RADIO FINGERPRINTING

By

MAJ HASSAN MOHIUDIN

CAPT ADEEM UL WAQAR

CAPT MUHAMMAD KALEEM

CAPT FAISAL RAHIM QASURIA

Project Supervisor

LT COL DR. TAUQEER AHMED, TI(M)

Submitted to the Faculty of Electrical Engineering Department, Military College of Signals, National University of Science and Technology Islamabad in partial fulfillment for the requirements of a B.E. Degree in Telecom Engineering

MAY 2019

ABSTRACT

Radio Fingerprinting is very vast and diverse concept and it can be applied using one of the different methods. Because of Communication Security and Intelligence gathering, it has become more popular. In the Present communication scenarios, the voice / data is highly secured because of complex encryption algorithms. However we can detect the transmitters using their electronic signature known as Radio Fingerprinting. We took different type of transmitters operating in different modes and extracted phase information of the radio signals, recorded in Intermediate Frequency (IF). It was the Steady State Analysis using the available Matlab tools to discriminate different set of emitters. Using the pattern with which phase is changing, we were able to distinguish the given set of transmitters with good accuracy. However signal data library development and more can be achieved in future.

Declaration

No portion of the work presented in this dissertation has been submitted in support of any other award or qualification either to this institution or elsewhere.

CERTIFICATE FOR CORRECTNESS AND APPROVAL

It is hereby certified that the form of the report and the contents of the project "**Radio Fingerprinting**" being submitted by the syndicate of students

1. Maj Hassan Mohiduin
2. Capt Adeem Ul Waqar
3. Capt Muhammad Kaleem
4. Capt Faisal Rahim Qasuria

Have been written well and found satisfactory as per the requirements of the B.E. Degree in Electrical (Telecom) Engineering.

APPROVED BY

_____

Lt Col Dr. Tauqeer Ahmed, TI (M)

Electrical Engineering Department

Military College of Signals (NUST)

DATED: ____ May 2019

DEDICATION

Almighty Allah,

Family, relatives and friends for their support

And faculty for their help.

Acknowledgments

We thank Allah Almighty for bestowing his countless blessing upon us without which nothing could have been achieved.

We are also most thankful and grateful to our parents especially our mothers who bore with us in times of difficulty and hardships and were such a support. Without their consistent support and encouragement, we would never have achieved the targets successfully.

We would like to specially thank **Col Dr. Adil Masood Siddiqui, HOD (EE)** for his keen interest in our project and providing us with help in terms of technical knowledge and insight whenever we needed to successfully complete the project. He was always kind and present to solve the little problems that we encountered.

We would like to specially thank our supervisor **Lt Col Dr. Tauqeer Ahmed** for his admirable support, guidance, motivation and critical reviews throughout the course of our project. We would also like to thank the faculty for being there for us whenever we needed help of any kind.

Table of Contents

List of Figures

Abbreviations

ELINT：Electronic Intelligence

VHF: Very High Frequency

AM: Amplitude Modulation

FM: Frequency Modulation

PM: Phase Modulation

ASK: Amplitude Shift Keying

FSK: Frequency Shift Keying

PSK: Phase Shift Keying

FFT: Fast Fourier Transform

IF: Intermediate Frequency

SEI: Special Emitter Identification

CHAPTER: 1

INTRODUCTION

1.1 Problem Statement

Identification of wireless devices in general and tactical radio sets in the particular based on the non-idealities either developed because of the hardware imperfections or due to the software radio waveform.

1.2 Project Overview

Radio Fingerprinting pertains to the field of electronic warfare. In the Present communication scenarios, the voice / data is highly secured because of complex encryption algorithm. This make enemy movements and plans maneuver more secure. However, there is still a room where we can detect the movement of a particular formation by knowing the electronic signature of the devices used by the particular formation, known as radio fingerprinting. The basic concept pertains to exploiting the minor imperfections like filters, amplifiers, changes in the transmitters, I/Q imbalances etc which in turn will affect the signal generated by the devices and distinguishing the emitters through the analysis of these signals. Various methods have been followed by many researchers e.g. the Steady State Analysis or Transient State Analysis which are the popular one. We extracted the phase information of the signal in frequency domain analysis.

The project deals with extracting features of IF recorded signal using Matlab tools and then discriminating the signal using key features. Many samples of the signals from different radio sets are recorded after down converting them. We then defined various parameters in the phase of the signal which stand out in a specific radio signals set and thus distinguishing it from others.

After doing the study on 5 radio sets we then proposed the results, limitations and future

plans.

CHAPTER: 2
Fundamentals of Radio Signal

2.1 Modulation Techniques

Modulation is a type of process used to change the properties of a periodic signal which is known as carrier signal with a modulating signal that normally contains data to be transferred. Modulation can be analog as used in earlier days or digital modulation techniques more common nowadays.

2.1.1 **Analog Modulation**

Analog modulation refers to the process of transferring analog low frequency baseband signal, like an audio or TV signal over a higher frequency carrier signal such as a radio frequency band. Baseband signal is always analog for this modulation. Three type of analog modulation were used. Details of which are as follow: -

2.1.1.1 ***Amplitude Modulation***

Amplitude modulation or AM is the process of varying the instantaneous amplitude of carrier signal accordingly with instantaneous amplitude of message signal. Let m(t) be the message signal and a carrier signal with frequency f_c is used for modulation. S (t) would be the modulated signal. The modulated signal will take the form as given in

Eq (2.1.1)

$$s(t) = m(t)\cos(2\pi f_c t) \qquad (2.1.1)$$

Lets see the same equation in frequency domain.

$$m(t)\cos(2\pi f_c t) \overset{F}{\Leftrightarrow} \frac{1}{2}[M(f + f_c) + M(f - f_c)] \qquad (2.1.2)$$

Original message signal will shift right by f_c in frequency domain. We use Matlab to show the amplitude modulated signal in both time and frequency domain.

