Project：RF Fingerprint Feature Extraction and Radio Device Identification

Author	

Background of RFF Research

Wireless communication is a subject of rapid development, in the coming era of the fifth generation wireless network, wireless communication network is anticipated to provide higher throughput, lower latency and higher quality of service (QoS)[1]. The high capability of 5G wireless network will boost the development of IoT applications and thus a surge increase of the population of RF devices is expected. On the other hand, with the wireless networks become more complicated, the demand of network security rises dramatically. For example, the future vehicle-to-everything (V2X) network depends on an unmistakable exchange of information between the vehicles and their surroundings. Under this network, an attack that provides fake information can possibly cause a huge danger to public health[2]. Thus, strong wireless security systems should be developed to guarantee the integration of future V2X systems. While there are lots of cryptography based security mechanisms designed for 5G and other wireless networks, physical layer security is also a new and promising topic.

Intuitively, physical layer security overtakes cryptography-based security (software layer security) by three aspects: 1. Physical layer security keys are hard to feign. The security keys of physical layer security systems are typically named "radio fingerprint", it exploits the hardware imperfection information of a radio device caused during manufacturing. 2. The performance of physical layer security systems does not depend explicitly on the computational complexity. The traditional cryptography-based security system relies on complex mathematical computation which is both power consuming and vulnerable to attackers with high computational ability, say, possibly quantum computers in the future. 3. The physical layer security keys are distributed automatically based on the device hardware information itself, which is easier for wireless network management under complex network structures compared with conventional approaches[3].

Notably, the most important component in a physical layer security system is the generation and distribution of security keys. In the context of this thesis, physical security key and radio frequency fingerprint are two interchangeable phrases. As a promising candidate to enhance or even replace the software layer security system of wireless networks, RFF systems are gaining the attentions of researchers in both institutes and industries. The following steps are presented in all works in designing RFF systems: 1. The original or down-converted RF signal is collected from the radio devices by oscilloscopes or SDR devices. 2. The acquired signal is processed with selected algorithms; this step is known as feature extraction. 3. The extracted features are fed to a classifier for classification. If the processed signal from different RF devices are separable from one another with considerable accuracy, the core functionality of the proposed RFF system is validated.

RFF Research Purposes

The two objectives of this thesis are: 1. Review the current development of radio frequency fingerprinting systems. 2. Propose, implement, and evaluate a universal software radio peripheral (USRP) and MATLAB based radio frequency fingerprinting system. The literature review should cover an overview of RFF systems' development during the last 10 years. A comprehensive analysis and comparison of current RFF systems will be conducted in the same chapter. The designed RFF system should successfully differentiate the RF fingerprints of cell phones with different brands using corresponding wireless local area network (WLAN) uplink signals. The system is implemented on USRP platform with MATLAB performing signal processing and machine learning tasks, a proper machine learning algorithm is chosen to maximize the performance. The performance of this system will be evaluated by testing the classification rate over a set of cell phones with different brands. As for future applications, the proposed RFF system could be implemented as the last defense in traditional radio access control systems so as to enhance the network security as physical level. The possibilities to further improve the RFF system will be discussed as well.

Overview of Related Technologies

Software Defined Radio:

The SDR platform is a handy tool for communications systems prototyping, the specific platform chosen in this thesis project is NI-USRP 2922. While most USRP platforms share the advantage of usability because they are officially supported by MATLAB, LabVIEW, GUN Radio and other open source software, USRP 2922 is chosen in this thesis for the following reasons:

1. The software of USRP2 platform is mature and stable, with easy access to many documents.
2. The hardware of USRP 2922 is just enough for this project: the RX bandwidth of USRP 2922 is 20MHz, which is sufficient for a lossless capture of typical WLAN signals; the RF sample rate of USRP 2922 can reach 25MSamples/s, providing over 200 samples for the WLAN L-STF signal, which is sufficient for wavelet transform.
3. The cost of USRP2 platform is much less than USRP3 platform, if a good performance of proven on the USRP2 platform, same result can be recurrent on better platforms.

In Fig. 1, the block diagram of NI-USRP 2922 is presented. During transmission, the digital signal is generated from the host personal computer (PC) and went through digital up-converter and digital to analog converter to become an analog signal. The signal then passes through the low-pass filter as a de-noise process before it is IQ modulated to the desired carrier frequency. Then, the signal is amplified and transmitted from the antenna. The receiving RF chain performs a similar but inversed process to capture, IQ demodulate, ADC and down-sample the RF signal collected from receiving (RX) antenna. Besides showing the detailed RF chain information, the diagram also indicated the information transmission bridge between USRP and the host PC. The host PC sends control information to USRP, which, in turn, submit the collected and down-sampled data to the host. The process is controlled indirectly by the software on the host PC using UHD API.

