Security of RF Sensing and Imaging Systems in the Age of Digital Twins *

Lhamo Dorje[1], Qian Qu[1], Xiaohua Li[1], Yu Chen[1], and Erika Ardiles-Cruz[2]

[1] Binghamton University, Binghamton NY 13902, USA
[2] The U.S. Air Force Research Laboratory, Rome, NY 13441, USA
{ldorje1,qqu2,xli,ychen}@binghamton.edu, erika.ardiles-cruz@us.af.mil

Abstract. Radio Frequency (RF) sensing and imaging are heavily used in remote sensing, security, and surveillance. This paper studies its security by developing a novel method that can compromise it in an evasive manner via the Digital Twins (DT) technology. The compromise method can make the imaging system generate false but normal-looking images. The method exploits a dynamic digital twin to emulate the imaging system, based on which compromise signals are optimized and transmitted while the victim system is conducting sensing. Simulations and experiments are conducted to demonstrate the validity of the proposed method.

Keywords: RF Sensing · Synthetic Aperture Radar (SAR) · Radar Imaging · Digital Twins · DDDAS · InfoSymbiotic Systems

1 Introduction

Radio Frequency (RF) sensing and imaging have found wide applications in remote sensing, medicine, surveillance, and other fields. Satellites or unmanned aerial vehicles (UAV) use synthetic aperture radar (SAR) technology to provide images of ground targets [9]. RF imaging systems are used to screen passengers in airports or detect objects through walls [1], [3], [5]. While this technology has been used broadly for security and surveillance, its security has not been sufficiently addressed. With regard to sensing, there are a lot of works conducted on GPS security [4], [7], but not many on RF imaging. Most existing security studies consider only techniques that deliberately interfere with or disrupt the sensing system via jamming, interfering, spoofing, etc. This kind of compromise technique can be easily detected by the sensing system and thus be avoided. The easy detection has given the RF sensing and imaging systems a false sense of security.

To make things worse, existing RF sensing and imaging systems usually use non-secure communication protocols to transmit and collect sensing data, which are usually unencrypted and unauthenticated. The parameters of the systems are

* This work is supported by the U.S. Air Force Office of Scientific Research (AFOSR) under Grant FA9550-20-1-0237. Approved for Public Release: Distribution Unlimited: Case Number AFRL-2024-3161.

usually public; for example, radar vendors are required to submit the technical specifications of all transmitting systems to the Federal Communications Committee (FCC), and these documents are publicly available. While public domain knowledge allows researchers to mirror physical imaging and sensing systems in cyberspace for higher intelligence [8], this leaves the wide open for compromise.

To show the security challenge of RF sensing and imaging, we develop a novel compromise method that makes the sensing system produce false but correct-looking sensing images, with only important objects changed. The approach is possible only when a dynamic digital twin can emulate the imaging system's operation. Since the compromised signal and the compromised sensing image look normal, the method can easily evade the detection of human beings and computer algorithms. Evasive compromise of RF sensing and imaging can be a critical challenge in many important applications. For example, in airport passenger screening, one may wear a transmitter and use this method to conceal weapons. In satellite/UAV SAR imaging, one can cause the imaging system to generate normal-looking images without or with a false target.

As shown by Fig. 1, this paper exemplifies the DDDAS paradigm by integrating dynamic data from an RF imaging system to continuously update a digital twin model, creating a feedback loop between the computational and physical systems. The method demonstrates adaptive modeling and real-time analysis, allowing for rapid decision-making in generating and transmitting compromise signals. This approach showcases the core DDDAS principles of dynamic data integration, adaptive modeling, and real-time analysis applied to a complex system, extending the paradigm into the realm of RF imaging security and illustrating its potential in exploring vulnerabilities in sensing technologies.

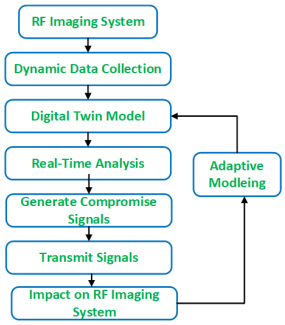

Fig. 1. DDDAS Feedback Loop.

2 System Model

Due to the broad scope of RF sensing and imaging, we limit our consideration to SAR-based two-dimensional (2D) imaging, specifically, satellite/UAV SAR imaging [6], [9] and millimeter-wave (mmWave) imaging [10], [11].