Message signal frequency= 20 Hz

Carrier signal frequency = 200 Hz

Sampling frequency= 1000 Hz

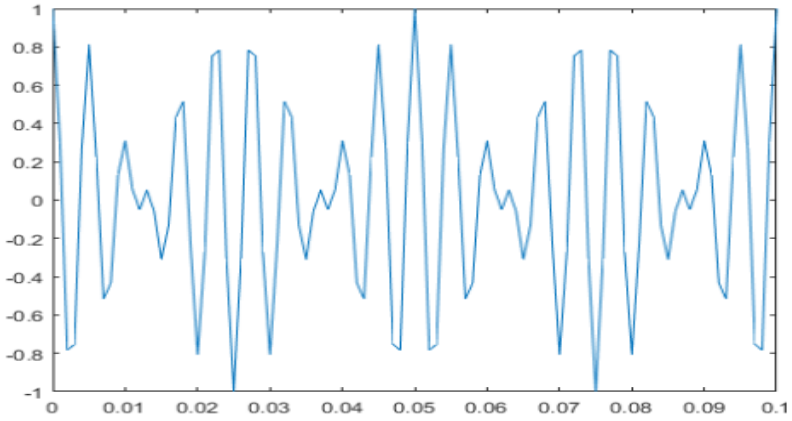

Figure 2.1.1.1 (a) Amplitude Modulated Signal in Time Domain

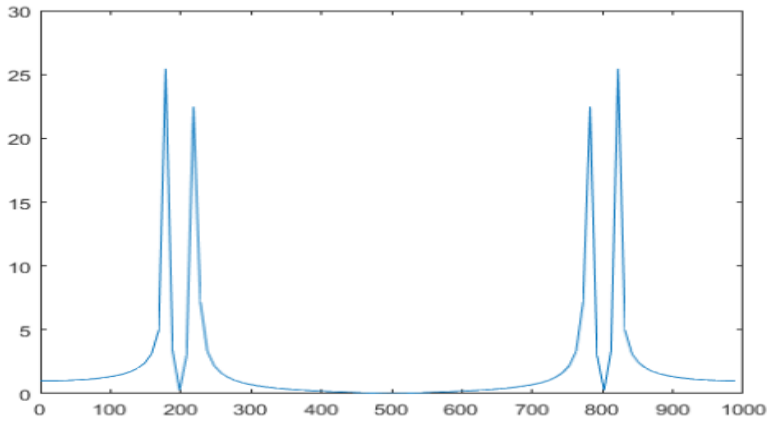

Figure 2.1.1.1 (b) Amplitude Modulated Signal in Frequency Domain

Matlab code as per **Appendix D**.

2.1.1.2 ***Frequency Modulation***

FM or Frequency modulation is the process of varying the instantaneous frequency of carrier signal accordingly with instantaneous amplitude of message signal. Let m(t) be the message signal and s(t) is fm modulated signal then fm modulation is represented as under in Eq (21.3) and Eq (2.1.4)

$$a(t) = \int_{-\infty}^{t} m(\alpha) d\alpha \qquad (2.1.3)$$

$$s(t) \approx A[\cos(\omega_c t - k_f a(t)\sin \omega_c t] \qquad (2.1.4)$$

Where k_f is the modulating index.

Matlab representation in both time and frequency domain of the modulated signal is as under: -

Frequency of message signal is 70 Hz and f_c is 200 Hz.

Sampling frequency is 1000 Hz.

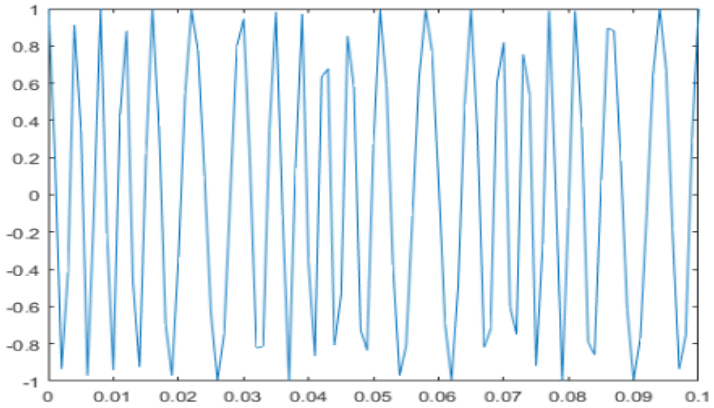

Figure 2.1.1.2 (a) Frequency Modulated Signal in Time Domain

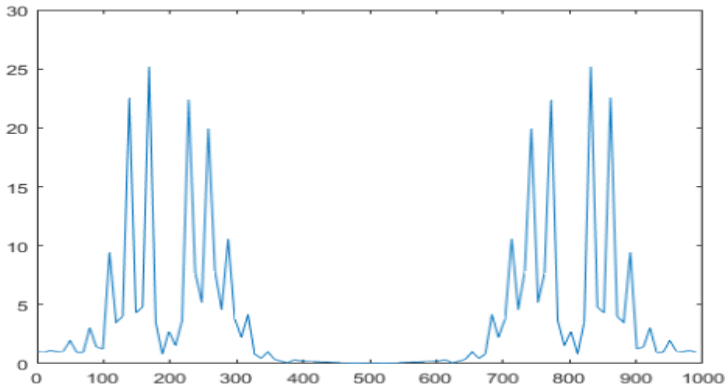

Figure 2.1.1.2 (b) Frequency Modulated Signal in Frequency Domain

Matlab code as per **Appendix E**.