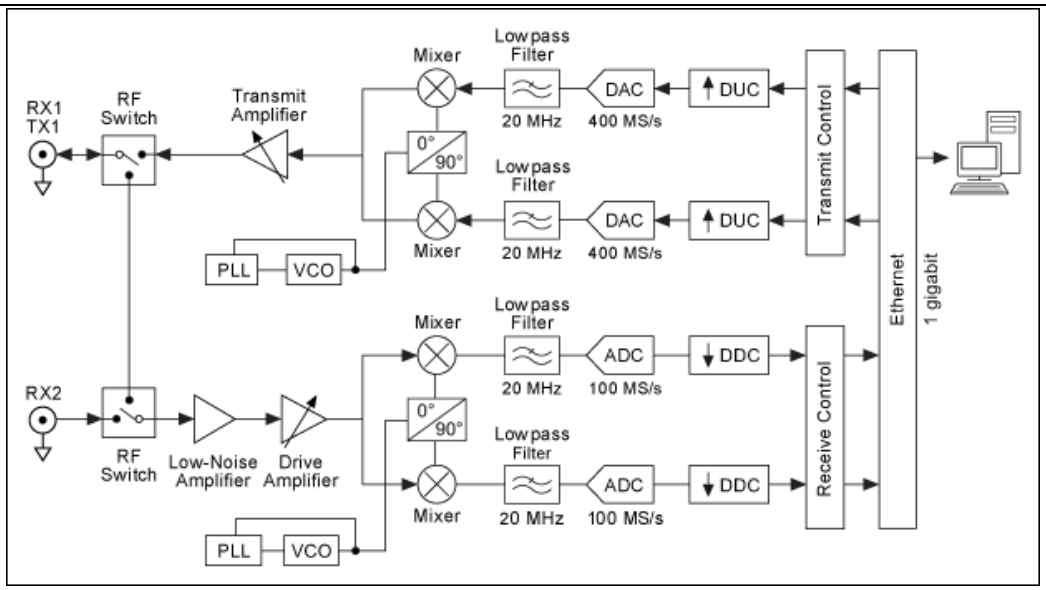

Fig. 1. The simplified block diagram of NI-USRP 2922[12] platform used in this project.

Wavelet Transform:

The wavelet transformation is different from Fourier transformations because it represents the signal with a property of "zooming" rather than frequency components. Initially, a wavelet is selected for the transformation, for illustration propose, we select the Haar wavelet to explain this transformation. The analytical function of Haar wavelet is given as[13]:

$$g(t) = \begin{cases} 1, & 0 \le t < 1/2 \\ -1, & 1/2 \le t < 1 \\ 0, & else \end{cases}$$

This wavelet can be translated and scaled to a family of wavelets using the following function:

$$g_{(a,b)}(t) = g\left(\frac{t-b}{a}\right)$$

The analytical equation of wavelet transform is given as an integral of the product of time domain signal with the selected wavelet using the following equation[13]:

$$S(a,b) = \int_{-\infty}^{+\infty} s(t) g_{(a,b)}(t) dt$$

where s(t) is the time domain signal, g_((a,b)) (t) is the wavelets as specified in equation 5. S(a,b) is the result of continuous wavelet transform as a function of a (scaling factor) and b (translational factor).

We illustrate the translation and scaling process in Fig. 2. The transformation of a time domain signal will be represented by the two parameters: a and b, where b contains the time domain information and a contains the scaling information, which is inversely proportional to angular frequency information ω.

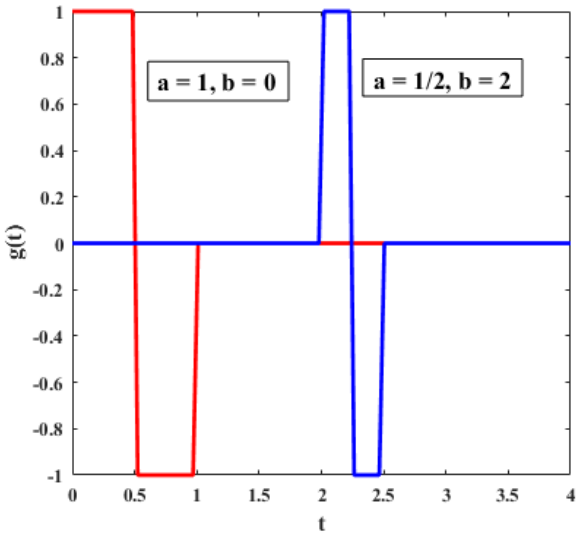

Fig. 2. The translation and scaling of Haar wavelet. the red waveform represents for the original Haar wavelet and the blue waveform represents for the Haar wavelet with a translation factor b=2 and scaling factor a=1\/2.

