SAKARYA UNIVERSITY JOURNAL OF COMPUTER AND INFORMATION SCIENCES
VOL. 5, NO. 2, AUGUST 2022
DOI: 10.35377/saucis.05.02. 1138577

Research Article

The Effect of Ambient Temperature On Device Classification Based On Radio Frequency Fingerprint Recognition

Ozkan Yilmaz[1], Mehmet Akif Yazici[2]
[1]Aselsan, Communications and Information Technologies Business Sector, Ankara, Türkiye; ozkanyilmaz@aselsan.com.tr
[2]Corresponding Author; Istanbul Technical University, Informatics Institute, Information and Communications Research Group, Istanbul, Türkiye; yazicima@itu.edu.tr; Tel: +90 212 285 71 94

Received 30 Jun 2022; Revised 06 August 2022; Accepted 06 August 2022; Published online 31 August 2022

Abstract

Physical layer authentication is an important technique for cybersecurity, especially in military scenarios. Device classification using radio frequency fingerprinting, which is based on recognizing device-unique characteristics of the transient waveform observed at the beginning of a transmission from a radio device, is a promising method in this context. In this study, the effect of the ambient temperature on the performance of radio device classification based on RF fingerprinting is investigated. The waveforms of the transient regions of the transmissions are recorded as images, and ResNet50 and InceptionV3 networks for image classification are used to determine the radio devices. The radio devices used in the study belong to the same brand, model, and production date, making the problem more difficult than classifying radio devices of different brands or models. Our results show that high levels of accuracy can be attained using convolutional neural network models such as ResNet50 and InceptionV3 when the test data and the training data are collected at the same temperature, whereas performance suffers when the test data and the training data belong to different temperature values. We provide the performance figures of a blended training model that uses training data taken at various temperature values. A comparison of the two networks is also provided.

Keywords: cybersecurity, device classification, radio frequency fingerprint, double sliding window, image classification, resnet50, inceptionV3

1. Introduction

Radio device recognition and classification is important from a cybersecurity point of view in many applications, such as law enforcement and military use cases. Radio frequency (RF) fingerprinting is one of the techniques that can be used in device classification. When a radio transmitter first turns on or starts broadcasting to the air, the signal emitted from the transmitter exhibits a transient behavior. The transient region duration may be in the order of microseconds, depending on the hardware of the transmitter. It has been shown that the transient behavior region contains unique features of the radio transmitter **[1]**. These unique features are due to the unique characteristics of hardware components such as analog converters, filters, power amplifiers, and frequency mixers used during the manufacturing of the transmitter layer, and various defects in the soldering process during the assembly of these components on the boards. In addition, the aging of the radio transmitter may cause the transient region to differ in devices with the same brand, model, and production date, even if they are products of a high quality manufacturing process. The signal characteristics in the transient region are different for each radio transmitter, which is called the RF fingerprint.

Encryption algorithms are mainly used to identify a wireless device that has been authorized by the system. In an encrypted communication system, a two-way communication is required to generate a session key **[2]**. However, the security algorithm will be compromised during access to the key, thus making it difficult to distinguish a legitimate key. Such problems encountered in encrypted communication systems can be effectively solved by using physical layer security **[3]**. At this point, it would be correct to explain the physical layer security. Physical layer security is the practice of identifying wireless devices by extracting unique features embedded in the electromagnetic waves

emitted from transmitters **[4]**. Physical layer security based on the recognition of these unique features is known as Radio Frequency (RF) fingerprinting **[5]**. Radio frequency fingerprinting has been applied to various communication technologies and standards, including cognitive radio networks **[6]**, Universal Mobile Telecommunications System (UMTS) **[7]**, Wi-Fi **[8]**, push-to-talk transmitters **[9]**, bluetooth **[10]**, and Radio-Frequency Identification (RFID) **[11]**.

RF fingerprint extraction has been done by high-end receiver devices in many studies. Rehman et al. **[12]** showed that there is practically no need for high-level receiver equipment to obtain RF fingerprinting, but low-level receiver equipment can also be used. In addition, they tested the performance of the RF fingerprinting systems they developed against impersonation attacks. Tekbas et al. **[13]** classified different models and brands of radios with RF fingerprints and examined the effects of ambient temperature, battery voltage, and ambient noise on the classification success during classification. High-end receiver equipment is used for RF fingerprinting. Riyaz et al. **[14]** examined the use of convolutional neural networks for device classification with RF fingerprinting. Rehman et al. **[15]** counts the effects of the ages of the devices, the ambient temperature, and the mobility of the devices during the fingerprinting process on the fingerprints as further issues to be explored. Wang et al. **[16]** discussed the low performance of device classification by RF fingerprinting, and proposed deep complex residual networks as a new method to overcome this problem. The deep complex residual network has been integrated into the RF fingerprint extraction and the device classification model, and it has been found that the accuracy rates in device classification have increased. Suski et al. **[17]** investigated the use of RF fingerprinting for the security of commercial devices broadcasting in the IEEE 802.11a standard. In many studies, the ambient temperature is ignored as a parameter of the device classification with RF fingerprinting.

In this study, narrowband radios with the same brand, model, and production date were used to investigate the effect of the ambient temperature on RF fingerprinting. We also demonstrate that device classification, identification, and similar procedures can be performed at low cost using low-level receiver hardware for RF fingerprinting. RF fingerprints of the radios were obtained at ambient temperatures of −5, 10, 25, and 40 ºC. The obtained RF fingerprints were classified at different temperatures with the convolutional neural network models ResNet50 and InceptionV3, which are branchs of deep learning. Contrary to the studies in the literature, the images of the waveforms of the transient regions of the radios were used to train the ResNet50 and InceptionV3 networks. In other words, RF fingerprint extraction is combined with image processing. The results show that the ambient temperature significantly affects the performance of device classification based on RF fingerprints.

2. Radio Frequency Fingerprint

Physical layer authentication is one of the key technologies used to secure wireless communications. RF fingerprints [18], which are the results of the electrical properties of the components on the device hardware, contain features that are difficult to clone. Classification of devices with RF fingerprinting consists of the steps shown in Figure 1.