2.1.1.3 ***Phase Modulation***

PM or Phase modulation is the process of varying the instantaneous phase of carrier signal accordingly with instantaneous amplitude of message signal. Let m(t) be the message signal and s(t) be the modulated signal. Then we can represent the phase modulation as under: -

$$s(t) = Acos[\omega_c t + k_p m(t)] \qquad (2.1.5)$$

Where k_p is the modulating index.

In Matlab we have shown the modulated signal in both time and frequency domain. Frequency of m(t) is 50 Hz, carrier signal frequency is 200 Hz and sampling frequency is 1000 Hz.

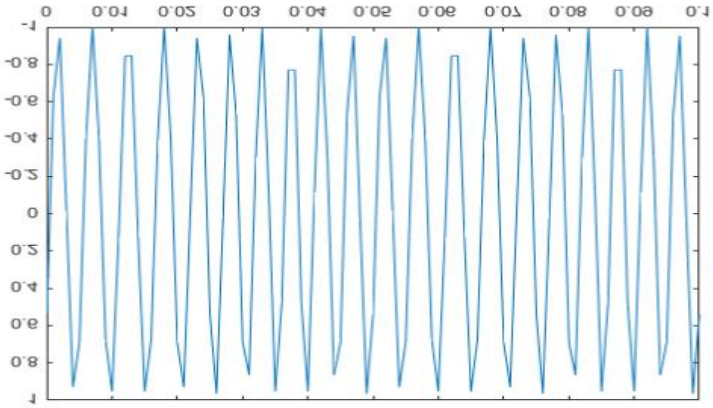

Figure 2.1.1.3 (a) Frequency Modulated Signal in Time Domain

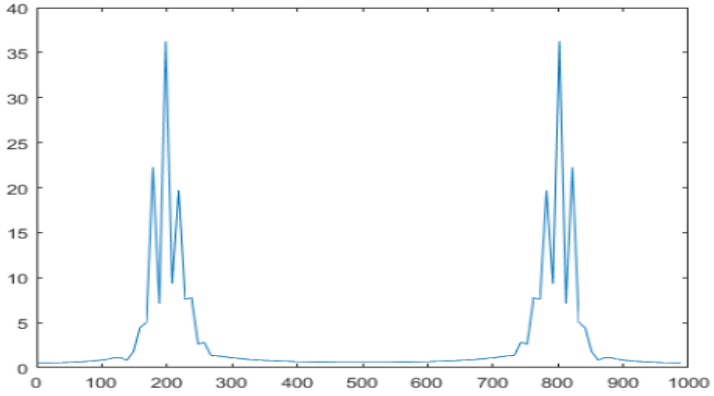

Figure 2.1.1.3 (b) Frequency Modulated Signal in Time Domain

Matlab code as per **Appendix F**.

2.1.2 Digital Modulation

Digital modulation follows similar way of modulations except of the fact that it has digital baseband signal which was analog in analog modulations. Basic three types of digital modulation are as follow: -

2.1.2.1 *ASK Modulation*

When carrier signal's amplitude is varied in accordance to input bit or symbol its called ASK modulation. For example, if a bit 1 is represented by amplitude 10 and bit 0 with amplitude 5 then its analytical expression is as follow: -

$$s(t) = \sqrt{\frac{2E_i}{T}} \cos(\omega_o t + \emptyset) \qquad (2.1.6)$$

$i = 1,2, \ldots, M$ Where there is M-array Ask

Let's have a carrier signal with bit period of 1µs and frequency ten times of the bitrate. Sampling frequency would be bp/100. We will see Matlab code on how to modulate digital sequence in both time and frequency domain (as per **Appendix A**).