To help the readers with a better understand of the wavelet transform, an example of this transform applying to a human Electrocardiography (ECG) signal is given. Notice the result of wavelet transform is a function depending on two variables, thus a good practice of visualization will be 2D graph. Presented in Fig. 3 is the original ECG signal and the wavelet transformed signal, the wavelet transform result is converted to time-frequency domain.

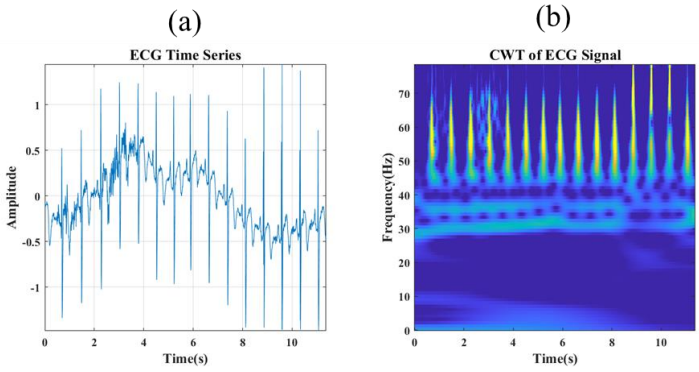

Fig. 3. The original ECG signal (a) and its time-frequency graph (b). The ECG data used is the "wecg" exemplary data in MATLAB[14].

By analyzing the time-frequency graph in Fig. 3, one will notice a steady-state frequency component between 30 and 40 hertz, as well as the peeks with over 70 hertz caused by heart beats. The time frequency graph generated by CWT helps revealing frequency information contained in the time series and at the same time, reserve the time sensitivity of original signal.

Convolutional Neural Network (CNN):

The CNN architecture, like any neural network, consist of three layers: input layer, hidden layer and output layer. The hidden layers of CNN are typically formed by convolutional layers, pooling layers, and fully connected layers. The simplified system diagram is given in Fig. 4.

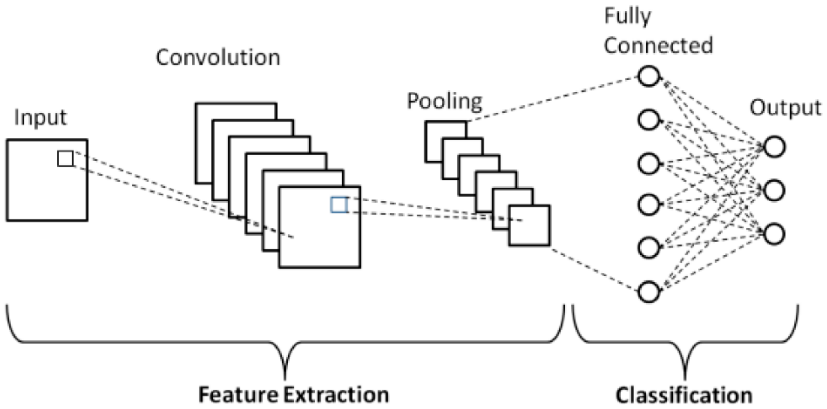

Fig. 4. Simplified diagram of a typical convolutional neural network.

the functions of each neural layer of this network are:

- A convolutional layer convolves the layer input to reduce its dimension and pass the result to the next layer. It is the core layer in CNN because it simplifies the number of neural drastically.
- The pooling layer is used to reduce the computation load by directly vanish some neural at the next layer. A pooling layer will typically divide inputs into several subclasses, select the maximum value or the average value in each subclass and pass the value to the next layer.
- Fully connected layer will not reduce the dimension of features, each neural in this layer is functional. This layer is reversion of the neural layers in shadow neural networks.

Benefited from the design of convolutional layers and pooling layer, the CNN is able to reduce the dimension of network input, thus reduce the computational complexity of image classification. The CNN featured in this thesis also works as an image classifier.

Proposed System Model

The RFF system proposed in this thesis consist of three major parts: data acquisition, wavelet transform and neural network. The overall system block diagram is given in Fig. 5, where the physical link is indicated by '--' arrows, the digital information flow is indicated with '-' arrows and the '.-' arrows give illustration figures showing the manipulation of data.

