Evasive Camouflage Attack of RF Sensing and Imaging Systems

Lhamo Dorje, Xiaohua Li
Department of Electrical and Computer Engineering
Binghamton University
Binghamton, NY 19312, USA
{ldorje1, xli}@binghamton.edu

Soamar Homsi
Information Warfare Division
Air Force Research Lab
Rome, NY 13440, USA
Soamar.Homsi@us.af.mil

***Abstract*—Radio frequency (RF) sensing and imaging systems play important roles today, from remote sensing to airport passenger screening to medical imaging. Nevertheless, the security of these systems has not been studied sufficiently. Existing attack methods under consideration are mostly jamming, interfering, etc. Because such attacks can easily be detected by the systems and thus be avoided, it has given a false sense of security in applying the sensing systems. This paper shows a more evasive attack called camouflage attack that makes the sensing systems generate false but normal-looking images and can evade the detection of the sensing systems. The proposed camouflage attack algorithm is conducted by a wireless transmitter to broadcast a signal designed according to the knowledge of the sensing system or according to the intercepted signals. Extensive simulations and experiments are conducted to verify the validity of this new attack. Especially, this attack is shown as transferable among different sensing/imaging algorithms and robust to sensor location ambiguities. The aim of this work is to encourage and motivate further research to strengthen the security of RF sensing systems.**

***Index Terms*—cyber attack, RF sensing, radar imaging, Synthetic Aperture Radar (SAR)**

I. Introduction

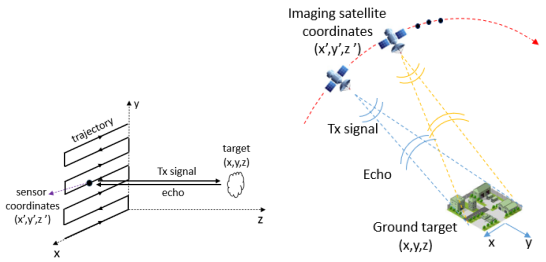
Radio frequency (RF) sensing and imaging systems play important roles across various domains, including medical imaging [1], [2], senior care [3], concealed weapon detection [4], [5], security and surveillance [6], etc. RF has the unique ability to address challenging issues associated with optical cameras, including blockage, privacy concerns, and limitations imposed by bad weather conditions or physical obstructions. Satellites or unmanned aerial vehicles (UAV) use synthetic aperture radar (SAR) technology to provide images of the earth's surface in adverse weather conditions like rain, fog, and haze. This has been widely used in ecological surveillance [7], [8], crisis management [9], [10], as well as public and national security [11]. More recently, with the ubiquitous presence of wireless communication devices such as smartphones, WiFi, and RFID, it has gained significant attention to implement RF sensing and imaging using small and smart mobile devices [12]–[15]. There are a lot of studies in which WiFi signals or millimeter wave signals are exploited to provide images of targets behind walls, under tree leaves, concealed in boxes, etc [3], [4], [16]–[18].

In contrast to the fast development of RF sensing and imaging systems, their security has not been sufficiently addressed. These systems use non-secure communication protocols to transmit and collect sensing signals which are usually unencrypted and unauthenticated. They lack protection against malicious attackers. The parameters of the sensing systems are usually public, e.g., radar vendors are required to submit the technical specifications of all transmitting systems to the FCC, and these documents are publicly available. The attackers can exploit this public knowledge to sophisticate their attacking strategies.

A noticeable gap exists in studies exploring the security concerns in RF sensing and imaging systems [19]. Most existing attack studies focus on deliberately interfering with or disrupting the sensing system's reception of signals via jamming, interfering, spoofing, etc. For example, numerous security-focused studies have concentrated on the susceptibility of the Global Navigation Satellite System (GNSS) to common attacks such as spoofing [20]–[22] and jamming [23]–[25]. The attacks can be easily detected, e.g., by measuring signal directions, and thus be avoided [26], [27]. Similarly, various studies [21], [28] (automobiles), [29], [30] (marine crafts), and [31], [32] (smartphones) have demonstrated the feasibility of cyber attacks by using readily available and cost-effective off-the-shelf hardware to jam GPS signals, which can also be easily detected and avoided. The easy detection has given the RF sensing and imaging systems a false sense of security.

In this paper, we develop a novel attack called "camouflage attack" on RF sensing and imaging systems, where the attacker's objective is to make the sensing system produce false but correct-looking sensing images and to evade detection. Due to the broad scope of RF sensing and imaging, we limit our consideration of camouflage attack to SAR-based 2D imaging systems, either RF radar imaging [5], [33] or satellite SAR imaging [9], [34]. We will develop the attack algorithm and provide extensive simulations to demonstrate its effectiveness, transferability, and robustness.

The rest of the paper is structured as follows. Section II gives the RF imaging system model and the attack model. Section III develops the attack algorithm. Section IV provides the simulation and experiment results. Conclusions are presented in Section V.