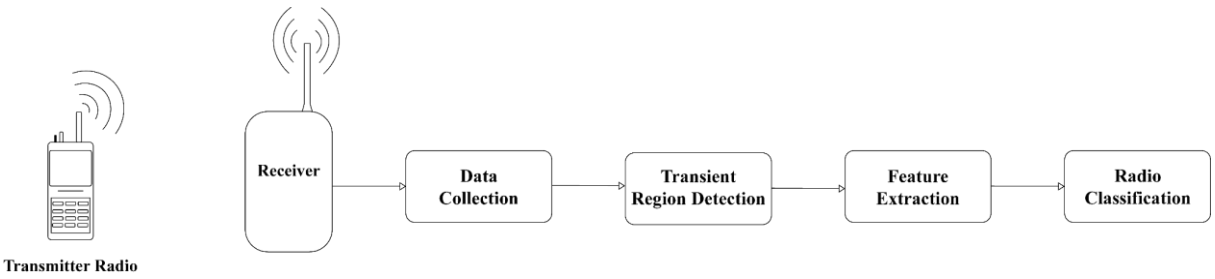

Figure 1 Device classification model with radio frequency fingerprint.

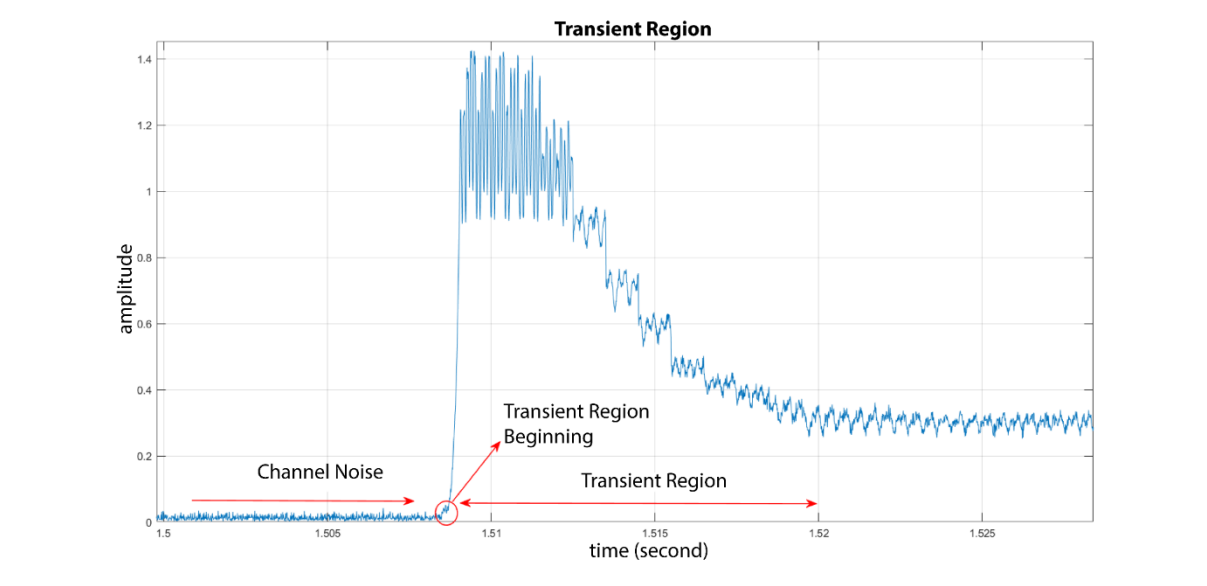

Figure 2 A sample transient region obtained during the study.

For this study, radios with the same brand, model, and production date operating in the UHF band are used as transmitter radios. In order to avoid the possible effects of aging on RF fingerprinting, care has been taken to ensure that the production dates are the same. A low-level commercial product, Adalm Pluto software defined radio (SDR) was used as the receiving device. Data collection was carried out with the help of the Adalm Pluto plugin of the Matlab software. Transient region detection, feature extraction, and device classification processes were also performed on Matlab.

2.1 Transient Region Detection

Detection of the transient region and fingerprinting from this region is the most important step in device identification with RF fingerprinting. An incorrectly detected transient region may adversely affect the fingerprinting step, and the classification process may therefore be inaccurate. For transient region detection, the features of the signal in the time domain are extracted. Bayesian step change, threshold detection, and double sliding window are the most widely used methods for transient region detection **[19]**. All three methods basically use the differences in the amplitudes of the signals in the noise region and transient region. The noisy region is the period where the channel is not carrying any data signals. During the transition from this region to the transient region, a sudden change occurs in the signal. In

For signals with gradual transitions, Bayesian step change and threshold detectors may be delayed to detect the beginning of the transient region. For this reason, their performance may suffer. Hence, the double sliding window method is preferred for the transient region detection.

2.2 The Double Sliding Window Method

The double sliding window method is a kind of rising edge detection algorithm that detects the energy increase in the incoming signal **[20]**. For this, the incoming signal is convolved with a two-window filter of a certain length. The signal energy covered under the right window is divided by the signal energy covered under the left window. At the starting point of the signal, the energy of the right window significantly exceeds the left window and an upward peak is formed in the running ratio. Likewise, when the double sliding window exits the signal, while the left window is still in the signal region, the right window switches to the noise section. Thus, the ratio of the energy of the signal corresponding to the right window to that of the left window peaks downward **[19]**. In Figure 3, the graph of the energy generated when the double sliding window moves over the signal while it passes into the transient region of the signal is demonstrated.

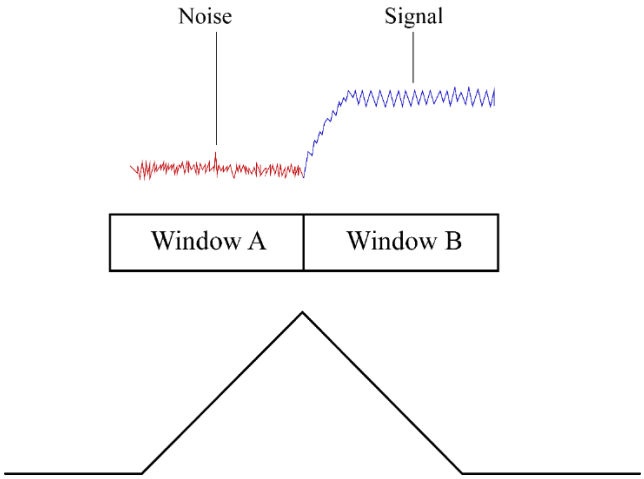

Figure 2 The ratio of the energy of the signal in window A to the energy of the signal in window B in the double sliding window method. The peak marks the beginning of the transient region.