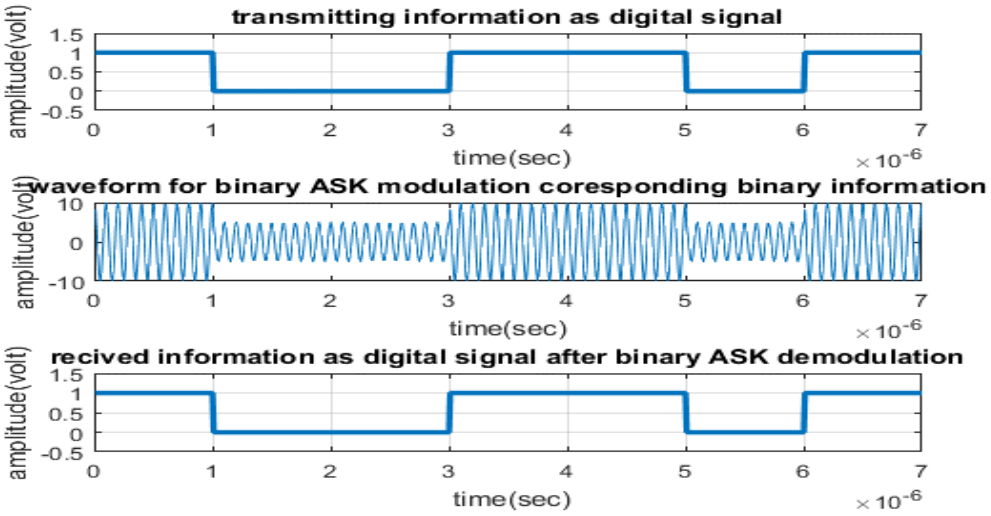

Figure 2.1.2.1 (a) ASK Modulation

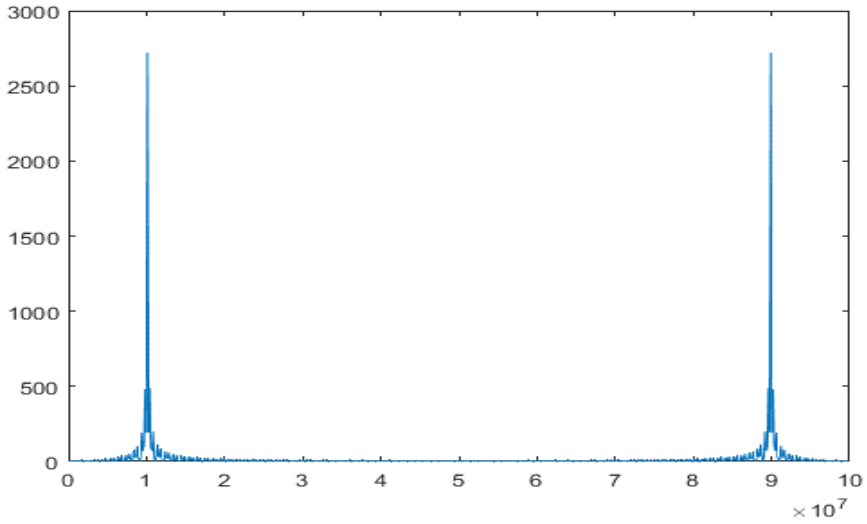

Figure 2.1.2.1 (b) ASK Modulation

2.1.2.2 ***FSK Modulation***

When carrier signal's frequency is varied in accordance to input bit or symbol it is FSK modulation. For example, if a bit 1 corresponds to 8000000 Hz of carrier and bit 0 corresponds to 2000000 Hz of carrier then its analytical expression is as under: -

$$s(t) = \sqrt{\frac{2E}{T}} \cos(\omega_i t + \emptyset) \qquad (2.1.7)$$

$i = 1,2, \dots, M$ Where there is M-array FSK

Let's have a carrier signal with bit period of 1μs and frequency for bit value 1 is br*8 = 8000000 Hz and for bit value zero is br*2 = 2000000 Hz bitrate. Sampling frequency would be bp/100. We will see Matlab code on how to modulate digital sequence in both time and frequency domain (as per **Appendix B**).

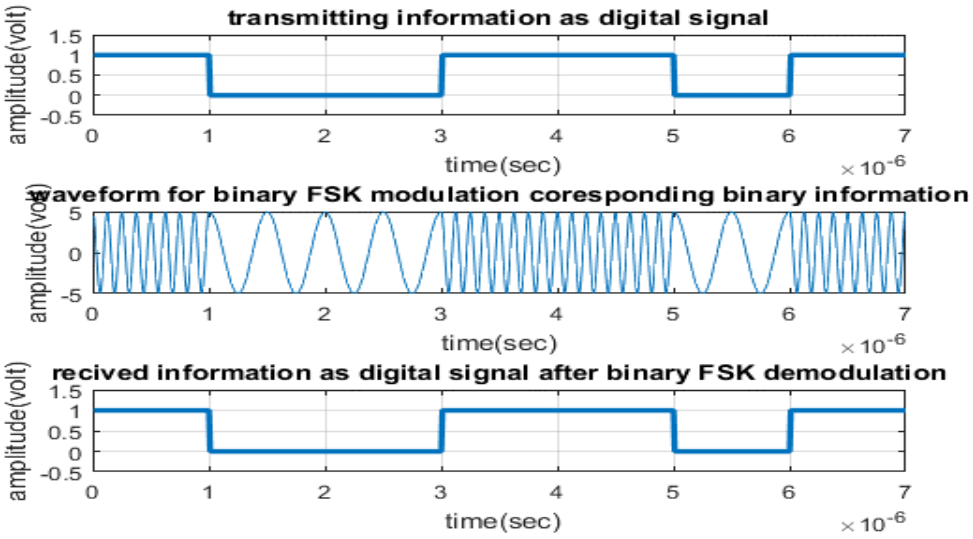

Figure 2.1.2.2 (a) FSK Modulation

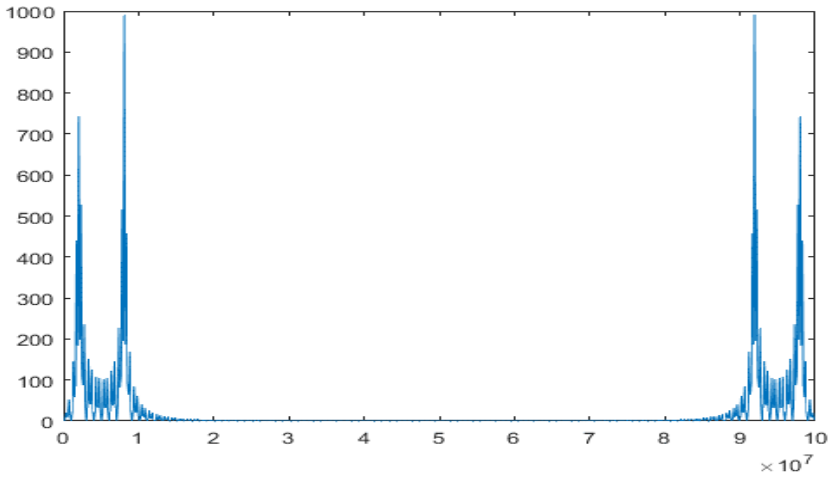

Figure 2.1.2.2 (b) FSK Modulation

2.1.2.3 ***PSK Modulation***

When carrier signal's phase is varied in accordance to input bit or symbol it is PSK modulation. For example, when a bit is 1 its phase is is zero and when bit is 0 then carrier has a phase shift of 180. Its analytical expression is as under: -

$$s(t) = \sqrt{\frac{2E}{T}} \cos(\omega_o t + 2\pi i/M) \qquad (2.1.8)$$

$i = 1,2, \ldots, M$ where there is M-array PSK

Let's have a carrier signal with bit period of 1μs and frequency double of the bitrate. Sampling frequency would be bp/100. We will see Matlab code on how to modulate digital sequence in both time and frequency domain (as per **Appendix C**).