(a) (b)

Fig. 1. RF imaging systems: (a) Short-range radar imaging; (b) Satellite imaging.

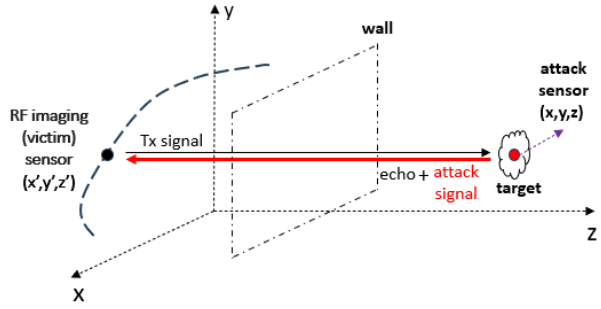


Fig. 2. Camouflage attack model: The attack sensor makes the victim sensor (RF imaging system) create an incorrect but normal image by injecting its attack signal into the victim sensor's received signal.

II. System Model

A. RF imaging model

Consider 2D imaging with two popular systems, i.e. short-range RF radar imaging and satellite imaging as illustrated in Fig. 1. They both apply the SAR principle to generate high-resolution 2D images. The SAR principle requires the imaging system to scan multiple sensing locations to create a virtual array with a large synthetic aperture. The scan can be realized by moving the sensor on a motorized scanner, as shown in Fig. 1(a), or on a satellite flying over the target area, as shown in Fig. 1(b).

The imaging process consists of two phases: the sensing phase which gathers sensing data, and the image reconstruction phase which calculates the image pixels from all the sensing data. In the sensing phase, the sensor moves to each sensing location $\mathbf{r}' = (x', y', z')$, transmits a sensing signal $p(t)$ toward the target location $\mathbf{r} = (x, y, z)$, receives the echo signal $s_{\mathbf{r}'}(t)$, and extracts a data sample $s_{\mathbf{r}'}$. All the locations $\mathbf{r}'$ form a one-dimension or two-dimensional regular grid. After collecting a sufficient number of data samples, it enters the image reconstruction phase, where the system calculates an image with all the received data samples $s_{\mathbf{r}'}$. There are many imaging reconstruction algorithms, such as the back-propagation algorithm (BPA).

B. Camouflage attack model

Evasive camouflage attacks can become a severe problem for the above-mentioned sensing systems in many important applications. For example, in RF radar imaging one may want to create an image of the target behind a wall, while a camouflage attack can conceal the target. With satellite imaging one may want to create an image of a valuable target on the ground, but the camouflage attack can make it generate an image either without the target or with a false target somewhere else. The problem becomes critical if the sensing system can not detect that there is an attack.

Based on the imaging scenario shown in Fig. 1(a), we consider the attack model illustrated in Fig. 2. The victim sensor is the RF imaging system, which wants to generate an image of the target behind a wall. The attack sensor is a sensor in the vicinity of the target. Without loss of generality, we assume the location of the attack sensor is $(x, y, z) = (0, 0, 0)$, which is also the center of the target image. The attack sensor can receive the victim sensor's signal, and transmit appropriate attack signals according to its received signals and/or its knowledge of the victim sensor. The objective is not to prevent the victim sensor from creating a clear image, but rather, to make it create a clear image with the target disappearing, camouflaged, or with some nonexistent targets.

To simplify formulation, we skip the attack sensor's signal interception procedure and just assume that it has a replica of the victim's sensing signal $p(t)$. It then transmits a signal similar to $p(t)$ but with some important attacking parameters optimized via the proposed camouflage algorithm. The victim sensor receives a mixture of the true echo signal and the attack signal, with which to generate the image. Because the attack sensor is close to the target and the attack signal is similar to the echo signal, it is difficult for the victim sensor to detect the attack.

III. Camouflage Attack Method

A. Victim Sensor's Imaging Procedure

Assume the victim sensor has a single transmit antenna and a single co-located receiving antenna. During the sensing phase, in each sensing position $\mathbf{r}'$, the sensor transmits its sensing signal $p^v(t)$ toward the target and captures the echo signal $s^v_{\mathbf{r}'}(t)$ from the target, expressed as

$$s^v_{\mathbf{r}'}(t) = \int_{\mathbf{r}} \sigma_{\mathbf{r}} p^v(t - \tau_{\mathbf{r}'\mathbf{r}}) d\mathbf{r} + v_{\mathbf{r}'}(t) \tag{1}$$

where $\tau_{\mathbf{r}'\mathbf{r}}$ is the propagation delay, $\sigma_{\mathbf{r}}$ is the target reflection coefficient, and $v_{\mathbf{r}'}(t)$ is noise, interference, and clutter. The superscript $(\cdot)^v$ is used to indicate this is the victim sensor's signal when there is no attack. We consider the frequency-modulated continuous-waveform (FMCW) radar signal in this paper

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

where f_c is the carrier frequency and K is the slope.