Figure 4 shows the detection of the beginning of the transient region with the double sliding window method on a sample signal obtained in the study. After the beginning of the transient region is determined, its end must also be determined. In this study, the end of the transient region was chosen based on the observations, going forward a certain time from the starting point on the time axis.

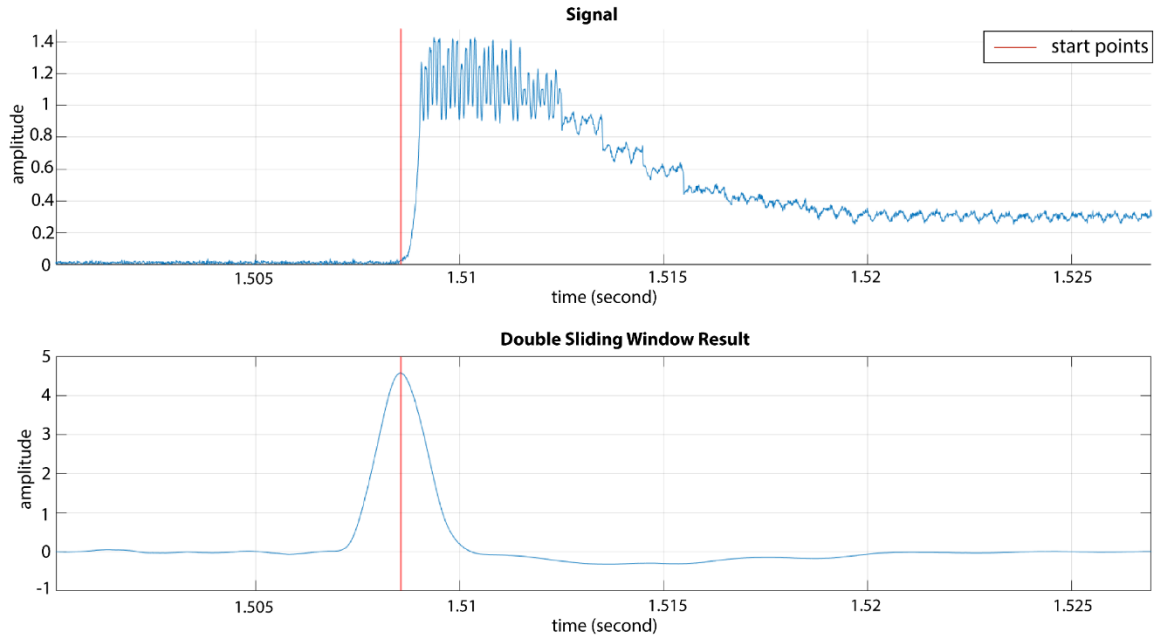

Figure 4 Detection of the transient region by the double sliding window method. The red bar marks the peak of the energy ratios in the bottom figure, and the beginning of the transient region in the top figure.

3. Methodology

The effect of ambient temperature on device classification with RF fingerprinting was investigated in a laboratory environment. For transient region detection, which is the most important step for RF fingerprinting, the double sliding window method is used. After the beginning of the transient region was determined, the end of the transient region was determined empirically, based on the experimental study. Unlike other studies, instead of using the I/Q data of the signals in the transient region, images of

the transient region in png format were used. 288.6 Gb data was collected in baseband (.bb) format with the help of Adalm Pluto SDR for 5 different radios of the same brand, model, and year of manufacturing at 4 temperature values. ResNet50 and inceptionV3 convolutional neural network models, two of the most successful models for image classification, in Matlab library were used for classification. A Weisstechnik brand temperature cabinet, which is an advanced ambient temperature test cabinet, was used to adjust the temperature of the environment. This cabinet constantly monitors the temperature inside, and ensures that the surface temperature of the radio device and the temperature of the inside of the cabinet are equal. After the devices were placed inside the cabinet, they were kept for 1 hour until the desired ambient temperature was achieved. The radio device under test is programmed to automatically transmit for 2 seconds via an option cable extended outside through the heat-proof slots at the entrance of the cabinet, followed by a 3-second silence, periodically.

In addition, an external thermocouple is mounted on the temperature pulse surface of the radio inside the cabinet. Thus, the temperature on the device was also monitored outside the cabinet's own thermometer. It was observed during the tests that the temperature on the surface of the devices increased up to a further 2 degrees beyond the temperature of the test cabinet. Adalm Pluto SDR is positioned as far away from the temperature test cabinet as possible so that the radio under test is not affected by the signals that may be reflected from its body as well as the antenna, and to avoid noise. The power outputs are programmed to be 1 Watt so that the radios do not overheat while transmitting. Furthermore, in order not to be affected by ambient noise, the air interface was scanned with an Aeroflex IFR device, and a frequency value (415.125 MHz) with minimal noise was selected. During the test process, batteries with high capacity were used to avoid possible current fluctuations that may occur near the end of the battery charge. The test setup is shown in Figure 5. The ResNet50 and inceptionV3 models were run on an NVIDIA GEFORCE 940MX graphics card.

4. Numerical Results

5 radios of the same brand, model, and production year were used for the study. The radios were given identification labels as A, B, D, E, and X. Each of the radios were placed in the test cabinet at temperatures of −5, 10, 25, and 40 ºC[*]. Each radio made 2200 transmissions at each temperature value. Therefore, a total of $\mathbf{5 \times 4 \times 2200 = 44000}$ png images were obtained as the data set. For each radio and temperature pair, 2000 images out of the total 2200 images were used for training the ResNet50 model, and the remaining 200 images were used for testing the device classification. The total number of images taken from 5 radios at each temperature for the training of ResNet is $\mathbf{5 \times 2000 = 10000}$.

Table 1 shows the ResNet50 performance of the classification by RF fingerprints from the baseband signals collected from these temperature values radios. We trained the model using the data from the four different temperature values, and tested for the four different temperature values. As can be seen in Table 1, the performance of the classification depends on the temperature.

[*] Extreme increases were detected in the surface temperatures of the radios under test in the temperature cabinet, measured by thermocouple at temperatures of 55 ºC, and hence, we decided not to collect data for 55 ºC and above.