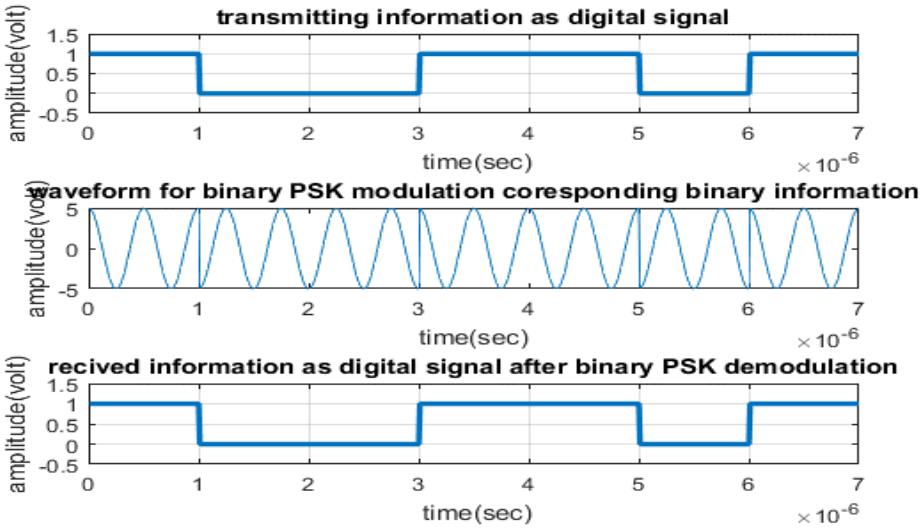

Figure 2.1.2.3 (a) PSK Modulation

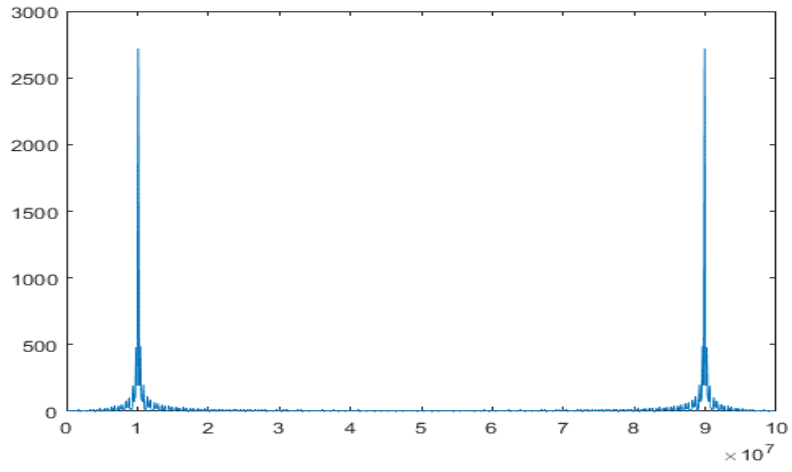

Figure 2.1.2.3 (b) PSK Modulation

2.2 Fourier Transform of a Signal

Fourier series was introduced in 1807 by a French engineer, Jean Baptiste Joseph de Fourier (1768-1830). He suggested that any arbitrary function defined over a finite interval by any piecewise graph, continuous or discontinuous, could be represented as an infinite sum of continuous functions such as sine and cosine.

Although almost all the members of the French Academy questioned its validity, it turned out to be one of the most powerful tools in signal processing. The basic concept of the Fourier transform is that any function in the time domain can be represented by an infinite number of sinusoidal functions. The Fourier transform is defined as, "A function *x(t)* in the time domain *t* has a corresponding function *X(f)* in the frequency domain". related by Eq (2.2.1)

$$\mathcal{F}[x(t)] \equiv X(f) = \int_{-\infty}^{\infty} x(t)e^{-j2\pi ft}dt \qquad (2.2.1)$$

Now a days in digital world we use different algorithms for discrete time Fourier transform. Fast Fourier transform is one of the most popular method. In Matlab we use FFT for analysing signal in frequency domain. In the diagram below is a synthetic signal in time domain and in frequency domain after applying FFT to it. Matlab code is as under: -

```
%synthetic signal used only
clear all
fs=50;      %must always greater the double of highest signal
freq NYquest
t=0:1/fs:1;
y=cos(2*pi*12*t)/2+cos(2*pi*18*t)/2;  %random received signal
synthetic
plot(t,y);        %time domain plot
```

```
%freq domain not centralized
x=fft(y);
f=(0:length(y)-1)*fs/length(y);
figure;
plot(f,abs(x));
figure;
plot(f,unwrap(angle(x)))
```

Here we have a y signal with two frequency components that is 12 Hz and 18 Hz which are sampled with sampling frequency of 50 Hz. Clearly the frequency domain signal highlights the frequency components clearly which can be difficult to visualize is time domain.