The victim sensor uses the transmitted signal $p^v(t)$ to dechirp (pulse-compress [18]) the received signal to

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

Then, Fourier transform is applied to $\tilde{s}^v_{\mathbf{r}'}(t)$, which gives $\tilde{S}^v_{\mathbf{r}'}(f)$, and the sample $\tilde{S}^v_{\mathbf{r}'}(K\tau_{\mathbf{r}'\mathbf{r}})$ is kept as data sample acquired at the sensing location $\mathbf{r}'$, i.e.

$$s^v_{\mathbf{r}'} = \tilde{S}^v_{\mathbf{r}'}(K\tau_{\mathbf{r}'\mathbf{r}}) = \int_{\mathbf{r}} \sigma_{\mathbf{r}} e^{j2\pi f_c \tau_{\mathbf{r}'\mathbf{r}}} d\mathbf{r} + v_{\mathbf{r}'} \tag{4}$$

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

In the image reconstruction phase, after acquiring M data samples at M different locations, the victim sensor stacks all the data samples into an M dimensional vector $\mathbf{y}^v$, whose mth element is $s^v_{\mathbf{r}'_m}$ obtained at sensing location (x'_m, y'_m, z'_m), $m = 0, \cdots, M-1$. Assume the victim sensor needs to generate a 2D target image $\mathbf{X}^v$ of $I \times J$ pixels. It discretizes the target image plane into $I \times J$ pixel points. In other words, the target coordinate $\mathbf{r} = (x, y, z_0)$ is discretized into

$$x = i\Delta x + x_0,\ y = j\Delta y + y_0, \tag{5}$$

where $0 \le i \le I-1$, $0 \le j \le J-1$, Δx and Δy represent the discretizing step size, while x_0 and y_0 are shifts in the coordinates. The image pixel is thus $X^v_{ij} = \sigma_{\mathbf{r}} \Delta x \Delta y$.

To apply the BPA algorithm to calculate pixel values from data samples $\mathbf{y}^v$, the victim sensor first stacks the columns of $\mathbf{X}^v$ into an N-dimensional column vector $\mathbf{x}^v$, where $N = IJ$. With this, the data sample is modeled as

$$\mathbf{y}^v = \mathbf{H}^v \mathbf{x}^v + \mathbf{v}, \tag{6}$$

where $\mathbf{H}^v$ is the $M \times N$ propagation matrix with elements denoted by $H^v_{mn} = e^{j4\pi R_{mn}/\lambda}$, where

$$\begin{aligned} R_{mn} = R_{m,jI+i} = ((x'_m - i\Delta x - x_0)^2 \\ + (y'_m - j\Delta y - y_0)^2 + (z'_m - z_0)^2)^{1/2} \end{aligned} \tag{7}$$

is the distance between the antenna and the image pixel, and λ is the wavelength. The vector $\mathbf{v}$ is noise, clutter, and interference. Based on the data model (6), the BPA reconstructs the image as

$$\hat{\mathbf{x}}^v = (\mathbf{H}^v)^H \mathbf{y}^v. \tag{8}$$

where $(\cdot)^H$ is the Hermitian transpose.

B. Attack Sensor's Attacking Procedure

When the victim sensor is conducting sensing at location $\mathbf{r}'$, the attack sensor transmits a carefully designed FMCW waveform as the attacking signal. Consequently, the victim sensor's received signal is a mixture of the original echo signal and the attack signal

$$s_{\mathbf{r}'}(t) = \int_{\mathbf{r}} \sigma_{\mathbf{r}} p^v(t - \tau_{\mathbf{r}'\mathbf{r}}) d\mathbf{r} + p^a_{\mathbf{r}'}(t) + v_{\mathbf{r}'}(t) \tag{9}$$

where

$$p^a_{\mathbf{r}'}(t) = \alpha_{\mathbf{r}'} p^v(t - \beta_{\mathbf{r}'}) \tag{10}$$

with parameters $\alpha_{\mathbf{r}'}$ and $\beta_{\mathbf{r}'}$ that are to be optimized by the attack algorithm.

Without knowing the attack, the victim sensor conducts the FMCW signal processing and image reconstruction procedure described in Section III-A. Then, (4) becomes

$$s_{\mathbf{r}'} = \int_{\mathbf{r}} \sigma_{\mathbf{r}} e^{j2\pi f_c \tau_{\mathbf{r}'\mathbf{r}}} d\mathbf{r} + e^{j2\pi f_c \tau_{\mathbf{r}'}} s^a_{\mathbf{r}'} + v_{\mathbf{r}'} \tag{11}$$

where $s^a_{\mathbf{r}'}$ is the attacking signal's contribution after dechirping and Fourier transform, and $\tau_{\mathbf{r}'}$ is the propagation delay from the attack location $(0,0,0)$ to the victim sensor location $\mathbf{r}'$. The model (6) becomes