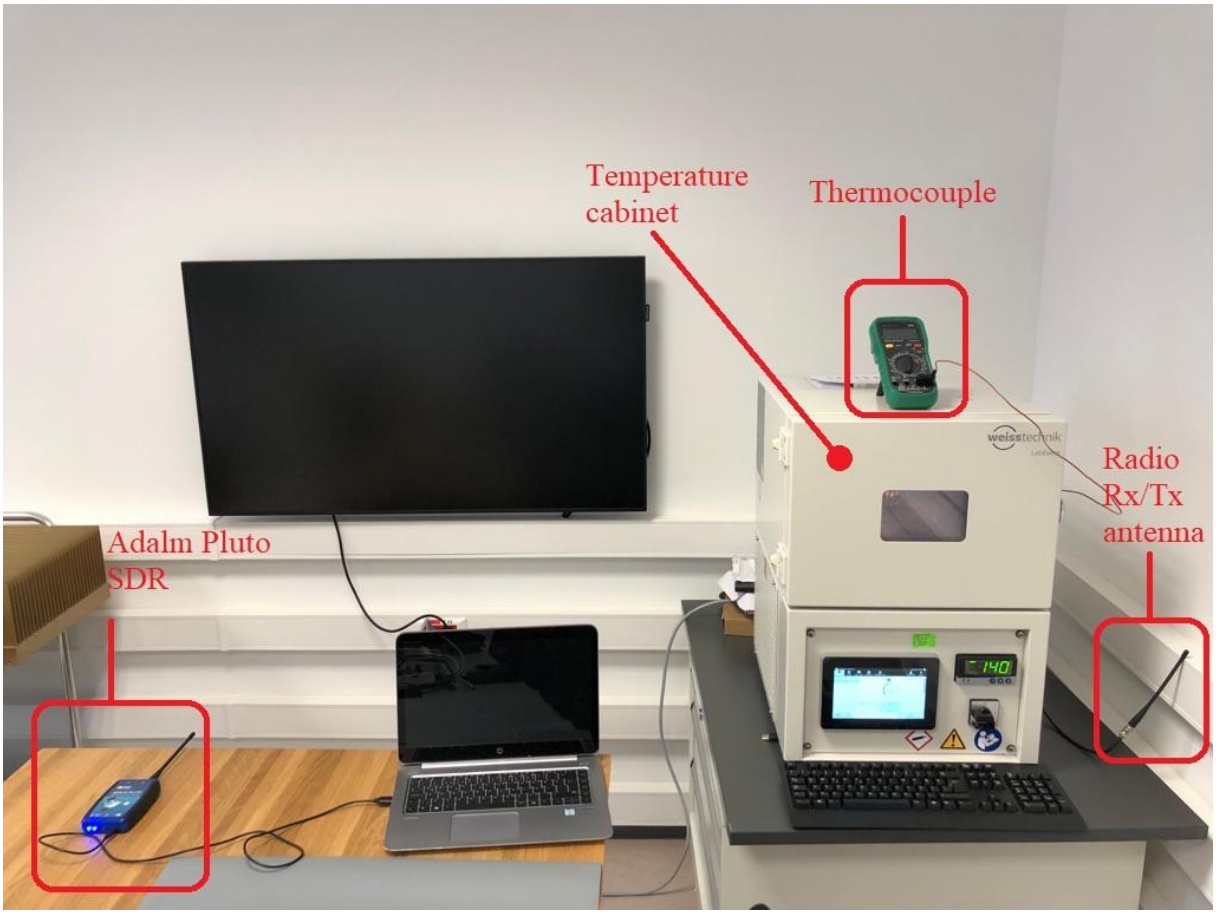

Figure 3 Data collection setup.

Table 1 ResNet50 classification performance of temperature dependent radios.

	Test Temperature			
Training Temperature	−5°C	10°C	25°C	40°C
−5°C	88.35%	42.04%	39.08%	43.04%
10°C	36.79%	91.02%	41.65%	21.47%
25°C	20.28%	51.73%	96.39%	32.94%
40°C	39.91%	19.9%	21.96%	94.7%

The best classification performance, 96.39% accuracy, was obtained with training and test data both collected at 25 ºC. On the other hand, the classification performance among the cases where the training and the test data belong to the same temperature value was the lowest at −5 ºC with an accuracy of 88.35%. While the performance is relatively high when training and test data come from the same temperature experiments, testing data from different temperatures than the training data was obtained seriously reduces the performance. The lowest performance was observed when the training data was taken at 40 ºC and the test data at 10 ºC.

Table 2 shows the InceptionV3 performance of the classification by RF fingerprints under the same scenario. As can be seen from Table 2, the best classification performance, 96.47% accuracy, was obtained with training and test data both collected at 40 ºC, closely followed by the case where the training and the test data both collected at 25 ºC. In the case of using test and training data at the same temperature, the lowest performance was obtained at −5 ºC with 86.42%. Similar to ResNet50, the classification performance obtained with the training and the test data selected at the same temperature in InceptionV3 is higher than the classification performance made with the test and training data at different temperatures. The lowest performance was observed when the training data was taken at 40 ºC and the test data at 25 ºC.

Table 2 InceptionV3 classification performance of temperature dependent radios.

	Test Temperature			
Training Temperature	−5°C	10°C	25°C	40°C
−5°C	86.42%	44.90%	41.75%	44.22%
10°C	35.57%	89.29%	43.95%	20.59%
25°C	22.36%	52.24%	95.67%	21.82%
40°C	39.81%	24.90%	20.31%	96.47%

As can be clearly understood from Tables 1 and 2, the ambient temperature is an important factor in device classification with RF fingerprinting and cannot be ignored. Another inference that can be made here is that the temperature of the devices significantly contributes to the RF fingerprints. Increases and decreases in ambient temperature cause the components in the hardware layer of the device to exhibit different characteristics, thus leading to somewhat different RF fingerprints for the same device at different temperatures.

4.1 Device Classification with Blended Training Model

In an effort to reduce the effect of ambient temperature on the performance, especially for the scenarios where the test case temperature differs from the temperature the training data was collected, the training data of the ResNet50 and InceptionV3 networks were selected for each radio in an equal amount from each temperature. Test data was given to these trained networks in an equal amount of data from each radio at every temperature, and the classification process was repeated. Classification performances are given in Tables 3 and 4 for ResNet50 and InceptionV3, respectively. As can be seen from the ResNet50 classification performance in Table 3, while the performances of the model for the test data collected at 10, 25, and 40 ºC are decent, the performance at −5 ºC turns out to be significantly lower.

