, e.g., noise suppression strategy [19].

To simultaneously guarantee a correct optical authentication and invisibility of the plaintext, an appropriate number of sparse Hadamard spectrum coefficients need to be randomly selected. Here, peak-to-correlation energy (PCE) is adopted to analyze nonlinear correlation results obtained between reference and the decrypted object, which is defined as

$$\mathrm{PCE} = \frac{\max NC}{\sum\sum NC}. \tag{7}$$

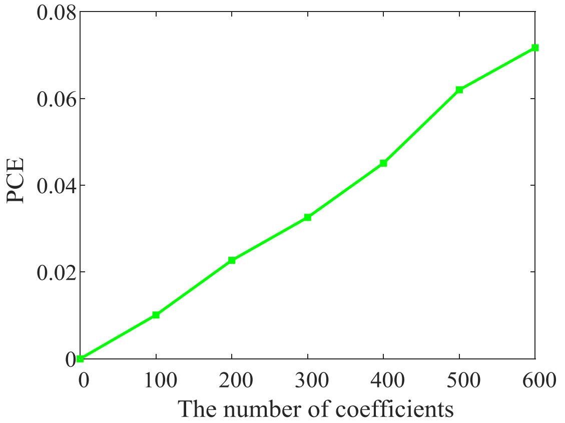


Fig. 3. PCE values versus the number of Hadamard spectrum coefficients.

As shown in Fig. 3, PCE values have a nearly linear growth with respect to the number of Hadamard spectrum coefficients. The larger PCE value represents a better correlation result. It is found that the developed optical authentication method shows good performance (i.e., a flat background and only one sharp peak in the generated nonlinear correlation map), when the number of Hadamard spectrum coefficients randomly selected is larger than 300. However, a larger number of Hadamard spectrum coefficients might lead to visibility of original information (i.e., plaintext). In the proposed method, original information can be effectively hidden in the decrypted object, when the number of Hadamard spectrum coefficients is smaller than 500. Hence, 300 points and 500 points serve as the lower limit and the upper limit in this study, respectively.

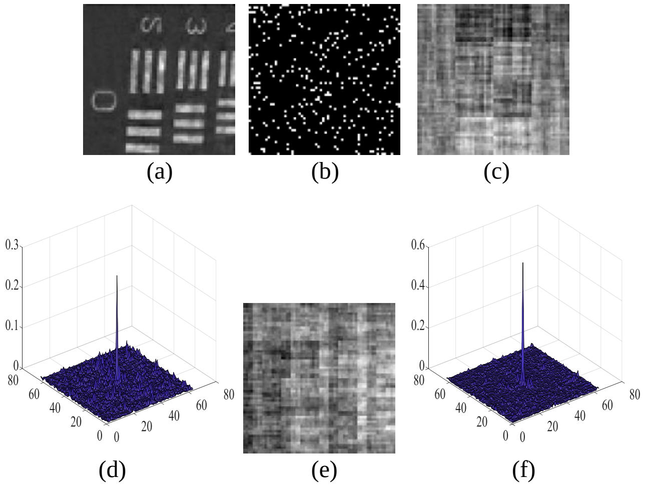


Fig. 4. (a) Original object (64×64 pixels) pre-recovered and stored in a database, (b) locations of 300 sparse Hadamard spectrum coefficients (i.e., the white points), (c) a decrypted object obtained by using correct keys, (d) nonlinear correlation map (*k*=0.3) obtained between (a) and (c), (e) a decrypted object obtained by using 500 sparse Hadamard spectrum coefficients, and (f) nonlinear correlation map (*k*=0.3) obtained between (a) and (e).

As shown in Fig. 4(a), original object is pre-recovered and stored in a database to act as reference for the proposed method. Subsequently, plaintext is encoded into a vector by using single-pixel detector according to the pre-designed sparse-coefficient location map. The 300 single-pixel intensity points (i.e., the lower limit in this study) are sequentially recorded and serve as ciphertext which will be further processed during the decryption to retrieve sparse Hadamard spectrum coefficients. The value α is set as 5, and locations of the sparse coefficients in Hadamard domain are also used as key as shown in Fig. 4(b). When correct keys are used by a receiver during the decryption, a decrypted object is obtained and shown in Fig. 4(c). It can be seen in Fig. 4(c) that the decrypted object cannot visually render information about the plaintext. The nonlinear correlation map obtained between Figs. 4(a) and 4(c) is shown in Fig. 4(d), which contains only one sharp peak. It means that the receiver is an authorized person who holds correct keys. When more sparse Hadamard spectrum coefficients (i.e., 500, the upper limit) are used, the decrypted object shown in Fig. 4(e) still effectively hides information about original object. In this case, the generated nonlinear correlation map shows a sharper peak and a more flat background as illustrated in Fig. 4(f).