2.3 Time domain signal

Below is the figure which represent signal in a time domain

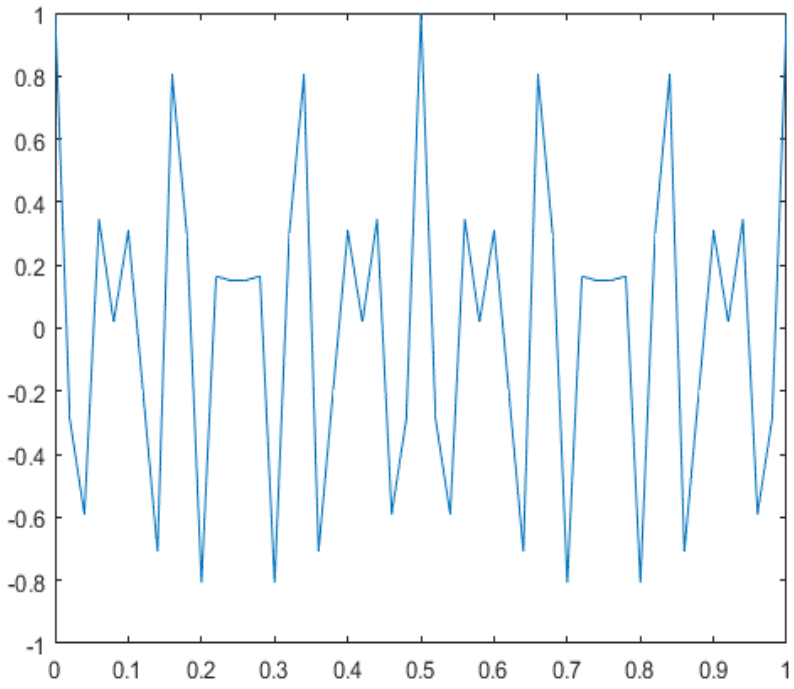

Figure 2.3 Time Domain Representation of a Signal

2.4 Magnitude Representation of Frequency Domain

Figure below clearly give us the magnitude peaks at 12 Hz and 18 Hz. So most of the signal resides in these two frequencies.

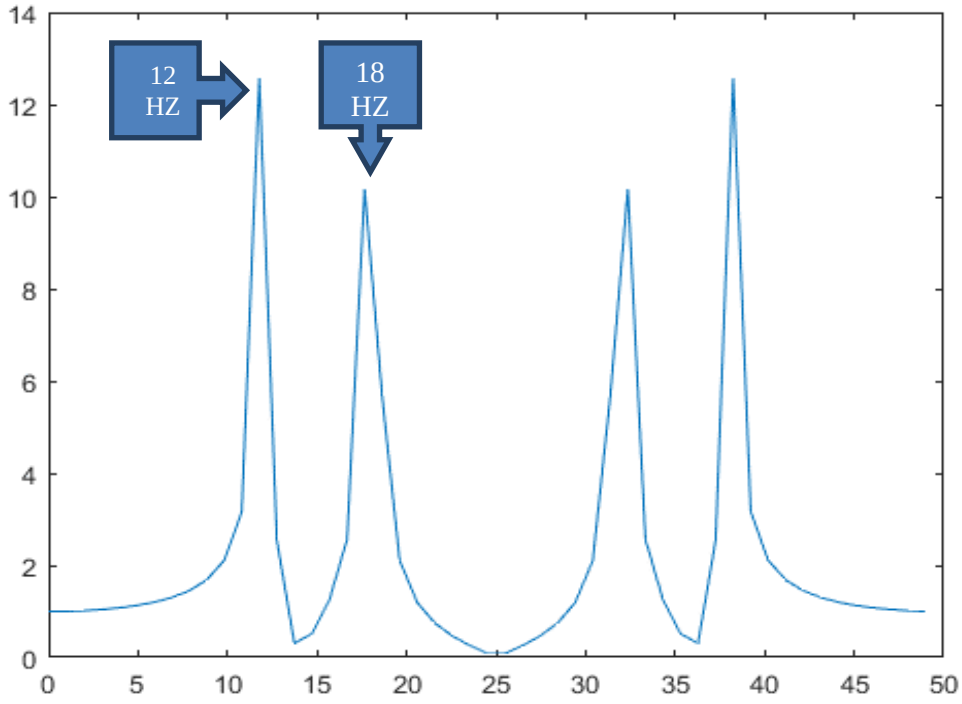

Figure 2.4 Magnitude Representation of Frequency Domain

2.5 Phase Representation of Frequency Domain

Below is the unwrapped phase of the frequency domain which tells us how phase is changing.