As can be seen from the InceptionV3 classification performance in Table 4, the lowest performance was obtained at the test temperature of −5 ºC, as in ResNet50. On the other hand, at test temperatures of −5, 10, and 25 ºC, ResNet50 showed better performance than InceptionV3. At 40 ºC, Inceptionv3 has a slightly better performance than ResNet50.

Table 3 ResNet50 classification performance of radios with training data including all temperatures.

	Test Temperature			
Training Temperature	−5°C	10°C	25°C	40°C
−5°, 10°, 25°, 40°C	52.08%			
−5°, 10°, 25°, 40°C		84.80%		
−5°, 10°, 25°, 40°C			88.35%	
−5°, 10°, 25°, 40°C				85.98%

Table 4 InceptionV3 classification performance of radios with training data including all temperatures.

	Test Temperature			
Training Temperature	−5°C	10°C	25°C	40°C
−5°, 10°, 25°, 40°C	44.62%			
−5°, 10°, 25°, 40°C		69.08%		
−5°, 10°, 25°, 40°C			71.96%	
−5°, 10°, 25°, 40°C				87.25%

4.2 Normalized Confusion Matrices

Figure 6 shows the classification performances and errors in percentage of the 5 radios trained at −5 ºC and classified with test data at −5 ºC for ResNet50 and InceptionV3 models. The horizontal axis shows the estimated classes of the radios on the model outputs, and the vertical axis shows the correct classes. The diagonal elements of the matrix indicate the percentage of a radio being classified correctly, and the other elements indicate the percentages of misclassification. Similarly, Figures 7 – 9 show the confusion matrices for training and test at 10, 25, and 40 ºC, respectively. Furthermore, Figures 10 – 13 show the confusion matrices for the blended training model for tests with –5, 10, 25, and 40 ºC. One observation from the confusion matrices is that in some settings, one or two radio devices are difficult to correctly classify, whereas the other devices are classified with high accuracy. One such example is radio device X under the setting where ResNet50 is used on the training and the test data collected at −5 ºC, seen in Figure 6.

The results demonstrate that while device classification based on RF fingerprinting using transient region images is viable, a difference in the temperature values that the training data was taken and the classification is executed significantly affects the accuracy. When the blended training data is used, the accuracy is improved compared to the settings where the temperature values for the training and the test data are different. In this case, ResNet50 performs better than InceptionV3. When the test is performed at – 5 ºC, both methods suffer significantly. Therefore, when operating at lower temperatures, better classifiers should be designed.

5 Conclusion and Future Work

In this study, we investigated the effect of the ambient temperature on the performance of radio device classification based on RF fingerprinting. The radio devices used in the study belong to the same brand, model, and production date, making the problem more difficult than classifying radio devices of different brands or models. In our study, we performed the classification of devices by processing the images of radio frequency fingerprints. In terms of this approach, we used a different method from other studies. Our results show that high levels of accuracy can be attained using convolutional neural network models such as ResNet50 and InceptionV3 when the test data and the training data are collected at the same temperature, whereas performance suffers when the test data and the training data belong to different temperature values. Hence, we conclude that the ambient temperature cannot be ignored in future studies in the field of RF fingerprinting. We have also shown that device classification via RF fingerprinting can be done using SDRs with lower cost, easier to use and open source applications, instead of using dedicated devices such as high-cost complex circuit receivers and oscilloscopes. On the other hand, no big difference in performance was observed in the classification made with ResNet50 and InceptionV3. It has also been observed that ResNet50 can classify more successfully at temperatures of –5, 10, 25 ºC in blended training model. In the same model, at 40 ºC, InceptionV3 had slightly better accuracy. For this reason, a mixed CNN model can be used for different temperatures as well as a blended training model.

Future studies will focus on improving the classification performance under different temperature values. Possible approaches to be investigated include training multiple models for different temperatures and making a classification decision based on the majority of these models.

During the collection of RF fingerprint data in this study, the transmitting and receiving devices were kept stationary. Collecting RF fingerprint data in scenarios where the receiver and transmitter are mobile will be an important study to see the effects of channel distortions. The aging of RF fingerprinted devices will change fingerprints. Therefore, the effect of device aging requires further research. The effects of the output power of the transmitter devices on the RF fingerprint should also be investigated as an open issue.

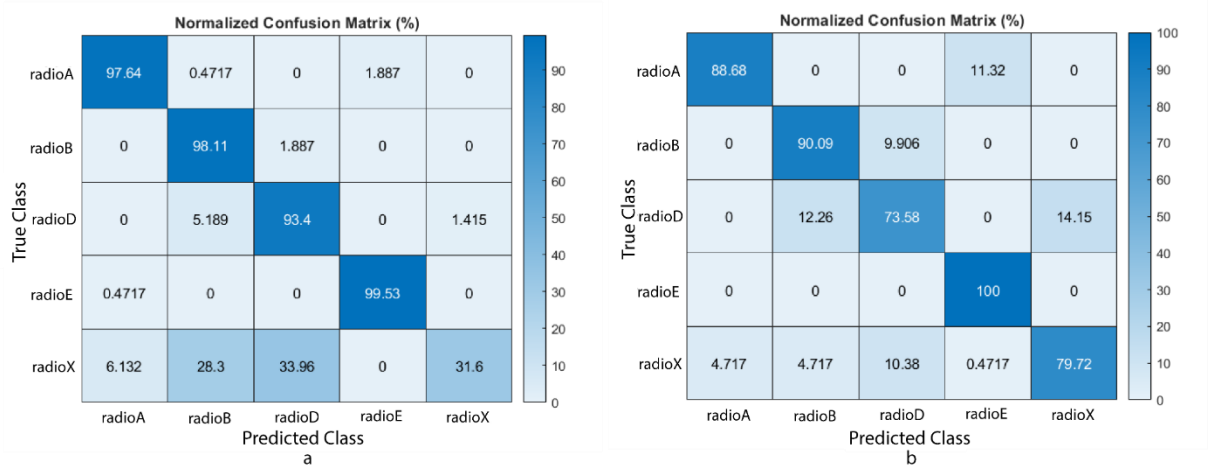

Figure 4 Normalized confusion matrices for: (a) −5 ºC training and test data for ResNet50, (b) −5 ºC training and test data for InceptionV3

