SCIENCE CHINA
Information Sciences

• LETTER •

August 2023, Vol. 66 189304:1–189304:2
https://doi.org/10.1007/s11432-022-3672-7

Few-shot RF fingerprinting recognition for secure satellite remote sensing and image processing

Di LIN, Su HU*, Weiwei WU & Gang WU

National Key Laboratory of Science and Technology on Communication, University of Electronic Science and Technology of China, Chengdu 610054, China

Received 11 August 2022/Revised 3 November 2022/Accepted 30 December 2022/Published online 26 July 2023

Citation Lin D, Hu S, Wu W W, et al. Few-shot RF fingerprinting recognition for secure satellite remote sensing and image processing. Sci China Inf Sci, 2023, 66(8): 189304, https://doi.org/10.1007/s11432-022-3672-7

We consider the security issues in a satellite remote sensing (SRS) and image processing system. Specifically, we present a novel architecture of a secure SRS image recognition system by using a radio frequency (RF) fingerprint to identify whether a satellite user is authenticated or not. For unauthenticated users, we address the method of adding perturbation into their received SRS images, which can degrade the performance of SRS image recognition at the end of unauthenticated users. For authenticated users, we propose a novel attention mechanism model to recognize rotating objects, which can increase the accuracy of detecting SRS images.

Few-shot RF fingerprinting recognition algorithm. In the first part, we focus on the RF fingerprinting recognition when only a few RF training samples are available. In such a scenario, the performance of most existing algorithms dramatically degrades. In this study, we propose a few-shot RF fingerprinting recognition algorithm based on a matching network model. A matching network consists of two parts: the embedding function module and the fully-conditional embedding (FCE) module.

We design the embedding function module by introducing an attention kernel function, which uses the Euclidean distance to calculate the similarity between samples as

$$L(f(x),g(\bar{x}))=\sqrt{(f(x_{\rm I})-g(\bar{x}_{\rm I}))^2+(f(x_{\rm Q})-g(\bar{x}_{\rm Q}))^2}, \tag{1}$$

where x and $\bar{x}$ represent the data in the support and query sets, respectively. $x_{\rm I}$ and $x_{\rm Q}$ represent the I-channel and Q-channel signals, respectively. g represents the embedding function on a support set, and f represents the embedding function on a query set.

The loss function of a matching network model can be represented as

$$\mathrm{Loss}(x)=\mathrm{E}\left\{\sum_x e^{L(f(x),g(\bar{x}))}\Big/\sum_{x,\bar{x}} e^{L(f(x),g(\bar{x}))}\right\}, \tag{2}$$

where $\mathrm{E}\{\cdot\}$ denotes the expectation.

We propose an FCE module which adopts the bidirectional long short-term memory (LSTM) network to strengthen the embedding functions g and f, respectively. Given the sample x in the support set, we can use the embedding function g to encode x as $g'(x)$. Afterward, we use the bidirectional LSTM model to obtain the forward output A and the backward output A'. Finally, we can attain the output vector $g(x)$ as

$$g(x)=g'(x)+A(g'(x))+A'(g'(x)). \tag{3}$$

For the embedding function f of the query set samples, an LSTM network model with an attention mechanism is adopted. We can achieve the state of the final hidden layer h_k with a step size of k by the function of $\mathrm{LSTM}(x,h,c)$ from (4). Also, we can calculate the attention kernel function with a bidirectional LSTM network $A_{\rm LSTM}$ as

$$(h_k,c_k)=\mathrm{LSTM}(f(x),h_{k-1},c_{k-1}), \tag{4}$$

$$A_{\rm LSTM}(h_{k-1},g(x))=e^{h_{k-1}g(x)}\Big/\sum_x e^{h_{k-1}g(x)}. \tag{5}$$

Image perturbation algorithm. We present image perturbation for unauthenticated users. For SRS image recognition, we need to consider the rotation of objects in an image. Thus, a few off-the-shelf adversarial algorithms which modify the values of pixels in the original images may have low performance on SRS image recognition. Therefore, we slightly change the directions of objects in the image to achieve high robustness of SRS image recognition. Specifically, we propose a spatially transformed adversarial (STA) algorithm for a high level of robustness in image recognition as follows.

Let F denote the pixel difference between the original image Q and the adversarial sample $Q_{\rm adv}$ (i.e., the image Q with perturbation). If $Q_{\rm adv}^{(j)}$ represents the jth pixel of $Q_{\rm adv}$, $(x_{\rm adv}^{(j)},y_{\rm adv}^{(j)})$ denotes the coordinate point of $Q_{\rm adv}^{(j)}$. Let $F_j=(\triangle x^{(j)},\triangle y^{(j)})$ be the difference between Q and $Q_{\rm adv}$ at their jth pixel point. We can calculate the coordinate point of $Q^{(j)}$ as $(x^{(j)},y^{(j)})=(x_{\rm adv}^{(j)}+\triangle x^{(j)},y_{\rm adv}^{(j)}+\triangle y^{(j)})$.

* Corresponding author (email: husu@uestc.edu.cn)

We employ a differentiable bilinear interpolation [1] to represent the values of pixels in the image as

$$Q_{\mathrm{adv}}^{(j)} = \sum_{i \in S(x^{(j)}, y^{(j)})} Q^{(i)}(1 - |x^{(j)} - x^{(i)}|)(1 - |y^{(j)} - y^{(i)}|), \tag{6}$$

where $S(x^{(j)}, y^{(j)})$ denotes the neighborhood of $(x^{(j)}, y^{(j)})$, including top-left, top-right, bottom-left, bottom-right pixels. With the function of F, we can modify the direction of the objects in the images, thereby improving the robustness of SRS image recognition.