Let the imaging system be Alice, and the one to compromise the system be Eve. Figure 2 shows the overall system model, where Alice's system is a millimeter-wave imaging system to detect weapons like a knife concealed inside a box. Alice uses the SAR principle to reconstruct the image of the target, which requires scanning a lot of sensing locations to create a large enough synthetic aperture. The scan can be realized by employing a large physical antenna array [10] or moving a single-antenna sensor over a motorized scanner [11] or on a flying satellite/UAV [6].

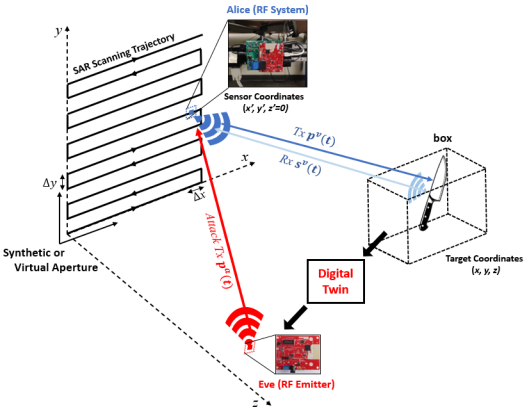

Fig. 2. System model.

To compromise Alice's imaging process, Eve uses a sensor located near the target to receive Alice's sensing signal and transmit the compromise signal. Eve also has a digital twin to emulate Alice's imaging procedure.

We assume that Eve can collect enough parameters of Alice's system from public domains to construct a dynamic digital twin of Alice's system. With the digital twin, Eve can simulate Alice's sensing procedure and sensing images. Based on this, the attacker designs and optimizes the attack signals.

We also assume the digital twin simulation is fast enough for Eve to use the simulation results to optimize and transmit the compromise signals while Alice collects sensing data. This is not a stringent assumption because mechanical scanning and data collection are much slower than computer simulation.

3 Digital Twins based Compromise Method

3.1 Alice's Imaging Procedure

First, we introduce Alice's imaging procedure when there is no compromise signal. Alice's imaging process consists of two phases: the sensing phase and the image reconstruction phase. In the sensing phase, the sensor moves to each sensing location $\mathbf{r}' = (x', y', z')$, transmits a sensing signal $p^a(t)$ toward the target location $\mathbf{r} = (x, y, z)$, receives the echo signal, and extracts data samples. Consider the frequency-modulated continuous-waveform (FMCW) radar signal

$$p^a(t) = e^{j2\pi(f_c t + \frac{1}{2}Kt^2)} \tag{1}$$

where f_c is the carrier frequency and K is the slope parameter. At each sensing location $\mathbf{r}'$, Alice transmits her sensing signal (1) toward the target and captures the echo signal $s^a_{\mathbf{r}'}(t)$, expressed as

$$s^a_{\mathbf{r}'}(t) = \int_{\mathbf{r}} \sigma_{\mathbf{r}} p^a(t - \tau_{\mathbf{r}'\mathbf{r}}) d\mathbf{r} + v_{\mathbf{r}'}(t) \tag{2}$$

where $\tau_{\mathbf{r}'\mathbf{r}}$ is the propagation delay, $\sigma_{\mathbf{r}}$ is the target reflection coefficient, and $v_{\mathbf{r}'}(t)$ includes noise, interference, and clutter. The superscript $(\cdot)^a$ indicates that this is Alice's signal when there is no compromise. After de-chirps (pulse-compresses) [5], Alice obtains signal

$$\tilde{s}^a_{\mathbf{r}'}(t) = \int_{\mathbf{r}} \sigma_{\mathbf{r}} e^{j2\pi(f_c \tau_{\mathbf{r}'\mathbf{r}} + K\tau_{\mathbf{r}'\mathbf{r}} t)} d\mathbf{r} + \tilde{v}_{\mathbf{r}'}(t). \tag{3}$$

With sufficient data samples, Alice enters the image reconstruction phase, where an image is calculated from the received data samples. There are many imaging reconstruction algorithms, and we consider the Range Migration Algorithm (RMA) [9] for satellite/UAV SAR imaging and the matched-filter algorithm (MFA) [11] for 2D millimeter-wave imaging, as outlined below.