$$\mathbf{y} = \mathbf{H}^v \mathbf{x}^v + \mathbf{H}^a \mathbf{x}^a + \mathbf{v}, \tag{12}$$

where $\mathbf{H}^a$ represents the propagation matrix from the attack sensor to the victim sensor. Note that the dimensions of $\mathbf{H}^v$ and $\mathbf{x}^v$ are $M \times N$ and $N \times 1$, respectively, while the dimensions of $\mathbf{H}^a$ and $\mathbf{x}^a$ are $M \times M$ and $M \times 1$, respectively. The element of $\mathbf{H}^a$ can be found as

$$H^a_{mc} = e^{j2\pi\sqrt{(x'_m)^2 + (y'_m)^2 + (z'_m)^2}/\lambda}, \tag{13}$$

where $\sqrt{(x'_m)^2 + (y'_m)^2 + (z'_m)^2}$ the distance from the attack sensor at location $(0,0,0)$ to the victim sensor at location (x'_m, y'_m, z'_m). With the data $\mathbf{y}$, the victim sensor gets image pixels as

$$\hat{\mathbf{x}} = (\mathbf{H}^v)^H \mathbf{y} \tag{14}$$

In the context of the attack scenario, the attack sensor's objective is to change certain portions of the target image, i.e., make $\hat{\mathbf{x}}$ different from $\hat{\mathbf{x}}^v$, using the signal (10). This means it needs to optimize the parameters $\alpha_{\mathbf{r}'}$ and $\beta_{\mathbf{r}'}$ according to the difference between $\hat{\mathbf{x}}$ and $\hat{\mathbf{x}}^v$.

A problem is that the attack node does not have the victim sensor's data $\mathbf{y}$, $\hat{\mathbf{x}}^v$, or $\hat{\mathbf{x}}$. Nevertheless, this is not a hurdle to the attacker. The main reason is that almost all the practically-used image reconstruction algorithms use a regular grid centered around a center point of the sensor grid. The algorithm just needs parameters like grid size and center location. Such parameters can be easily obtained by the attacker. For example, it is fairly easy to estimate satellite locations and signals from public-domain knowledge.

The attacker's estimated parameters may be different from the victim sensor's true parameters. Fortunately, this is not a big problem. The reason is that there is usually just a global phase difference between the pre-measured (or estimated) data and the true victim sensor's data. For many imaging system, there is a location parameter $\mathbf{r}_c$ that specifies the center of sensor array, and all the sensor elements are located on a regular grid around this center with half-wavelength grid distance. In other words, once $\mathbf{r}_c$ is known, then the locations of all the sensor elements are known. Therefore, the matrix $\mathbf{H}^v$ is a function of $\mathbf{r}_c$ only. If $\mathbf{r}_c$ is estimated as $\mathbf{r}'$ with some errors, then the matrix $\mathbf{H}'^v$ (calculated based on $\mathbf{r}'$) is different from $\mathbf{H}^v$ (calculated based on $\mathbf{r}_c$) by a scalar phase multiplication factor.

To simplify notations, we assume the attack sensor knows $\mathbf{y}^v$, $\mathbf{H}^v$ and $\mathbf{H}^a$. To conduct attacks, the attack sensor first

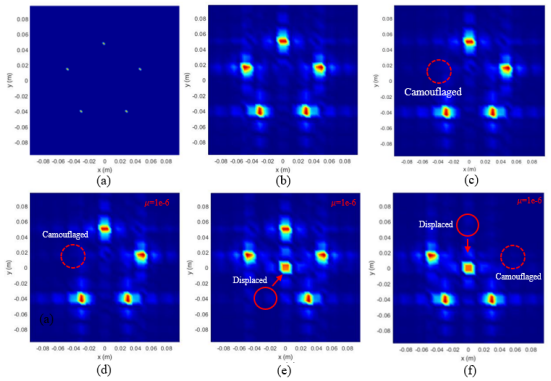


Fig. 3. RF imaging simulation. (a) A five-point target for millimeter wave radar imaging; (b) Reconstructed image $\hat{\mathbf{x}}^v$ without attack. (c) Desired target image $\mathbf{x}^t$. (d) Reconstructed camouflage image $\hat{\mathbf{x}}$ under the proposed attack. (e)-(f) Reconstructed images with displacement and/or camouflage desired by the attack algorithm.

chooses a target image $\mathbf{x}^t$ that it wants the victim sensor to generate. Then, it minimizes the pixel-wise difference between $\hat{\mathbf{x}}$ (which it can calculate from the known data) and $\mathbf{x}^t$ via

$$\arg\min_{\mathbf{x}^a} \ \|\hat{\mathbf{x}} - \mathbf{x}^t\|^2. \tag{15}$$

This optimization should be conducted via gradient optimization. Although a closed-form solution can be derived, it requires matrix inversion, which is highly ill-conditioned because the matrices $\mathbf{H}^v$ and $\mathbf{H}^a$ are too big. Computational complexity is also too expensive.