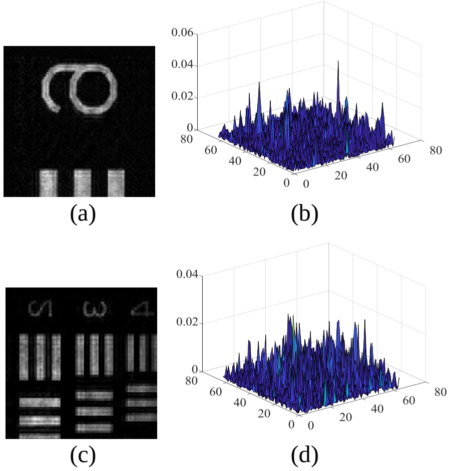
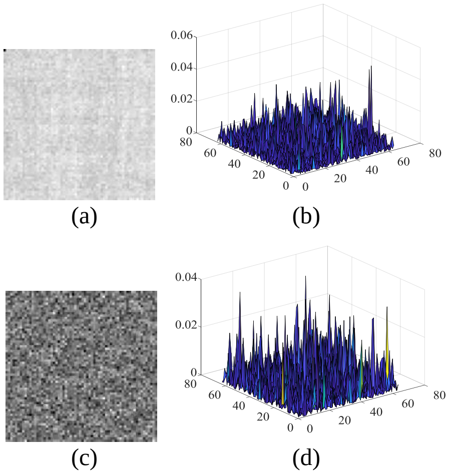


Fig. 5. (a) A different original object (64×64 pixels) stored in a database, (b) nonlinear correlation map (*k*=0.3) obtained between (a) and Fig. 4(c), (c) another original object (64×64 pixels) similar to Fig. 4(a), and (d) nonlinear correlation map (*k*=0.3) obtained between (c) and Fig. 4(c).

To show discrimination capability of the proposed method, the decrypted object in Fig. 4(c) is also nonlinearly correlated with different original objects pre-recovered and stored in the database which are respectively shown in Figs. 5(a) and 5(c). For a largely different original object shown in Fig. 5(a), it is illustrated in Fig. 5(b) that only noisy background appears in the generated nonlinear correlation map. For a similarly original object shown in Fig. 5(c), optical authentication distribution is shown in Fig. 5(d) which also contains only noisy background. It can be seen in Fig. 5(d) that there is only noisy background in the generated nonlinear correlation map. The decrypted object in Fig. 4(c) cannot be authenticated by using incorrect original objects stored in the database. Much experimental work has been carried out for testing discrimination capability of the proposed method, and experimental results always show that the decrypted object can be authenticated only by using its corresponding original object stored in the database. It also means that the proposed method possesses a high discrimination capability.



(a) (b)

(c) (d)

Fig. 6. (a) A decrypted object obtained by using a wrong value α, (b) a nonlinear correlation map (k=0.3) obtained between (a) and Fig. 4(a), (c) a decrypted object obtained using a wrong location map of sparse Hadamard spectrum coefficients, and (d) a nonlinear correlation map (k=0.3) obtained between (c) and Fig. 4(a).

To further illustrate system security, the decryption is also conducted under another two conditions, i.e., a wrong value α with a correct location map of sparse Hadamard spectrum coefficients and a correct value α with a wrong location map of sparse Hadamard spectrum coefficients. When value α used for the decryption is set as 4.5, a decrypted object is shown in Fig. 6(a). The corresponding optical authentication distribution is generated and shown in Fig. 6(b) which contains only noisy background. When a wrong location map of sparse Hadamard spectrum coefficients is used, a decrypted object is shown in Fig. 6(c). The corresponding authentication distribution is generated and shown in Fig. 6(d) which also contains only noisy background. For the sake of brevity, other keys, e.g., $F(0,0)$, are not analyzed here. The proposed method can effectively resolve the problems existing in conventional SPI-based optical authentication, and the proposed method using a small number of sparse Hadamard spectrum coefficients in the SPI is experimentally verified to be feasible and effective.

IV. Conclusions

We have experimentally presented optical authentication based on the SPI using sparse Hadamard spectrum coefficients. Only a small number of sparse Hadamard spectrum coefficients are randomly selected and used for the decryption and authentication. Optical experimental results and analyses demonstrate that the proposed method is feasible and effective. The existing problems in the SPI-based optical authentication can be effectively resolved. It is believed that the proposed method can provide a promising strategy for single-pixel optical authentication by using either a virtual or optical way, and it also has a potential for security applications through scattering media [25].

References

[1] A Valencia, G. Scarcelli, M. D’. Angelo, and Y. Shih, “Two photon imaging with thermal light,” Phys. Rev. Lett., vol. 94, no. 6, Art. no. 063601, Feb. 2005.

[2] J. H. Shapiro, “Computational ghost imaging,” Phys. Rev. A, vol. 78, no. 6, Art. no. 061802R, Dec. 2008.

[3] Y. Bromberg, O. Katz, and Y. Silberberg, “Ghost imaging with a single detector,” Phys. Rev. A, vol. 79, no. 5, Art. no. 053840, May 2009.