Satellite/UAV SAR Imaging with RMA At each sensing location $\mathbf{r}'$, the signal (3) is sampled into discrete-time signal $\tilde{s}^a_{\mathbf{r}'}(n)$, $n = 0, \cdots, N-1$, with certain sampling rate F_s. Considering M sensing locations, which are denoted as $\mathbf{r}'_m$, $m = 0, \cdots, M-1$, Alice acquires an $M \times N$ data matrix $\tilde{s}^a_{\mathbf{r}'_m}(n)$, with which it will reconstruct the image using the RMA algorithm.

Typically, the sensing locations $\mathbf{r}'_m$ are evenly distributed along the flight trajectory of the satellite or UAV with an equal adjacent point distance of $\frac{\mathbf{v}}{\mathrm{PRF}}$, where $\mathbf{v}$ is the flight speed and PRF is the pulse repetition rate. This arrangement allows the application of the efficient 2D FFT and IFFT.

With RMA, Alice first creates a 2D filter which, when described in the space-frequency domain, is an $M \times N$ matrix $H(f_c, F_s, \mathrm{PRF}, \mathbf{v}, R_c)$, where R_c is a reference distance between the sensor trajectory center and the target center. The filter is a sole function of system parameters $f_c, F_s, \mathrm{PRF}, \mathbf{v}$ and R_c. Next, 2D FFT-based frequency domain filtering is applied to obtain

$$\mathbf{Y}^a = \mathrm{FFT2}\left[\tilde{s}^a_{\mathbf{r}'_m}(n)\right] \odot H(f_c, F_s, \mathrm{PRF}, \mathbf{v}, R_c), \tag{4}$$

where $\odot$ denotes element-wise or Hadamard product. Finally, Stolt interpolation is applied to reconstruct the image as

$$\mathbf{X}^a = \mathrm{IFFT2}\left[\mathrm{Stolt}\left(\mathbf{Y}^a, H(f_c, F_s, \mathrm{PRF}, \mathbf{v}, R_c)\right)\right]. \tag{5}$$

Millimeter-wave Imaging with MFA Based on the decompressed signal (3), Fourier transform is applied to transform $\tilde{s}^a_{\mathbf{r}'}(t)$ into $\tilde{S}^a_{\mathbf{r}'}(f)$, and a single data sample $\tilde{S}^a_{\mathbf{r}'}\left(K\tau_{\mathbf{r}'\mathbf{r}}\right)$ is kept as the data acquired at the sensing location $\mathbf{r}'$, which can be written as

$$s^a_{\mathbf{r}'} \triangleq \tilde{S}^a_{\mathbf{r}'}\left(K\tau_{\mathbf{r}'\mathbf{r}}\right) = \int_{\mathbf{r}} \sigma_{\mathbf{r}} e^{j2\pi f_c \tau_{\mathbf{r}'\mathbf{r}}} d\mathbf{r} + v_{\mathbf{r}'} \tag{6}$$

where $v_{\mathbf{r}'}$ is the processed $v_{\mathbf{r}'}(t)$.

The 2D mmWave imaging requires the sensing locations to form a regular 2D grid with equal distance, which we call *grid size* among adjacent sensing locations. With an $M \times N$ sensing grid of MN sensing locations $\mathbf{r}'_m$, $m = 0, \cdots, MN-1$, Alice acquires an $M \times N$ data matrix based on (6), which can be written as $s^a_{\mathbf{r}'_m}$. Next, the victim creates a $M \times N$ 2D matched filter $H(f_c, \Delta x, \Delta y, R_c)$, which stores the propagation phase from each sensing location to a reference point such as the target center. The filter is determined uniquely by system parameters such as the carrier frequency f_c, the grid sizes Δx and Δy, and the reference distance R_c. The image is then constructed as

$$\mathbf{X}^a = \mathrm{IFFT2}\left[\mathrm{FFT2}[s^a_{\mathbf{r}'_m}] \odot \mathrm{FFT2}[H(f_c, \Delta x, \Delta y, R_c)]\right]. \tag{7}$$

3.2 Eve's Digital Twin of Alice's Imaging Procedure

To compromise the imaging system, Eve must know Alice's imaging procedure and imaging results. Section 3.1 shows that Eve can construct a dynamic digital twin of Alice's imaging procedure based on public parameters and the reference distance R_c. R_c can be estimated once Eve receives Alice's transmitted sensing signal because he can use the signal to estimate Alice's location. Eve then runs the digital twin to simulate Alice's sensing and imaging procedure. Based on some model of the target echo $\sigma_{\mathbf{r}}$, Eve can simulate Alice's sensing signal (2)-(3) and estimate the image $\mathbf{X}^a$.