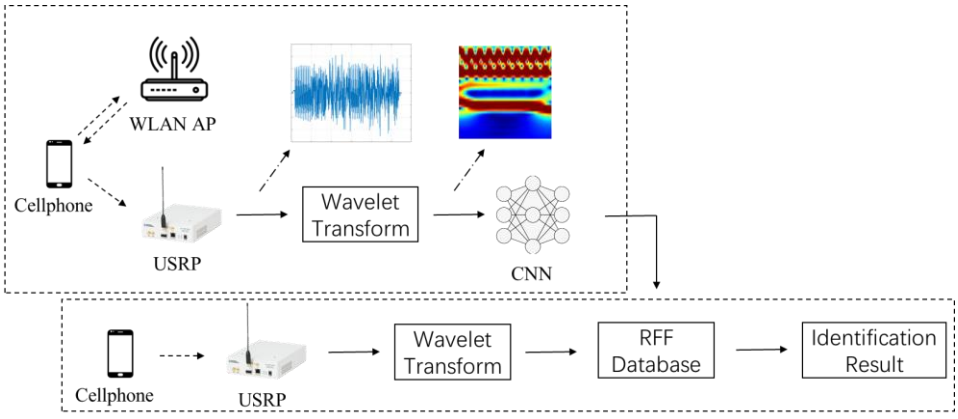

Fig. 5. System block diagram of the proposed RFF system.

The upper box in Fig. 4 shows the process of RFF database initialization. Firstly, USRP monitors the link between cellphone and WLAN access point (AP) and capture the packets transmitted by the cellphone. The signal is then sent to the host computer where the WLAN detection algorithm is running. The detection algorithm utilizes the auto correlation property of the WLAN legacy short training field (L-STF) training sequence[28] to detect the start of the L-STF of each packet. Then the entire L-STF sequence, considered as the carrier of RF fingerprint, is selected and passed to the wavelet transform algorithm. The wavelet transform algorithm then convert the time domain L-STF signal to time frequency domain graphs as shown in Fig. 4. The above sequence is performed for multiple times to collect enough time frequency graphs to train and validate the CNN classifier. Lastly, the trained classifier is stored at the local PC or the cloud server as an RFF database for radio device identification in the future.

The lower box in Fig. 4 demonstrates the process of device identification with an existing RFF database. The method of RF signal collection, WLAN packet detection and wavelet transform are identical to the database initialization process. After one L-STF sequence collected from an unknown device is converted to its time frequency graph, the figure is fed to the CNN classifiers running on local or cloud servers. To enhance the classification accuracy, the identity of more than one time-frequency graphs of the same unknown device should be evaluated at the classifier, and a voting algorithm will combine the classification results and give feedback to the network manager.

Theoretical Analysis

Carrier Frequency Offset:

n wireless transmitters, the carrier frequency is generated by the crystal oscillator and refined by phase lock loop (PLL). Because every transmitter is featured with an internal crystal oscillator, differences can occur with the carrier frequencies they generated[30]. Consider a transceiver system with accurate receiving carrier frequency, the offset of carrier frequency caused by the transmitter can be modeled as:

$$x_{offset}(t) = x(t)e^{j2\pi(f_{Tx}-f_{carrier})t} = x(t)e^{j2\pi\triangle_{CFO}t}$$

where Δ_CFO is the difference between standard carrier frequency and transmitter carrier frequency, x(t) is the baseband transmitting signal, and x_offset (t) is the received, offset signal.

The original signal is offset by △_CFO from the standard carrier frequency. To help with an intuitive understanding of the influence of carrier frequency, the constellation and time-frequency graphs of L-STF signal before and after frequency offset is given in Fig. 6. Notice the carrier frequency offset of 2Hz has caused a rotation of constellation points with constant angular frequency.

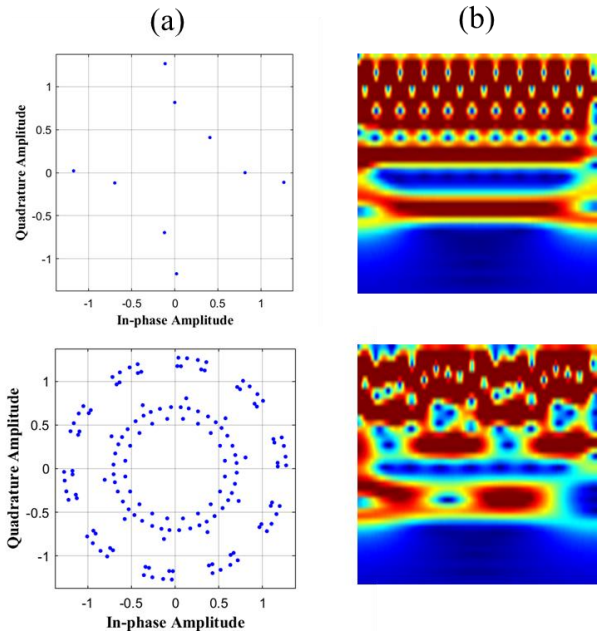

Fig. 6. The distortion of signal due to carrier frequency offset of 2Hz. (a) constellation graph and (b) time-frequency graph.