The gradient of the error of (15) with respect $\mathbf{x}^a$ is

$$\frac{\partial}{\partial(\mathbf{x}^a)^H}\left[(\hat{\mathbf{x}} - \mathbf{x}^t)^H(\hat{\mathbf{x}} - \mathbf{x}^t)\right] = (\mathbf{H}^a)^H\mathbf{H}^v(\hat{\mathbf{x}} - \mathbf{x}^t). \tag{16}$$

Then the following optimization is conducted iteratively until converges,

$$\mathbf{x}^a \leftarrow \mathbf{x}^a - \mu(\mathbf{H}^a)^H\mathbf{H}^v(\hat{\mathbf{x}} - \mathbf{x}^t). \tag{17}$$

The victim sensor's image reconstruction procedure will then produce image $\mathbf{x}^t$ instead of $\hat{\mathbf{x}}$. The attack method is summarized in **Algorithm 1**.

Algorithm 1 Camouflage Attack Algorithm

1: **Initialization**: Attack sensor acquires reference data $\mathbf{y}^v$, $\mathbf{H}^v$ and $\mathbf{H}^a$,
2: **Sensing Phase**:
3: *Victim Sensor*: at each location $\mathbf{r}'$, transmit $p(t)$, receive and process signal to get data sample $s_{\mathbf{r}'}$,
4: *Attack Sensor*: for each $\mathbf{r}'$, calculate $\mathbf{x}^a$ and $p^a(t)$, transmit $p^a(t)$,
5: **Imaging Phase**: Victim sensor reconstructs image $\hat{\mathbf{x}}$.

IV. Simulations

A. Simulated Attack on RF Imaging System

First, we implement the attack algorithm over a simulated millimeter wave imaging system. The victim sensor images a target with five-point sources arranged in a circular pattern, shown in Fig. 3 (a), located 500 cm away from the imaging sensor. Without attack, a target image ($\hat{\mathbf{x}}^v$) of size $I \times J = 30 \times 30$ is reconstructed using the BPA algorithm, shown in Fig. 3(b). Then, we simulate the camouflage attack to render the victim sensor to generate a clear yet incorrect target image, with certain critical portions of the image camouflaged or invisible. Fig. 3(c) shows the desired target image ($\mathbf{x}^t$). Under the attack, the victim sensor generates the image shown in Fig. 3(d). Comparing (c) and (d), we can see that the camouflage attack is successful. Furthermore, figures (e) and (d) show other successful camouflage-attacked images with displaced target points.

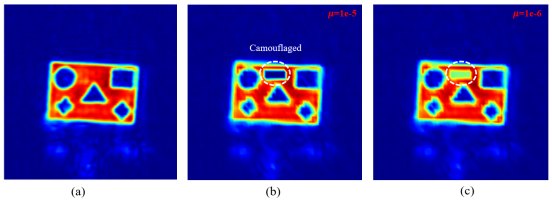


Fig. 4. Experiment over a real mmWave radar dataset. (a) Victim sensor's reconstructed image without attack; (b) Victim sensor's reconstructed image under attack with learning rate $\mu = 1\text{e-}5$, and (c) reconstructed image under attack with learning rate $\mu = 1\text{e-}6$.

B. Attack Experiment with Real Measured RF Imaging Data

To demonstrate the effectiveness of our attack method on real imaging systems, we use the millimeter wave radar dataset from [33]. This dataset was generated by moving a 79 GHz mmWave radar sensor in a rectangular grid shown in Fig. 1(a). A target with different-shaped cutouts was positioned 28 cm away from the sensor. Without attack, the victim sensor's image of the target is shown in Fig. 4(a). Fig. 4 (b)(c) shows the victim sensor's imaging results when the attack is applied, where a rectangular part of the image is camouflaged successfully.

C. Real Experiment with TI's mmWave Radar Sensor

We have conducted a practical attack experiment utilizing Texas Instrument's (TI) IWR1843 Single-Chip 76-81 GHz FMCW mmWave sensor. The sensor can detect a person by showing its location, not generating a 2D image of the person. The experiment setting is shown in Fig. 5(a) with a person located approximately 1 meter away from the sensor. Fig. 5(b) shows the radar image when there is no attack. It clearly shows the presence of the person in front of the sensor. In contrast, our attack algorithm successfully achieves the camouflage of the person. The results are shown in Fig. 5(c)(d).