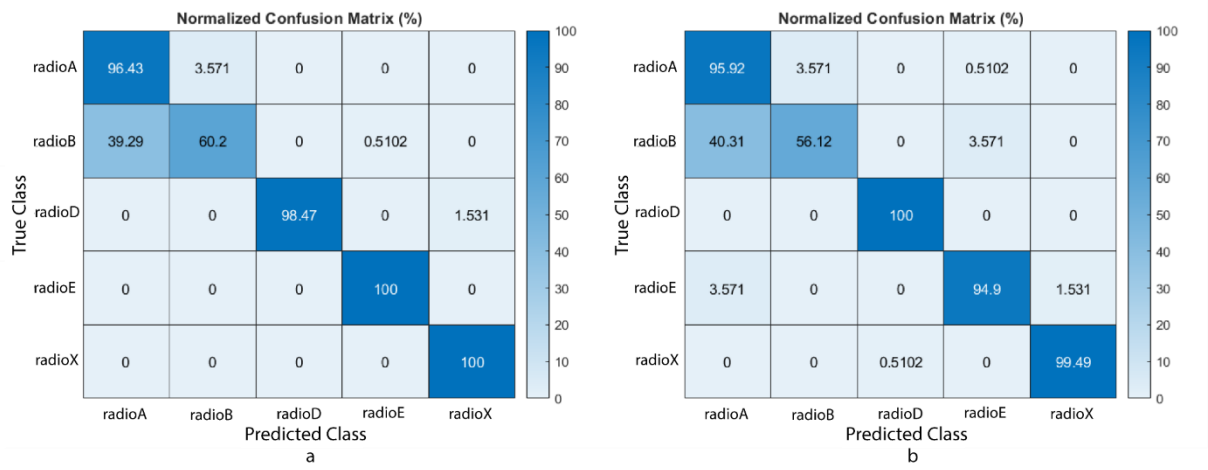

Figure 7 Normalized confusion matrices for: (a) 10 ºC training and test data for ResNet50, (b) 10 ºC training and test data for InceptionV3.

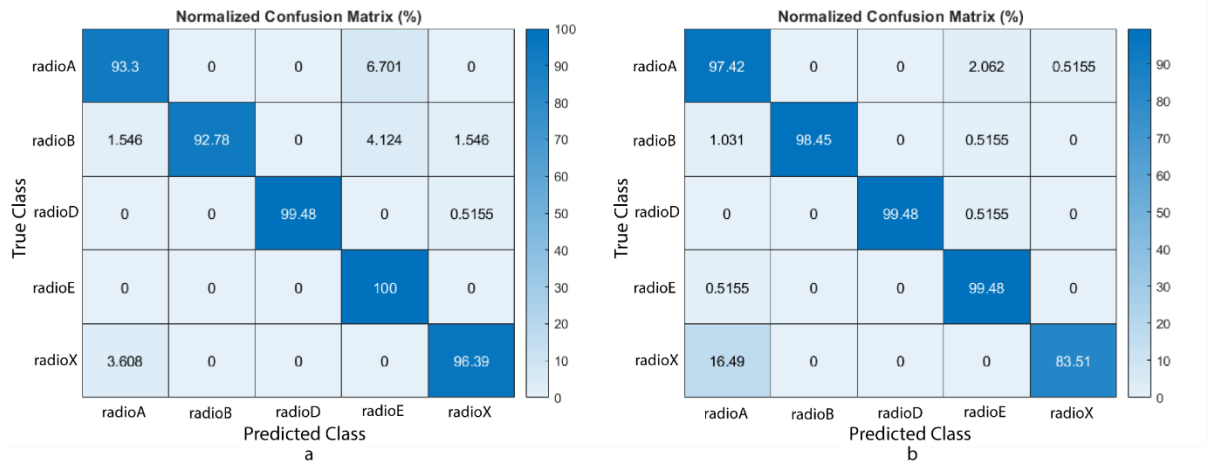

Figure 8 Normalized confusion matrices for: (a) 25 ºC training and test data for ResNet50, (b) 25 ºC training and test data for InceptionV3.

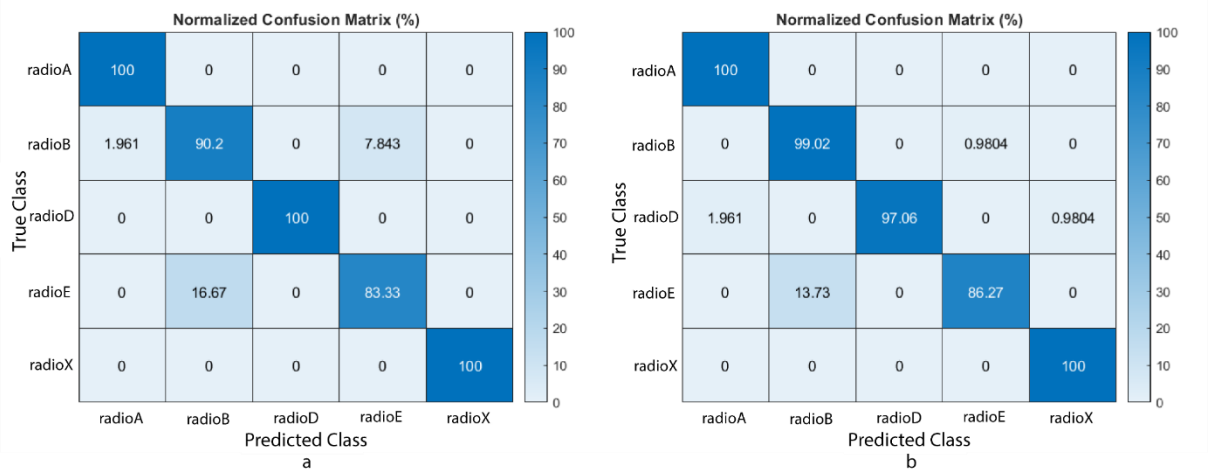

Figure 9 Normalized confusion matrices for: (a) 40 ºC training and test data for ResNet50, (b) 40 ºC training and test data for InceptionV3.