IQ Imbalance:

The signal distortion due to IQ impairment is shown in Fig. 7. Consistent to the above analysis, the constellation points are shifted around the genuine points. Notice that the shift distance for constellation points farer from the origin is longer than the inner ones. Fig. 7 (b) shows that the influence of IQ imbalance is visible on time-frequency domain, although the difference is vague to human eyes, a designated CNN classifier will tell it.

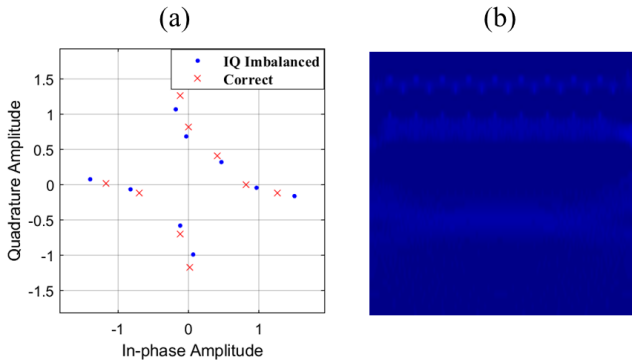

Fig. 7. The distortion of signal due to IQ imbalance (gain: 3dB, phase: π\/72). (a) comparison between correct constellation points and shifted points due to IQ imbalance. (b) differentiation result of time-frequency graphs w/ and w/o IQ imbalance

Nonlinear Distortions:

The nonlinear distortion modeled using refined Saleh model is presented in Fig. 8. It is noticeable that the influence due to nonlinearity is similar to that of IQ imbalance. Also, the time-frequency graph in Fig. 8(b) is more significantly different from the undistorted graph.

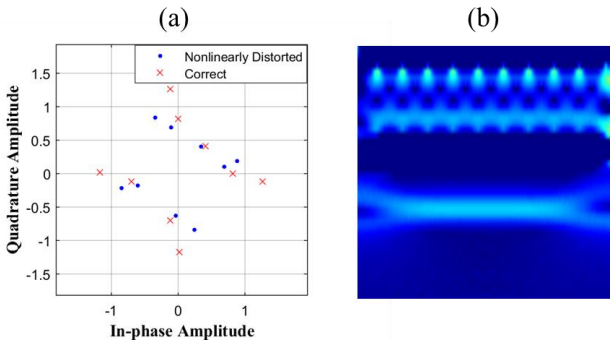

Fig. 8. Nonlinear distortion due to PAs, refined Saleh model. (a) comparison between correct constellation points and nonlinearly distorted points. (b) differentiation result of time-frequency graphs w/ and w/o nonlinear distortion.

Experiment Detail

USRP RF Signal Acquisition:

Recall Fig. 5 in the previous chapter, the USRP RF signal collection functionality is used in both the database initialization and device identification processes. And as the fundamental step of the proposed RFF system, a robust and effective RF signal acquisition block should be designed.

Firstly, under the circumstance of database initialization, to keep the WLAN signal of cellphone separable from that of WLAN AP, the USRP should be placed in close proximity to the cellphone. Secondly, the USRP is configured to work in burst mode which helps to identify whether the USRP is in underrun or overrun. The length of each frame collected from USRP is set to 10000 in this thesis and a total length of two seconds is collected.

RF Signal Preprocessing:

After the RF signal is collected from USRP and before submitting it to the CNN classifier, the WLAN L-STF sequences are selected from the collected signal. Then the time-domain graphs are generated based on continuous wavelet transform of selected L-STF signals.

After the starting samples of every effective WLAN packets are decided by the above algorithm, the L-STF sequence is selected. As defined in 802.11 documentation, the duration of the short training field is 8us, which corresponds to 160 samples if captured with a sample rate of 20MSamples/s. The selected STF sequences will likely be emitted by both the UE and the AP, thus, an algorithm is designed to separation STFs sent from different devices. The algorithm is based on received signal strength (RSS) of STFs, a primitive but effective method is to remove STFs with energy less than half of the maximum STF energy collected. This algorithm is sufficient for applications where the energy of STF signal remain relatively stable during the capturing period, and the power of AP sent STF signal is lower than one half of the UE transmitted STF signal. The above described scenario holds with most static WLAN systems.