D. Simulated Attack on Satellite Imaging System

Following [34], we simulate a satellite imaging system using real SpaceX Satellite constellation orbital data obtained from https://celestrak.org. A 12-point target, shown in Fig.6(a), is located approximately 462 km away from the satellite constellation. Satellites from the constellation fly over the

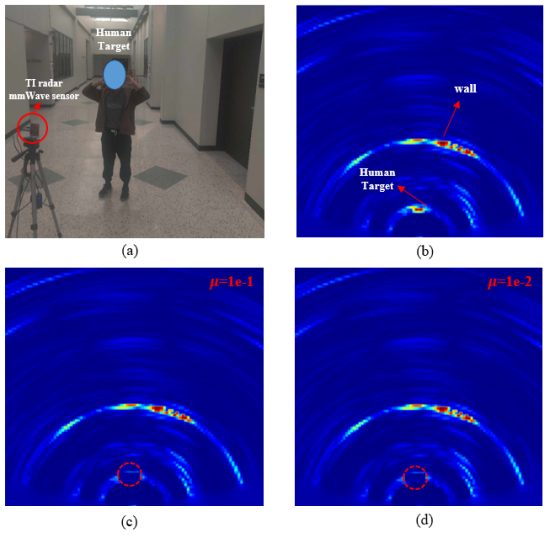


Fig. 5. Real attack experiment using the TI radar sensor. (a) A person (target) stands in front of the sensor. (b) Sensing results without attack. (c)-(d) The target is camouflaged with our attack.

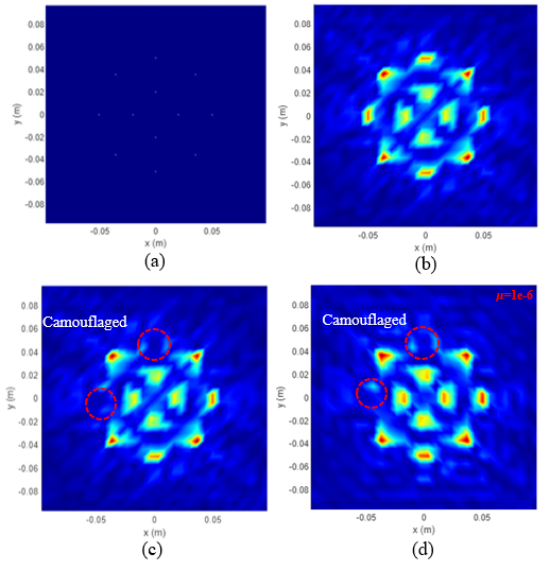


Fig. 6. Satellite imaging simulation. (a) A twelve-point target for satellite imaging. (b) Satellite image without attack. (c) Desired image with camouflage. (d) Reconstructed camouflage image under attack.

target for imaging. The reconstructed image $\hat{\mathbf{x}}^v$ without attack is shown in Fig.6(b). The desired camouflage image $\mathbf{x}^t$ is shown in Fig.6(c). With the attack, the satellite generates the image $\hat{\mathbf{x}}$ shown in Fig.6(d), which fits well with the desired image Fig.6(c).

E. Transferability of the Attack

So far we have assumed both the victim sensor and the attack sensor use the BPA algorithm. To verify the transferability of our attack algorithm, we let the victim sensor use the LIA algorithm, a lightweight RF imaging algorithm from

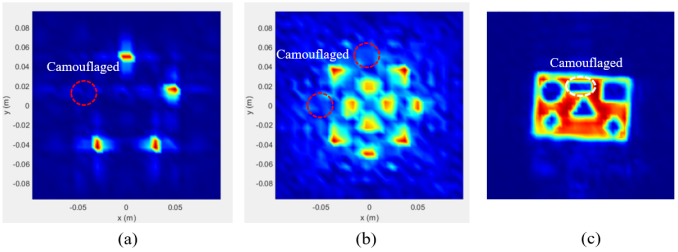


Fig. 7. Transferability: when the victim sensor and the attack sensor use different imaging algorithms, (a),(b), and (c) are similar to the results obtained in Simulations A, D, B.

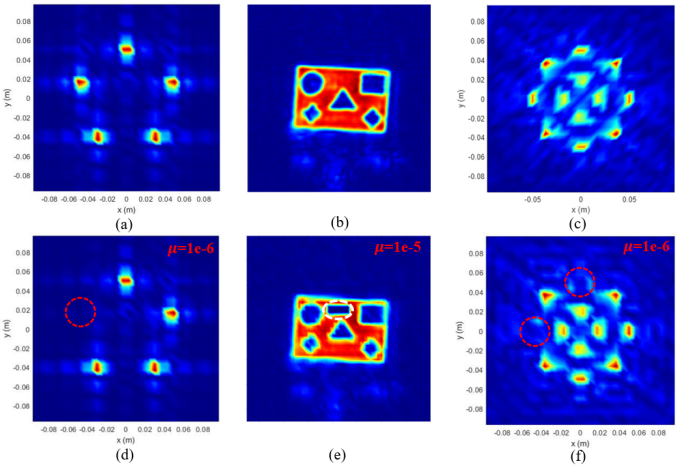


Fig. 8. Robustness of attack when exact sensor location is unknown. (a)-(c) images without attack. (d)-(f) victim sensor's images under attack.