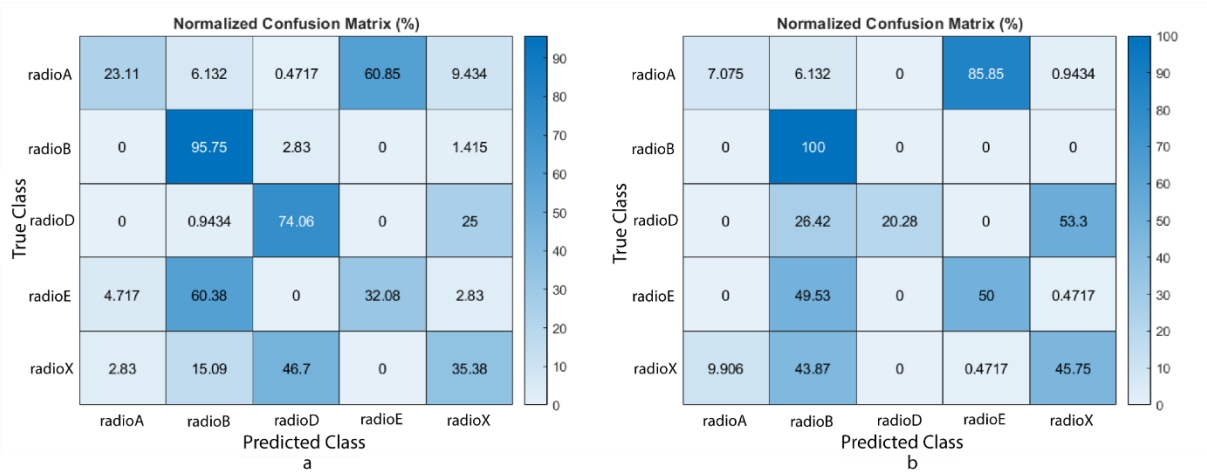

Figure 10 Normalized confusion matrices for −5, 10, 25, and 40 ºC blended training data and (a) −5 ºC test data for ResNet50, (b) −5 ºC test data for InceptionV3.

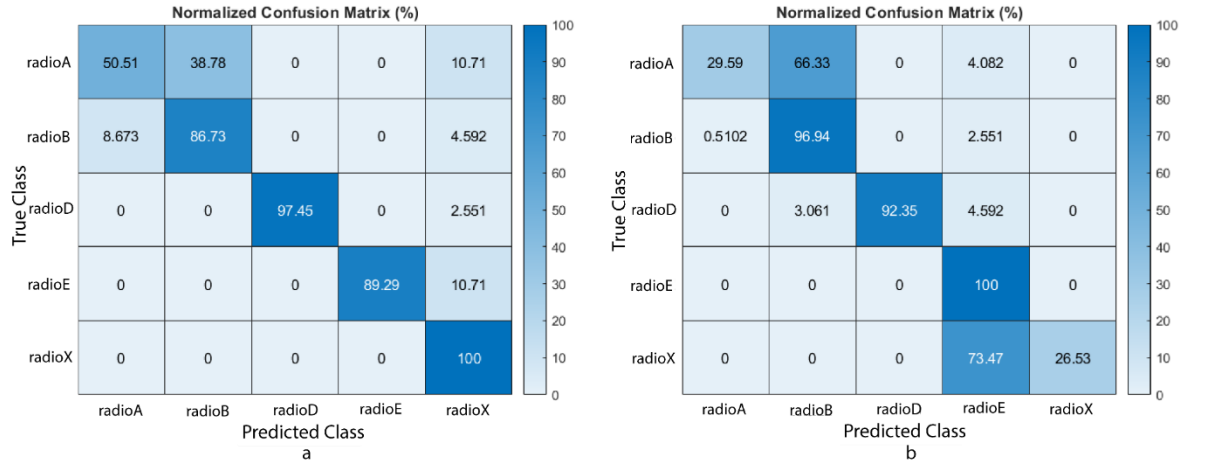

Figure 11 Normalized confusion matrices for −5, 10, 25, and 40 ºC blended training data and (a) 10 ºC test data for ResNet50, (b) 10 ºC test data for InceptionV3.

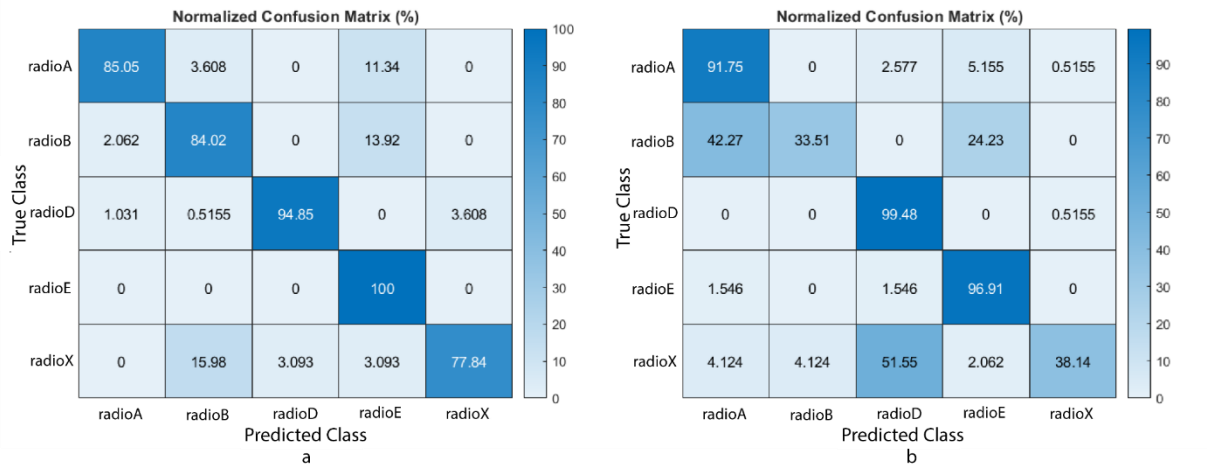

Figure 12 Normalized confusion matrices for −5, 10, 25, and 40 ºC blended training data and (a) 25 ºC test data for ResNet50, (b) 25 ºC test data for InceptionV3.