The next step is to perform CWT on selected STF sequences. Similar to the algorithm of STF detection, before the time domain signal is pass to the CWT computer, it is normalized by its total power. This preprocessing makes sure that RSS does not become a dominant feature of the device fingerprint. The normalized STF sequence is then transformed to time-frequency

graphs by calling "cwt" function using Morse wavelet at a sample rate of 20MHz. Lastly, the scalograms are resized to 224*244*3 RGB figured and saved in jpeg format to the local file system.

Deep Learning Classification:

As already discussed above, the convolutional neural network is a powerful tool to classify the images. However, to train a neural network from sketch is still a computationally expensive task and requires a large amount of training data. Both of these criteria are not realistic during the design of this project. Thus, a substitutional CNN learning scheme is chosen in the fulfillment of this thesis. This scheme is known as transfer learning, which, based on an already-trained CNN classifier, leveraging its weights and modify the minimum number of layers to suit to the new classification task. In this case, the transfer learning algorithm aims to utilize an existing CNN to classify time-frequency graphs.

A widely used and well-performed CNN image classifier is GoogLeNet[36]. The network is of 22 layers deep and used a multi-convolutional layer structure to reduce the number of parameters. It is both powerful because of its great network depth, and easy to train due to its special feature reduction structure. Additionally, the GoogLeNet network is officially supported by MATLAB deep learning toolbox with two pre-trained versions, trained with ImageNet or Places365 datasets. These advantages of GoogLeNet makes it suitable for the transfer learning application in this project.

Experiment Result

Table 1 Testing device model and the corresponding abbreviation used in this thesis

Device model	Abbreviation
iPhone se (2020), white	IP_w
iPhone 8, black	IP_b
Redmi note 8, blue	RM_bl
Redmi note 8, white	RM_w
Honor 10 se, blue	HN_bl

In this experiment, a test set of five cellphones is selected as presented in table 1. They are selected for the following reasons:

1. The comparison between devices manufactured by three different brands tests the feasibility of the proposed RFF system with respect to the ability of differentiating different device manufacturers.
2. The classification rate of two different modeled iPhones can demonstrate the accuracy of the proposed RFF system when separating different device models from the same manufacturer.
3. The differentiation rate between two Redmi devices can evaluate the performance of the proposed RFF system when expected to identify different devices with “theoretically identical” hardware.

For each device, a two second signal is captured, which contains the WLAN packets sent

during the communication between this UE and the AP. One WLAN OFDM packet (I branch) for each cellphone is presented in Fig. 9, note the packets in this figure are separately collected and cascaded in one figure manually for better illustration.

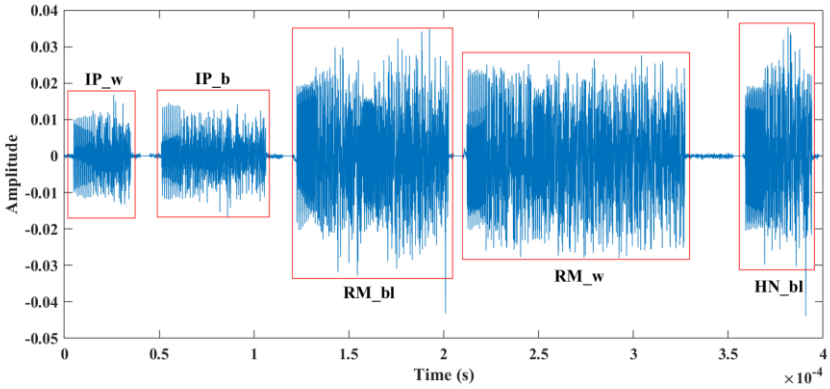

Fig. 9. Real part of raw WLAN packets collected from 5 devices under test. They are, from left to right: 1. IP_w; 2. IP_b; 3. RM_bl; 4. RM_w and 5. HN_bl.

We notice in Fig. 9, despite the signal power and packet length of these packets varies, all WLAN packets are complied with the 802.11 specifications, starting with L-STF sequence.

Next, the L-STF sequence is selected from the captured signal. During this process, a correlation based method is used to detect the start of every L-STF sequence, and the L-STF sequence of AP is filtered out based on a power selection algorithm as illustrated in Fig. 10.