[18], while the attack sensor still uses BPA. For the simulation scenarios A, D, and B, the reconstructed images under the new attack are shown in Fig. 7. We can see that the attack is still successful, which demonstrates that the attack is transferable among various imaging algorithms.

F. Robustness of the Attack

The victim's sensor's true location $\mathbf{r}'$ as well as the matrices $\mathbf{H}^v$ and $\mathbf{H}^a$ may be different from those estimated by the attack sensor. To assess the robustness of our attack method in this case, we simulate a scenario where the attacker lacks accurate sensor location information. We generate several different sensor location groups. One group is used by the attack sensor to generate reference data, while the victim sensor uses another group randomly. Applying this strategy, we rerun Simulations A, B, and D. The victim sensor's reconstructed images without attack and with attack are shown in Fig. 8. The camouflage attack is still successful, which demonstrates that the attack is fairly robust.

V. Conclusion

Despite the significant research focus on RF sensing and imaging systems, the susceptibility of these systems to cyber threats, especially evasive attacks, has received limited

attention. In this paper, we introduce a new evasive attack called "camouflage attack" that can make the RF imaging system produce clear yet erroneous images and can evade the detection of the RF imaging system. We demonstrate its effectiveness, transferability, and robustness via a set of simulations with simulated data, real measured data, as well as real experiments. Our future work will focus on mitigating the vulnerabilities of RF imaging systems to prevent attack scenarios such as the one introduced in this paper.

ACKNOWLEGEMENT

This paper is approved for Public Release on 27 March 2024. Distribution is Unlimited. Case Number: AFRL-2024-1676.

This research was partly supported by the Air Force Office for Scientific Research (AFOSR) and the Air Force Research Laboratory / Information Directorate (AFRL/RI) Internship program for summer 2023. The views and conclusions contained herein are those of the authors and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of the Air Force Research Laboratory or the U.S. Government.

REFERENCES

[1] L. Chao, M. N. Afsar, and K. A. Korolev, "Millimeter wave dielectric spectroscopy and breast cancer imaging," in *2012 7th European Microwave Integrated Circuit Conference*, pp. 572–575, IEEE, 2012.

[2] V. Dey, V. Pudi, A. Chattopadhyay, and Y. Elovici, "Security vulnerabilities of unmanned aerial vehicles and countermeasures: An experimental study," in *2018 31st international conference on VLSI design and 2018 17th international conference on embedded systems (VLSID)*, pp. 398–403, IEEE, 2018.

[3] S. Z. Gurbuz and M. G. Amin, "Radar-based human-motion recognition with deep learning: Promising applications for indoor monitoring," *IEEE Signal Processing Magazine*, vol. 36, no. 4, pp. 16–28, 2019.

[4] F. García-Rial, D. Montesano, I. Gómez, C. Callejero, F. Bazus, and J. Grajal, "Combining commercially available active and passive sensors into a millimeter-wave imager for concealed weapon detection," *IEEE Transactions on Microwave Theory and Techniques*, vol. 67, no. 3, pp. 1167–1183, 2018.

[5] D. M. Sheen, D. L. McMakin, and T. E. Hall, "Three-dimensional millimeter-wave imaging for concealed weapon detection," *IEEE Transactions on microwave theory and techniques*, vol. 49, no. 9, pp. 1581–1592, 2001.

[6] K. Chetty, G. E. Smith, and K. Woodbridge, "Through-the-wall sensing of personnel using passive bistatic wifi radar at standoff distances," *IEEE Transactions on Geoscience and Remote Sensing*, vol. 50, no. 4, pp. 1218–1226, 2011.

[7] S. Dahhani, M. Raji, M. Hakdaoui, and R. Lhissou, "Land cover mapping using sentinel-1 time-series data and machine-learning classifiers in agricultural sub-saharan landscape," *Remote Sensing*, vol. 15, no. 1, p. 65, 2022.

[8] A. M. Akhtar, W. A. Qazi, S. R. Ahmad, H. Gilani, S. A. Mahmood, and A. Rasool, "Integration of high-resolution optical and sar satellite remote sensing datasets for aboveground biomass estimation in subtropical pine forest, pakistan," *Environmental Monitoring and Assessment*, vol. 192, pp. 1–17, 2020.

[9] P. Ge, H. Gokon, and K. Meguro, "A review on synthetic aperture radar-based building damage assessment in disasters," *Remote Sensing of Environment*, vol. 240, p. 111693, 2020.

[10] J. Elliott, "Earth observation for the assessment of earthquake hazard, risk and disaster management," *Surveys in geophysics*, vol. 41, no. 6, pp. 1323–1354, 2020.

[11] J. P. Robin, M. Lafitte, and E. Coiras, "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.

[12] J. Liu, H. Liu, Y. Chen, Y. Wang, and C. Wang, "Wireless sensing for human activity: A survey," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 3, pp. 1629–1645, 2019.