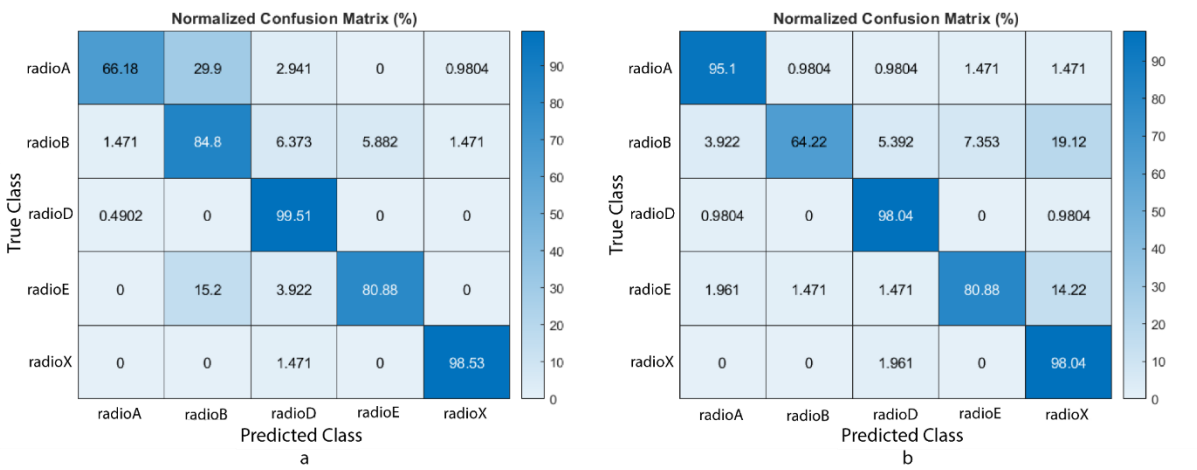

Figure 13 Normalized confusion matrices for −5, 10, 25, and 40 ºC blended training data and (a) 40 ºC test data for ResNet50, (b) 40 ºC test data for InceptionV3.

References

[1] O. Ureten and N. Serinken, "Wireless security through RF fingerprinting," *Canadian Journal of Electrical and Computer Engineering*, vol. 32, no. 1, pp. 27-33, 2007.

[2] D. R. Reising, M. A. Temple and M. J. Mendenhall, "Improving intra-cellular security using air monitoring with RF fingerprints," in *2010 IEEE Wireless Communication and Networking Conference*, Sydney, NSW, Australia, 2010.

[3] A. C. Polak, S. Dolatshahi and D. L. Goeckel, "Identifying wireless users via transmitter imperfections," *IEEE Journal on selected areas in communications*, vol. 29, no. 7, pp. 1469-1479, 2011.

[4] S. Mathur, A. Reznik, C. Ye, R. Mukherjee, A. Rahman, Y. Shah, W. Trappe and N. Mandayam, "Exploiting the physical layer for enhanced security [security and privacy in emerging wireless networks]," *IEEE Wireless Communications*, vol. 17, no. 5, pp. 63-70, 2010.

[5] B. Danev, H. Luecken, S. Capkun and K. El Defrawy, "Attacks on physical-layer identification," in *Proceedings of the third ACM conference on Wireless network security*, Hoboken, New Jersey, USA, 2010.

[6] K. Merchant, S. Revay, G. Stantchev and B. Nousain, "Deep learning for RF device fingerprinting in cognitive communication networks," *IEEE Journal of Selected Topics in Signal Processing*, vol. 12, no. 1, pp. 160-167, 2018.

[7] I. O. Kennedy and A. M. Kuzminskiy, "RF fingerprint detection in a wireless multipath channel," in *7th International Symposium on Wireless Communication Systems*, York, UK, 2010.

[8] O. Ureten and N. Serinken, "Bayesian detection of Wi-Fi transmitter RF fingerprints," *Electronics Letters*, vol. 41, no. 6, pp. 373-374, 2005.

[9] J. Toonstra and W. Kinsner, "A radio transmitter fingerprinting system ODO-1," in *Proceedings of 1996 Canadian Conference on Electrical and Computer Engineering*, Calgary, AB, Canada, 1996.

[10] M. Woelfle, M. Temple, M. Mullins and M. Mendenhall, "Detecting, identifying and locating bluetooth devices using RF fingerprints," in *2009 Military Communications Conference (MILCOM 2009)*, Boston, MA, USA, 2009.

[11] D. Zanetti, B. Danev and S. Capkun, "Physical-layer identification of UHF RFID tags," in *Proceedings of the sixteenth annual international conference on Mobile computing and networking*, Chicago, IL, USA, 2010.

[12] S. U. Rehman, K. W. Sowerby and C. Coghill, "Analysis of impersonation attacks on systems using RF fingerprinting and low-end receivers," *Journal of Computer and System Sciences*, vol. 80, no. 3, pp. 591-601, 2014.

[13] O. Tekbas, N. Serinken and O. Ureten, "An experimental performance evaluation of a novel radio-transmitter identification system under diverse environmental conditions," *Canadian Journal of Electrical and Computer Engineering*, vol. 29, no. 3, pp. 203-209, 2004.

[14] S. Riyaz, K. Sankhe, S. Ioannidis and K. Chowdhury, "Deep learning convolutional neural networks for radio identification," *IEEE Communications Magazine*, vol. 56, no. 9, pp. 146-152, 2018.

[15] S. U. Rehman, K. W. Sowerby, S. Alam and I. Ardekani, "Radio frequency fingerprinting and its challenges," in *2014 IEEE Conference on Communications and Network Security*, San Francisco, CA, USA, 2014.

[16] S. Wang, H. Jiang, X. Fang, Y. Ying, J. Li and B. Zhang, "Radio frequency fingerprint identification based on deep complex residual network," *IEEE Access*, vol. 8, pp. 204417-204424, 2020.

[17] W. C. Suski II, M. A. Temple, M. J. Mendenhall and R. F. Mills, "Radio frequency fingerprinting commercial communication devices to enhance electronic security," *International Journal of Electronic Security and Digital Forensics*, vol. 1, no. 3, pp. 301-322, 2008.

[18] N. Soltanieh, Y. Norouzi, Y. Yang and N. C. Karmakar, "A review of radio frequency fingerprinting techniques," *IEEE Journal of Radio Frequency Identification*, vol. 4, no. 3, pp. 222-233, 2020.

[19] D. Shaw and W. Kinsner, "Multifractal modelling of radio transmitter transients for classification," in *IEEE WESCANEX 97 Communications, Power and Computing*, Winnipeg, MB, Canada, 1997.

[20] J. Terry and J. Heiskala, OFDM wireless LANs: A theoretical and practical guide, Indianapolis, Indiana, USA: Sams publishing, 2002.

[21] J. Li, D. Bi, Y. Ying, K. Wei and B. Zhang, "An improved algorithm for extracting subtle features of radiation source individual signals," *Electronics*, vol. 8, no. 2, p. 246, 2019.