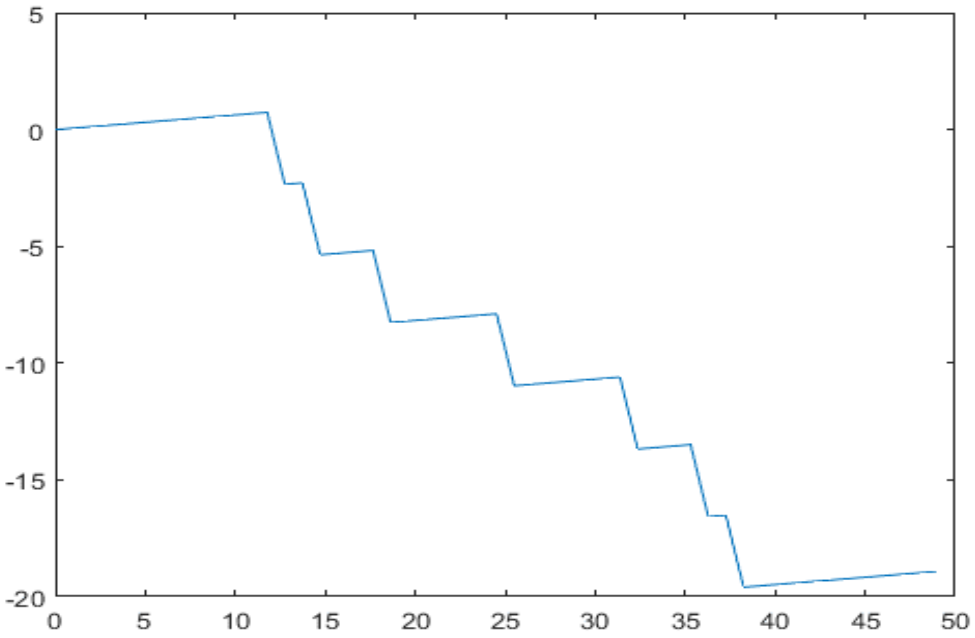

Figure 2.5 Phase Representation of Frequency Domain

CHAPTER: 3
LITERATURE REVIEW

In literature review we will discuss the motivation behind the concept of radio fingerprinting and the summary of the type of literature developed so far.

3.1 How the Research Work Started

This subject was not so popular until in mid of last decade when United States priority problem was the transmitter recognition and tracking for the purpose of security gathering and intelligence. United States wanted to recognize the enemy and friendly radars as well. Dedicated efforts started for the said purpose and now a large amount of research work is available using different methods on this subject.

The term used was the Specific Emitter Identification (SEI) by Northrop Grumman Mission system who developed the projects for US government. Over the span of next 40 years they applied the studies to the different type of transmitters in different systems operating in different frequency ranges.

Application of these projects reached out to the private set up as well after being popular in government and military. These techniques enabled the communication security for the telecommunication companies and were also applied to other cyber fields and networks. Some research work which can give insight on the subject [1,2,3,4].

3.2 Possible ways to approach the subject

In SEI systems the term identification was more complex and advanced then the recognition for the transmitters. Identification means to classify the emitters of same make and type while recognition means only to classify the type of transmitters.

Broadly, the specific emitter identification is divided into two categories. Details are as follow: -

3.2.1 Radar based SEI

In radar based identification some measured and derived parameters are of prime importance i.e. frequency, angle of arrival, pulse width, pulse repetition interval or PRI type.

3.2.2 Communication signal based SEI

Our area of interest is communication signal based radio finger printing. In this field work is broadly done in three possible ways i.e. Transient state analysis, Steady state analysis, Non linear techniques. Basic concept of digital communication and digital signal processing were understood well [5,6].

Time during which a radio ramps up the power and achieve a steady state is the transient state of radio, after that before the end it occupies the steady state. As illustrated in the figure below.

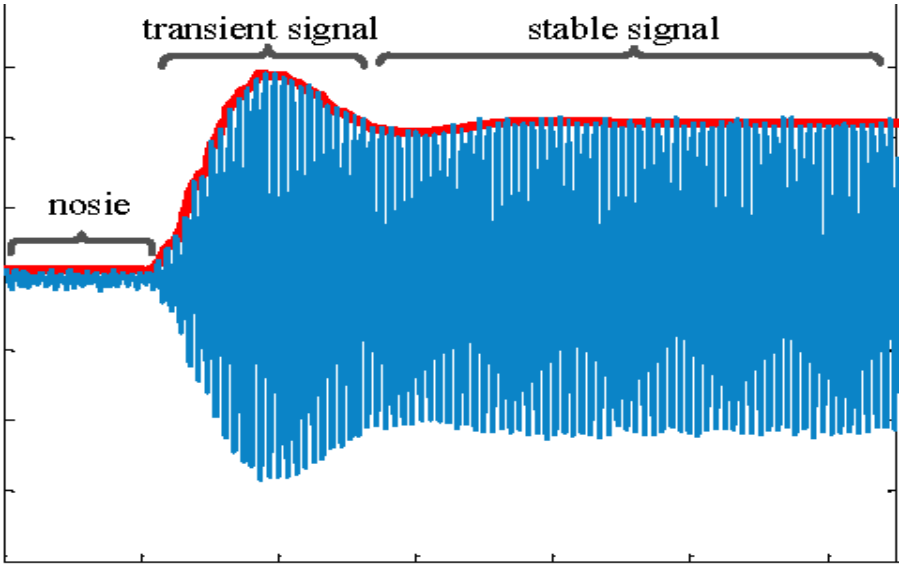

Figure 3.2.2 Communication signal based SEI

3.2.2.1 *Transient State Analysis*

Transient state analysis distinguishes the transmitters using the way radio behaves when it is turned on and at the end of the transmission. It is for very short duration i.e. in micro seconds, so to get the fingerprint we need very high sampling rate to get enough data. However the data is very small and analysis becomes more complex. Tools and receivers held with most of the researcher are not supportive of that much high sampling rates, thus this approach is much challenging.

For example Serinkin approach [7] used 5 Giga samples per second and Bayesian step change detector [8, 9] used the amplitude information in transient state. Hall also proposed the use of phase in the transient state [10,11] and used 500 mega samples per second. All of them used high SNR value to compute the results. Such high sampling rate cannot be processed in normal systems. Similarly much of work on transient state has been done but there is not enough data in that small duration thus can be challenging.

3.2.2.2 *Steady state Analysis*

Steady state analysis is not as complex as the transient state thus is more practical. Some waveform based techniques and modulation based techniques were used.

For example Brik [12] used modulation based techniques from steady state signals and Scalan used spectral averaging techniques in steady state [13]. But these methods were performed in anechoic chamber thus not in real conditions. Modulation based techniques contain more information than the waveform based, because it can exploit the modulation means of transmitters into the feature for fingerprinting.