To achieve the function of F, we can define the objective function as

$$F^* = \arg\min_F \mathcal{G}_{\mathrm{adv}}(Q, F) + \epsilon \mathcal{G}_{\mathrm{smo}}(F), \tag{7}$$

where $\mathcal{G}_{\mathrm{adv}}(Q, F)$ denotes the loss of object misclassification, $\mathcal{G}_{\mathrm{smo}}(F)$ indicates the loss of the smoothness of spatial changes, and ϵ denotes the balance between two losses. We present two types of losses as

$$\mathcal{G}_{\mathrm{adv}}(Q, F) = \max_{i \neq j} C(Q_{\mathrm{adv}})_i - C(Q_{\mathrm{adv}})_j, \tag{8}$$

where $C(p)$ represents the classification of p;

$$\mathcal{G}_{\mathrm{smo}}(F) = \sum_i^{\text{all pixels}} \sum_{j \in S(i)} \sqrt{\left\|\triangle x^{(i)} - \triangle x^{(j)}\right\|_2^2 + \left\|\triangle y^{(i)} - \triangle y^{(j)}\right\|_2^2}, \tag{9}$$

where $\mathcal{G}_{\mathrm{smo}}(F)$ represents the total difference of coordinate points around a pixel. The minimum loss in (9) can guarantee the similar difference and direction of the points around the pixel point i to smooth the spatial changes.

Image recognition algorithm. We present the problem of image recognition when a satellite user is identified as authenticated. This model primarily includes a convolutional attention mechanism module.

By introducing the attention mechanism, we propose a novel convolutional block attention module (CBAM) for image recognition. A CBAM model comprises two independent modules: the channel attention module and the spatial attention module. Channel attention is responsible for understanding which input features are expected to extract, and its mathematical representation is shown as

$$M_{\mathrm{c}}(F) = \sigma(W_1(W_0(F_{\mathrm{avg}}^c)) + W_1(W_0(F_{\mathrm{max}}^c))), \tag{10}$$

where F_{max}^c and F_{avg}^c represent the maximum pooling and mean pooling on the feature map F, respectively. W_0 and W_1 are the weights of a two-layer neural network. σ represents the parameter of ReLU in the neural network. $M_{\mathrm{c}}(F)$ represents the output of channel attention.

Spatial attention is responsible for understanding which pixels to focus on, and its mathematical representation is shown as

$$M_{\mathrm{s}}(F) = \sigma(G(F_{\mathrm{max}}^c, F_{\mathrm{avg}}^c)), \tag{11}$$

where $G(x)$ represents a convolutional layer to extract the features. $M_{\mathrm{s}}(F)$ represents the output of spatial attention.

Experiments. For RF fingerprinting recognition, we experiment by collecting RF data with universal software radio peripherals (USRP), composed of a NI-PXIe 1085 device and three USRP-RIO-2943 devices to simulate four satellite earth stations [2]. For image recognition, we collect the SRS images from the dataset of DOTA. These SRS images are originally from different data sources, including Google Earth and JL-1 satellite [3]. These DOTA images contain various objects at different scales, orientations, and shapes, and they are annotated by experts using 15 common object classes.

The experiment results show that our matching network-based algorithm can outperform the other RF fingerprinting recognition algorithms when only a small amount of RF data are available, e.g., in remote sensing. Also, our proposed STA algorithm can dramatically reduce image recognition accuracy at the unauthenticated user end. This algorithm outperforms its benchmark algorithms in confusing unauthenticated users. Our proposed CBAM algorithm for image recognition outperforms its benchmarks, including the SCRDet algorithm, the R3Det algorithm, the YOLOv5 algorithm, and the ROT-YOLOv5 algorithm [4], which are the most widely used algorithms for target detection.

Conclusion. This study has proposed a secure SRS image processing system with RF fingerprinting for user authentication. Considering the small amount of RF data, we offer a few-shot RF fingerprinting recognition algorithm based on a matching network. Also, we propose an image perturbation method with the STA algorithm to confuse unauthenticated users to reduce the accuracy of recognizing SRS images. We design a CBAM-based image recognition algorithm for authenticated users to detect rotating targets. By comparing with a few benchmark algorithms, our proposed RF fingerprinting recognition algorithm, STA-based image perturbation method, and CBAM-based image recognition algorithm can achieve better performance.

Acknowledgements This work was partially supported by National Natural Science Foundation of China (Grant Nos. 61971092, 62222121) and Fundamental Research Funds for the Central Universities (Grant Nos. ZYGX2020ZB045, ZYGX2019J123, ZYGX2019J076).

Supporting information Appendixes A–D. The supporting information is available online at info.scichina.com and link.springer.com. The supporting materials are published as submitted, without typesetting or editing. The responsibility for scientific accuracy and content remains entirely with the authors.

References

1 Wu W W, Hu S, Lin D, et al. Reliable resource allocation with RF fingerprinting authentication in secure IoT networks. Sci China Inf Sci, 2022, 65: 170304

2 Xu Y, Tang J, Li B, et al. Adaptive aggregate transmission for device-to-multi-device aided cooperative NOMA networks. IEEE J Sel Areas Commun, 2022, 40: 1355–1370

3 Xia G S, Bai X, Ding J, et al. DOTA: a large-scale dataset for object detection in aerial images. In: Proceedings of IEEE/CVF Conference on Computer Vision and Pattern Recognition, 2018. 3974–3983

4 Li J, Li Y F, He L, et al. Spatio-temporal fusion for remote sensing data: an overview and new benchmark. Sci China Inf Sci, 2020, 63: 140301