To guarantee the performance of digital twins in a dynamic environment, Dynamic Data Driven Applications Systems (DDDAS) design principles [2] can be adopted to address the challenging multi-objective parameterization among imaging resolution, data collection, and data processing. Specifically, starting from the first sensed Alice's signal, DDDAS leverages continuous measurement data and the digital twins to adjust the compromise signals adaptively. This way, Eve can generate compromise signals with an affordable complexity and speed to cope with the dynamic victim-sensing procedure.

3.3 Eve's Compromising Procedure

Based on the estimated image $\mathbf{X}^a$ from the digital twins, Eve can create a target image $\mathbf{X}^t$ with some pixels modified to hide import objects. According to $\mathbf{X}^t$, Eve designs the compromise signal

$$p^e_{\mathbf{r}'}(t) = \alpha_{\mathbf{r}'} p^e(t - \beta_{\mathbf{r}'}) \tag{8}$$

where the parameters $\alpha_{\mathbf{r}'}$ and $\beta_{\mathbf{r}'}$ are to be optimized. The superscript $(\cdot)^e$ denotes Eve.

When Alice is conducting sensing at location $\mathbf{r}'$, i.e., transmitting its sensing signal $p^a(t)$, Eve transmits the compromise signal (8) to trickle Alice to get the image $\mathbf{X}^t$ instead of $\mathbf{X}^a$. In this case, Alice's received signal is a mixture of the original echo signal (2) and the compromise signal (8), i.e.

$$s^e_{\mathbf{r}'}(t) = \int_{\mathbf{r}} \sigma_{\mathbf{r}} p^a(t - \tau_{\mathbf{r}'\mathbf{r}}) d\mathbf{r} + p^e_{\mathbf{r}'}(t) + v_{\mathbf{r}'}(t). \tag{9}$$

Unaware of the compromise, Alice conducts the imaging procedure described in Section 3.1. Then, (3) becomes

$$\tilde{s}^e_{\mathbf{r}'}(t) = \int_{\mathbf{r}} \sigma_{\mathbf{r}} e^{j2\pi(f_c \tau_{\mathbf{r}'\mathbf{r}} + K\tau_{\mathbf{r}'\mathbf{r}} t)} d\mathbf{r} + e^{j2\pi f_c \tau_{\mathbf{r}'} t} s^e_{\mathbf{r}'} + v_{\mathbf{r}'} \tag{10}$$

where $s^e_{\mathbf{r}'}$ is the compromise signal's contribution after de-chirping, and $\tau_{\mathbf{r}'}$ is the propagation delay from Eve's location $(0, 0, 0)$ to Alice's location $\mathbf{r}'$.

When Alice uses RMA for image reconstruction, (4) becomes

$$\mathbf{Y}^e = \mathrm{FFT2}[\tilde{s}^a_{\mathbf{r}'_m}(n) + s^e_{\mathbf{r}'_m}] \odot H(f_c, F_s, \mathrm{PRF}, \mathbf{v}, R_c) \tag{11}$$

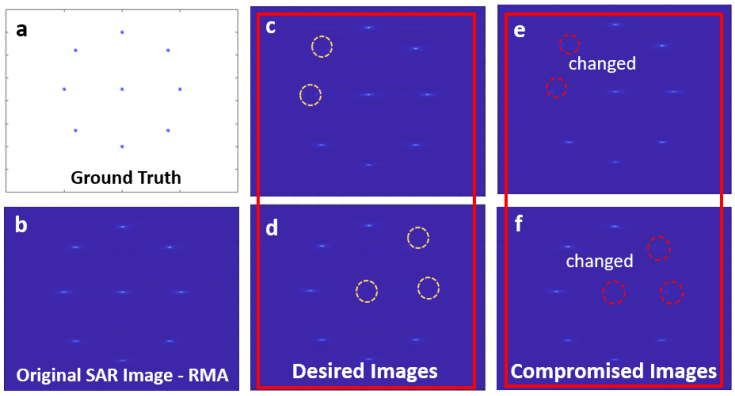

Fig. 3. Compromise UAV SAR imaging over the simulated dataset: (a) ground target, (b) reconstructed image (without compromise) $\mathbf{X}^a$, (c)(d) desired target images $\mathbf{X}^t$, and (e)(f) compromised images $\mathbf{X}^e$.