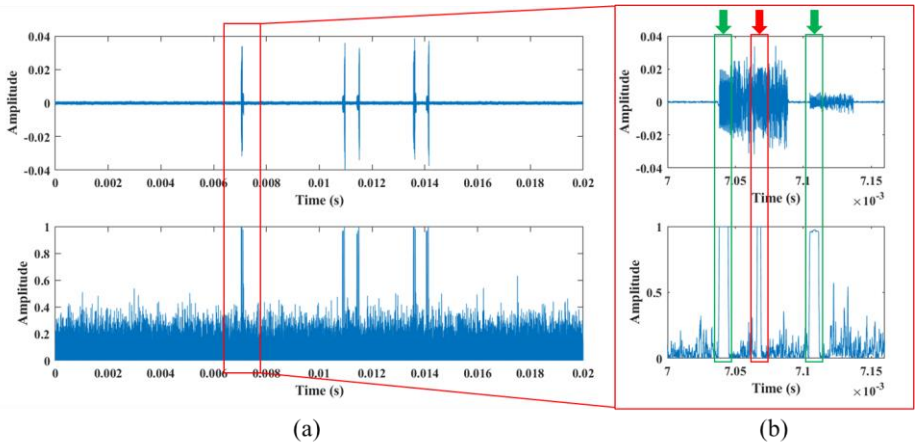

Fig. 10. Selected part of raw captured signal (upper subfigure) and corresponding WLAN packet detection decision static (lower subfigure). (a) General view of 0.02 second signal. (b) zoomed view of detection result.

The selected L-STF sequences are then transformed to its corresponding time-frequency graphs using the CWT algorithm provided by MATLAB wavelet toolbox, the process is shown in Fig. 11.

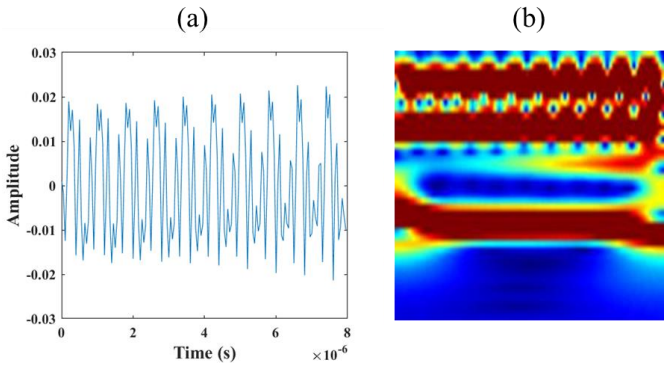

Fig. 11. Selected L-STF signal (a) and its CWT result (b).

After all signals from all five cellphone are processed with the above methods. A CNN classifier is trained with these images. The information of this image set is given in table 2.

Table 2 Number of images in the dataset used to train CNN

Device	Training set	Validation set	Total
IP_w	273	68	341
IP_b	197	49	246
RM_bl	137	34	171
RM_w	98	24	122
HN_bl	204	51	255

A pretrained GoogLeNet is utilized for the transfer learning process. The accuracy and loss information is shown in Fig. 12.

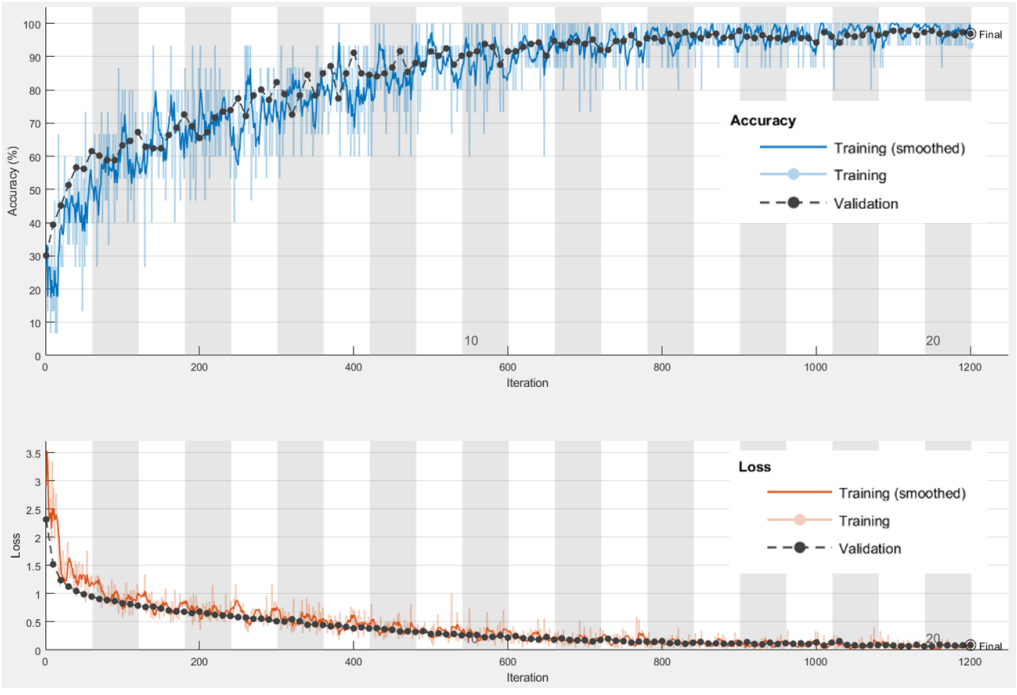

Fig. 12. The accuracy-iteration graph (upper) and training loss information (lower) of the transfer learning process.