[4] R. E. Meyers, K. S. Deacon, and Y. Shih, “Turbulence-free ghost imaging,” Appl. Phys. Lett., vol. 98, no. 11, Art. no. 111115, Mar. 2011.

[5] W. Chen, and X. D. Chen, “Marked ghost imaging,” Appl. Phys. Lett., vol. 104, no. 25, Art. no. 251109, Jun. 2014.

[6] O. Katz, Y. Bromberg, and Y. Silberberg, “Compressive ghost imaging,” Appl. Phys. Lett., vol. 95, no. 13, Art. no. 131110, Sep. 2009.

[7] A. Gatti. E. Brambilla, M. Bache, and L. A. Lugiato, “Ghost imaging with thermal light: comparing entanglement and classical correlation,” Phys. Rev. Lett., vol. 93, no. 9, Art. no. 093602, Aug. 2004.

[8] M. Tanha, R. Kheradmand, and S. Ahmadi-Kandjani, “Gray-scale and color optical encryption based on computational ghost imaging,” Appl. Phys. Lett., vol. 101, no. 10, Art. no. 101108, Sep. 2012.

[9] W. Chen and X. D. Chen, “Ghost imaging for three-dimensional optical security,” Appl. Phys. Lett., vol. 103, no. 22, Art. no. 221106, Nov. 2013.

[10] P. Clemente, V. Durán, V. Torres-Company, E. Tajahuerce, and J. Lancis, “Optical encryption based on computational ghost imaging,” Opt. Lett., vol. 35, no. 14, pp. 2391–2393, Jul. 2010.

[11] W. Chen and X. Chen, “Grayscale object authentication based on ghost imaging using binary signals,” *EPL*, vol. 110, no. 4, pp. 44002, May 2015.

[12] W. Chen and X. Chen, “Object authentication in computational ghost imaging with the realizations less than 5% of Nyquist limit,” *Opt. Lett.*, vol. 38, no. 4, pp. 546–548, Feb. 2013.

[13] Z. B. Zhang, X. Y. Wang, G. A. Zheng, and J. G. Zhong, “Hadamard single-pixel imaging versus Fourier single-pixel imaging,” Opt. Express, vol. 25, no. 16, pp. 19619-19639, Aug. 2017.

[14] Z. B. Zhang, X. Ma, and J. G. Zhong, “Single-pixel imaging by means of Fourier spectrum acquisition,” *Nat. Commun*., vol. 6, pp. 6225, Feb. 2015.

[15] H. D. Ren, S. M. Zhao, and J. Gruska, “Edge detection based on single-pixel imaging,” Opt. Express, vol. 26, no. 5, pp. 5501–5511, Mar. 2018.

[16] M. J. Sun, M. P. Edgar, D. B. Phillips, G. M. Gibson, and M. J. Padgett, “Improving the signal-to-noise ratio of single-pixel imaging using digital microscanning,” Opt. Express, vol. 24, no. 10, pp. 10476–10485, May 2016.

[17] P. Clemente, V. Durán, E. Tajahuerce, P. Andrés, V. Climent, and J. Lancis, “Compressive holography with a single-pixel detector,” Opt. Lett., vol. 38, no. 14, pp. 2524–2527, Jul. 2013.

[18] B. L. Liu, Z. H. Yang, X. Liu, and L. A. Wu, “Coloured computational imaging with single-pixel detectors based on a 2D discrete cosine transform,” J. Mod. Opt., vol. 64, no. 3, pp. 259–264, Sep. 2017.

[19] Y. Xiao, L. N. Zhou, and W. Chen, “Direct single-step measurement of Hadamard spectrum using single-pixel optical detection,” *IEEE Photon. Tech. Lett.*, vol. 31, no. 11, pp. 845–848, 2019.

[20] B. Javidi, “Nonlinear joint power spectrum based optical correlation,” Appl. Opt., vol. 28, no. 12, pp. 2358–2367, Jun.1989.

[21] E. Pérez-Cabré, M. Cho, and B. Javidi, “Information authentication using photon-counting double-random-phase encryption images,” *Opt. Lett.*, vol. 36, no. 1, pp. 22–24, Jan. 2011.

[22] W. Chen, B. Javidi, and X. Chen, “Advances in optical security systems,” *Adv. Opt. Photon*., vol. 6, no. 2, pp. 120–155, Apr. 2014.

[23] W. Chen, “3D Gerchberg-Saxton optical correlation,” IEEE Photon. J., vol. 10, no. 2, Art. no. 7800409, Apr. 2018.

[24] W. Chen, “Ghost identification based on single-pixel imaging in big data environment,” Opt. Express, vol. 25, no. 14, pp. 16509–16516, Jul. 2017.

[25] X. D. Chen, Computational Methods for Electromagnetic Inverse Scattering. Hoboken, NJ, USA: Wiley, 2018.