with which (5) is applied to generate the image. When Alice uses MFA for image reconstruction, (7) becomes

$$\mathbf{X}^e = \text{IFFT2}\left[\text{FFT2}[s^a_{\mathbf{r}'_m} + s^e_{\mathbf{r}'_m}] \odot \text{FFT2}[H(f_c, \Delta x, \Delta dy, R_c)]\right] \tag{12}$$

In both cases, Eve can optimize $s^e_{\mathbf{r}'_m}$ to make Alice to generate image $\mathbf{X}^e \approx \mathbf{X}^t$ instead of $\mathbf{X}^a$. He just needs to optimize the parameters $\alpha_{\mathbf{r}'}$ and $\beta_{\mathbf{r}'}$ to minimize

$$\min_{\{\alpha_{\mathbf{r}'}, \beta_{\mathbf{r}'}\}} \|\mathbf{X}^e(\alpha_{\mathbf{r}'}, \beta_{\mathbf{r}'}) - \mathbf{X}^t\|^2 \tag{13}$$

where $\mathbf{X}^e(\alpha_{\mathbf{r}'}, \beta_{\mathbf{r}'})$ is just $\mathbf{X}^e$ in (12) with the optimization variables shown. (13) is solved once Eve obtains Alice's sensing signal.

4 Simulations

Compromise SAR Imaging over Simulated UAV Dataset. First, a UAV SAR imaging system was simulated as Alice. The true target consisted of 8 reflectors arranged in a circular pattern, as shown in Fig. 3(a). Without Eve, the imaging system accurately formed an image of the target $\mathbf{X}^a$ using the RMA algorithm, shown in (b). We then simulated Eve's operation. Comparing the target image $\mathbf{X}^t$ in (c) and (d) with the compromised images $\mathbf{X}^e$ in (e) and (f), we can see that Eve successfully generated normal-looking but false images with some reflectors changed.

Compromise SAR Imaging over Real Satellite Dataset. To validate the proposed method on real-world imaging systems, we employed a real satellite dataset, i.e., the ERS-1 data from the European Space Agency's (ESA) ERS-1 and ERS-2 satellites (https://search.asf.alaska.edu). One example of a clean image $\mathbf{X}^a$, including single-look and multi-look processing using the RMA, is

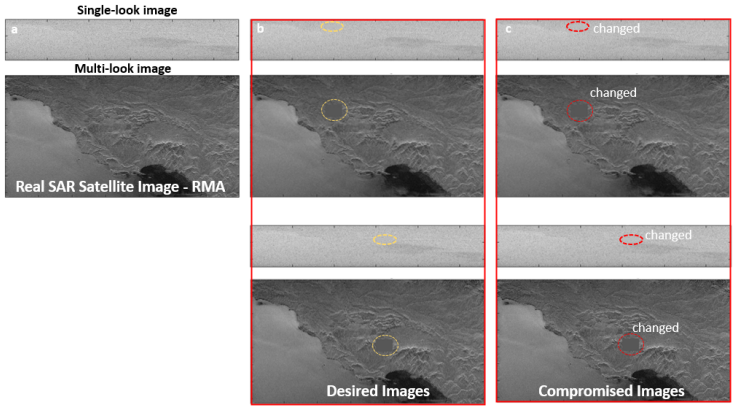

Fig. 4. Compromise satellite SAR imaging over real dataset: (a) images (without compromise) $\mathbf{X}^a$, (b) desired images $\mathbf{X}^t$, and (c) Compromised images $\mathbf{X}^e$.

shown in Fig. 4(a). Eve aimed to achieve the desired images $\mathbf{X}^t$ depicted in (b), where two geographic locations were missing. (c) shows the compromised system's reconstructed images $\mathbf{X}^e$ after Eve's operation. We can observe that Eve successfully changed specific parts of the images, leaving other areas visually indistinguishable from the original.