[13] S. A. Shah and F. Fioranelli, "Rf sensing technologies for assisted daily living in healthcare: A comprehensive review," *IEEE Aerospace and Electronic Systems Magazine*, vol. 34, no. 11, pp. 26–44, 2019.

[14] X. Wang, X. Wang, and S. Mao, "Rf sensing in the internet of things: A general deep learning framework," *IEEE Communications Magazine*, vol. 56, no. 9, pp. 62–67, 2018.

[15] Y. Gu, J. Zhan, Y. Ji, J. Li, F. Ren, and S. Gao, "Mosense: An rf-based motion detection system via off-the-shelf wifi devices," *IEEE Internet of Things Journal*, vol. 4, no. 6, pp. 2326–2341, 2017.

[16] E. J. Baranoski, "Through-wall imaging: Historical perspective and future directions," *Journal of the Franklin Institute*, vol. 345, no. 6, pp. 556–569, 2008.

[17] F. Adib and D. Katabi, "See through walls with wifi!," in *Proceedings of the ACM SIGCOMM 2013 conference on SIGCOMM*, pp. 75–86, 2013.

[18] X. Li and Y. Chen, "Lightweight 2d imaging for integrated imaging and communication applications," *IEEE Signal Processing Letters*, vol. 28, pp. 528–532, 2021.

[19] H. Kim, R. Bandyopadhyay, M. O. Ozmen, Z. B. Celik, A. Bianchi, Y. Kim, and D. Xu, "A systematic study of physical sensor attack hardness," in *2024 IEEE Symposium on Security and Privacy (SP)*, pp. 143–143, IEEE Computer Society, 2024.

[20] M. L. Psiaki and T. E. Humphreys, "Gnss spoofing and detection," *Proceedings of the IEEE*, vol. 104, no. 6, pp. 1258–1270, 2016.

[21] J. S. Warner and R. G. Johnston, "A simple demonstration that the global positioning system (gps) is vulnerable to spoofing," *Journal of security administration*, vol. 25, no. 2, pp. 19–27, 2002.

[22] T. E. Humphreys, B. M. Ledvina, M. L. Psiaki, B. W. O'Hanlon, P. M. Kintner, *et al.*, "Assessing the spoofing threat: Development of a portable gps civilian spoofer," in *Proceedings of the 21st International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS 2008)*, pp. 2314–2325, 2008.

[23] T. Morong, P. Puričer, and P. Kovář, "Study of the gnss jamming in real environment," *International Journal of Electronics and Telecommunications*, pp. 65–70, 2019.

[24] F. Dimc, M. Bažec, D. Borio, C. Gioia, G. Baldini, and M. Basso, "An experimental evaluation of low-cost gnss jamming sensors," *Navigation: Journal of The Institute of Navigation*, vol. 64, no. 1, pp. 93–109, 2017.

[25] H. Hu and N. Wei, "A study of gps jamming and anti-jamming," in *2009 2nd international conference on power electronics and intelligent transportation system (PEITS)*, vol. 1, pp. 388–391, IEEE, 2009.

[26] Z. Haider and S. Khalid, "Survey on effective gps spoofing countermeasures," in *2016 Sixth International Conference on Innovative Computing Technology (INTECH)*, pp. 573–577, IEEE, 2016.

[27] S. Liu, X. Cheng, H. Yang, Y. Shu, X. Weng, P. Guo, K. C. Zeng, and Y. Yang, "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.

[28] K. C. Zeng, Y. Shu, S. Liu, Y. Dou, and Y. Yang, "A practical gps location spoofing attack in road navigation scenario," in *Proceedings of the 18th international workshop on mobile computing systems and applications*, pp. 85–90, 2017.

[29] J. Bhatti and T. E. Humphreys, "Hostile control of ships via false gps signals: Demonstration and detection," *NAVIGATION: Journal of the Institute of Navigation*, vol. 64, no. 1, pp. 51–66, 2017.

[30] M. L. Psiaki, S. P. Powell, and B. W. O'Hanlon, "Gnss spoofing detection using high-frequency antenna motion and carrier-phase data," in *proceedings of the 26th international technical meeting of the satellite division of the Institute of Navigation (ION GNSS+ 2013)*, pp. 2949–2991, 2013.

[31] K. Wang, S. Chen, and A. Pan, "Time and position spoofing with open source projects," *black hat Europe*, vol. 148, pp. 1–8, 2015.

[32] D. A. M. d. Silva, "Gps jammimg and spoofing using software defined radio," Master's thesis, University Institute Of Lisbon, 2017.

[33] M. E. Yanik, *Millimeter-Wave Imaging Using MIMO-SAR Techniques*. The University of Texas at Dallas, 2020.

[34] X. Li, L. Dorje, Y. Wang, Y. Chen, and E. Ardiles-Cruz, "High-resolution imaging satellite constellation," in *Proceedings of the InforSymbiotics/Dynamic Data Driven Applications Systems (DDDAS2022)*, pp. 1–5, 2022.