Since the training set used in this thesis is relatively small for a CNN, it is important to evaluate whether this network has overfitted during training. Overfitting describes a scenario where the neural network simply memorizes the training set rather that learn its features. This will cause a performance decrease when classifying validation data. Shown in Fig. 12, during

the training process, the validation accuracy is close to the training accuracy, also, the validation loss is decreasing with training loss and both are approximating zero. Judging from these aspects, the CNN trained in this thesis is not overfitted.

In this thesis, we consider the trained CNN classifier as the target RFF database. Next, the device identification process is presented with a GUI demo given in Fig. 13. This GUI is packaged with MATLAB compiler (MATLAB coder is not used because the CWT algorithm can't be converted to C code due to copyright issues).

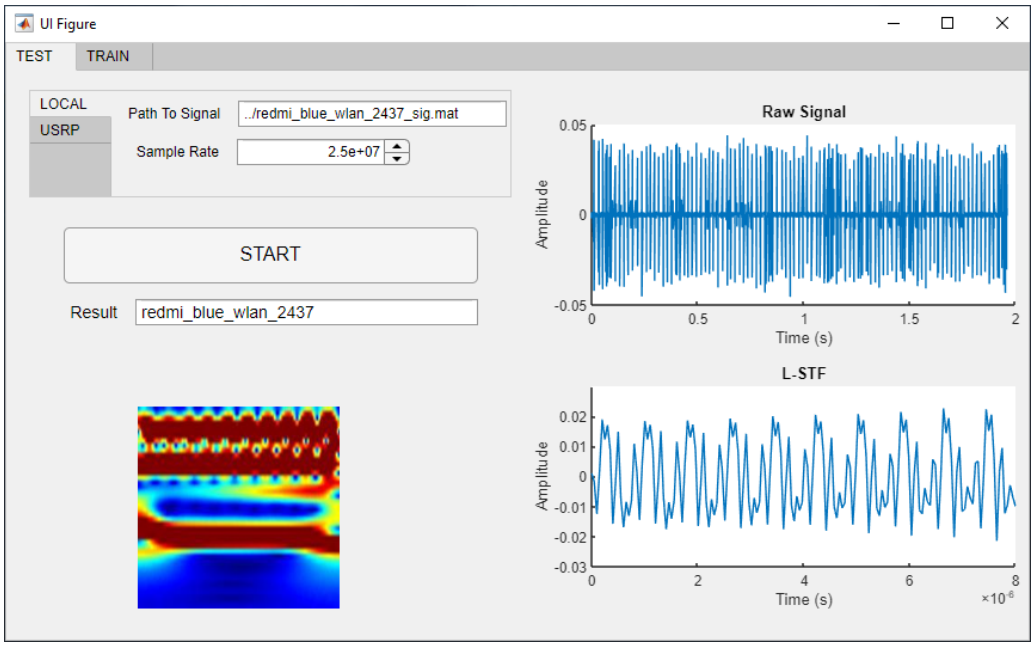

Fig. 13. GUI of RFF device identification system.

While testing the device identification system, a pre-recorded signal is loaded from the file system, which is different from the signal used during training. Following the identical process of database training, the CWT results of L-STF sequences in this signal are calculated. Finally, these results are all labeled by the trained CNN classifier, and the majority label is selected as the device RFF identity. We tested this system on 10 different signals captured from these five cellphones two weeks after training. All cases are successfully identified.

Experience

In this report, the theoretical analysis of the generation of radio fingerprint is conducted. A novel radio frequency fingerprinting system is then designed and evaluated. The proposed RFF system is implemented on a USRP 2922 platform. The feasibility of the proposed system is tested on a dataset of 1134 time-frequency images collected from five cellphones. It is proven by the testing that the designed RFF system can achieve a classification accuracy of over 96%, which is among the best tier of RFF systems. The system is proposed and evaluated based on WLAN signal, but the idea can be generalized to most modern communication networks

Score	