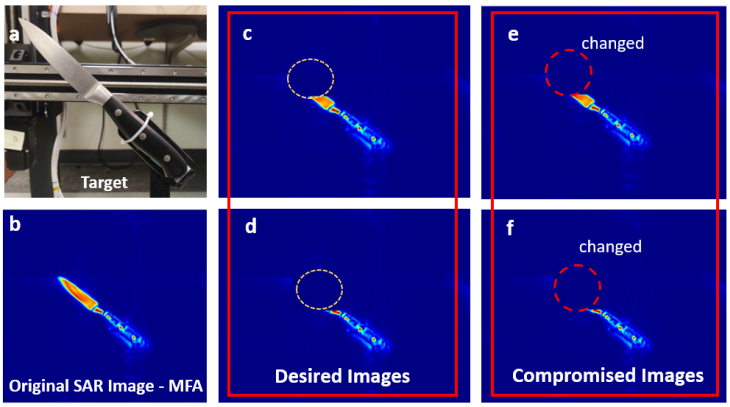

Fig. 5. Millimeter-wave imaging experiment: (a) photo of the real target, (b) reconstructed image (without attack) $\mathbf{X}^v$, (c)(d) target images $\mathbf{X}^t$, (e)(f) attacked images $\mathbf{X}^a$.

Compromise Experimental Millimeter-wave Imaging System. This experiment used our custom-built 2D mmWave imager to implement Fig. 2 for data capture. Imaging results are presented in Fig. 5. (b) shows the reconstructed image $\mathbf{X}^a$ without compromise. In (c) and (d), the desired target images $\mathbf{X}^t$ are depicted. (e) and (f) show the images $\mathbf{X}^a$ under Eve's operation. Looking at the

images generated by Alice after Eve's operation, it is hard to identify the threat object, a knife, potentially allowing Eve to evade detection.

5 Conclusions

This paper studies the security of RF sensing and imaging when digital twins can be constructed to emulate the system operation. The paper shows that a new evasive compromising method can make the imaging system generate false but normal-looking images. The compromise can evade the detection of the RF imaging system. The elusive nature makes the compromise a new challenge to RF sensing and imaging systems.

References

1. Adib, F., Katabi, D.: See through walls with wifi! In: Proceedings of the ACM SIGCOMM 2013 conference on SIGCOMM. pp. 75–86 (2013)
2. Blasch, E., Ravela, S., Aved, A.: Handbook of dynamic data driven applications systems. Springer (2018)
3. García-Rial, F., Montesano, D., Gómez, I., Callejero, C., Bazus, F., Grajal, J.: Combining commercially available active and passive sensors into a millimeter-wave imager for concealed weapon detection. IEEE Transactions on Microwave Theory and Techniques **67**(3), 1167–1183 (2018)
4. Haider, Z., Khalid, S.: Survey on effective gps spoofing countermeasures. In: 2016 Sixth International Conference on Innovative Computing Technology (INTECH). pp. 573–577. IEEE (2016)
5. Li, X., Chen, Y.: Lightweight 2d imaging for integrated imaging and communication applications. IEEE Signal Processing Letters **28**, 528–532 (2021)
6. Li, X., Dorje, L., Wang, Y., Chen, Y., Ardiles-Cruz, E.: High-resolution imaging satellite constellation. In: Proceedings of the InforSymbiotics/Dynamic Data Driven Applications Systems (DDDAS2022). pp. 1–5 (2022)
7. Liu, S., Cheng, X., Yang, H., Shu, Y., Weng, X., Guo, P., Zeng, K.C., Yang, Y.: Stars can tell: A robust method to defend against gps spoofing using off-the-shelf chipset. In: Proceedings of The 30th USENIX Security Symposium (USENIX Security) (2021)
8. Liu, Y., Shen, Y., Fan, L., Tian, Y., Ai, Y., Tian, B., Liu, Z., Wang, F.Y.: Parallel radars: from digital twins to digital intelligence for smart radar systems. Sensors **22**(24), 9930 (2022)
9. Robin, J.P., Lafitte, M., Coiras, E.: A review of sar imagery exploitation methods in support of defence and security missions. In: Proceedings of EUSAR 2016: 11th European Conference on Synthetic Aperture Radar. pp. 1–5 (2016)
10. Sheen, D.M., McMakin, D.L., Hall, T.E.: Three-dimensional millimeter-wave imaging for concealed weapon detection. IEEE Transactions on microwave theory and techniques **49**(9), 1581–1592 (2001)
11. Yanik, M.E., Torlak, M.: Near-field mimo-sar millimeter-wave imaging with sparsely sampled aperture data. IEEE Access **7**, 31801–31819 (2019)