3.2.2.3 *Non Linear techniques*

It is divided into two categories one is the based on nonlinear characteristic while one is based on non linear modeling.

- Nonlinear techniques such as non linearity of amplifiers and digital to analogue converter are being analyzed for fingerprinting. However it requires more data and time for reliable results.

  Carrol[14] used the nonlinearity of the amplifiers in his study and based on phase space analysis. While polak used the no linear modeling techniques by modeling the nonlinearities in digital to analog converter and amplifiers but for it to work the model should match with real signals and are more complex[15]. Similarly more work is done using nonlinear techniques. [16,17]

3.2.3 The Basic process for fingerprinting

- Accurately measuring the features which are consistent in all the transmissions of single transmitter and with that they must differ from all the transmissions of other transmitters.
- Keep on finding different transmitter's features and keep gathering them in a continuous process.
- Maintain a database for each emitter that comes in your area of interest after extraction of the features.
- Produce results, errors, correction and amount of accuracy.

CHAPTER: 4
METHODOLOGY

Our project is divided into two phases. In phase I we made synthetic signals, modulated them and then did signal detection. This helped us understand the way signal communication is carried out and how to approach the extraction of features from the modulated and down converted signal.

In phase II we recorded the real signals in a noisy environment. We used frequency domain approach and tried to extract the features that are important for the radio fingerprinting.

4.1 Phase I

Using Matlab tools we made different modulated signals and then we detected back the baseband signal. Then we analyzed the modulated signal in frequency domain.

4.1.1 Preparation of Synthetic Signal, PSK

A sequence of seven bits is being modulated using BPSK modulation. Each bit 0 or 1 is represented by a sinusoidal signal with the phase difference of 180°. Below is the Matlab code used for the modulation: -

4.1.1.1 *Code for displaying Binary Information*

```
x=[ 1 0 0 1 1 0 1];                                          %
BinaryInformation
bp=.000001;
bit=[];
for n=1:1:length(x)
    if x(n)==1;
       se=ones(1,100);
    else x(n)==0;
        se=zeros(1,100);
    end
     bit=[bit se];
end
```

```
t1=bp/100:bp/100:100*length(x)*(bp/100);
subplot(3,1,1);
plot(t1,bit,'lineWidth',2.5);grid on;
```

4.1.1.2 *Code for BPSK Modulation*

```
m=[];
for (i=1:1:length(x))
    if (x(i)==1)
        y=A*cos(2*pi*f*t2);
    else
        y=A*cos(2*pi*f*t2+pi);    %A*cos(2*pi*f*t+pi) means -
A*cos(2*pi*f*t)
    end
    m=[m y];
end
t3=bp/99:bp/99:bp*length(x);
subplot(3,1,2);
plot(t3,m);
```

4.1.2 Detection of Signals

Detection of signal is being done by integrating the sinusoidal signal over its time. If the signal has the magnitude greater then 1 then its mean phase was 0° otherwise 180°. Code is as below: -

```
mn=[];
for n=ss:ss:length(m)
  t=bp/99:bp/99:bp;
  y=cos(2*pi*f*t);                                    %
carrier siignal
  mm=y.*m((n-(ss-1)):n);
  t4=bp/99:bp/99:bp;
  z=trapz(t4,mm) ;
% intregation
```

```
  zz=round((2*z/bp));
  if(zz>0)                                          % logic
level = (A+A)/2=0
                          %becouse A*cos(2*pi*f*t+pi) means -
A*cos(2*pi*f*t)
    a=1;
  else
    a=0;
  end
  mn=[mn a];
end
disp(' Binary information at Reciver :');
disp(mn);
```

4.1.3 Extraction of Features

Input bit stream, the modulated signal and output bit bitstream after demodulation is as below:-

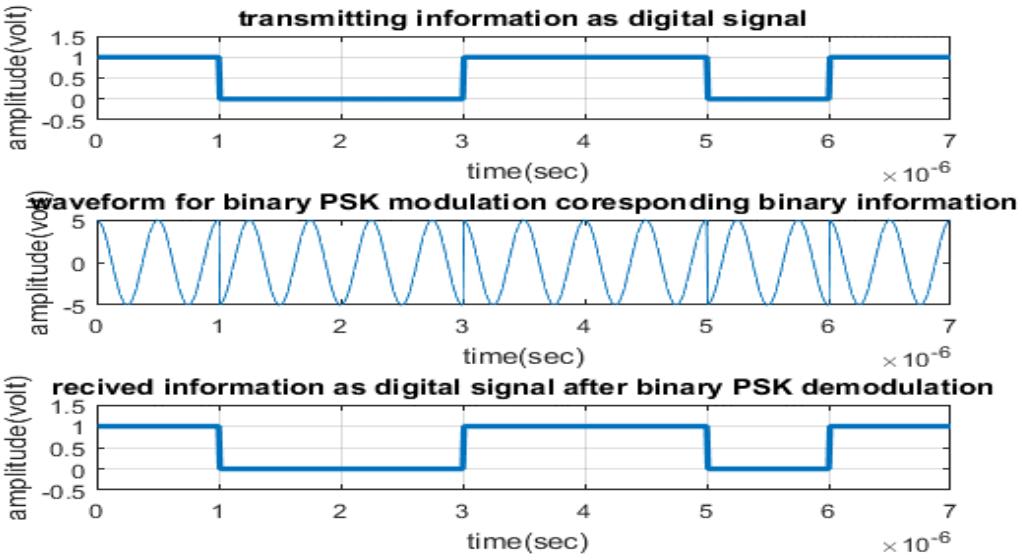

Figure 4.1.3 BPSK Modulation

Some important features of the signals are: -

Bit period (bp)= 1 microsecond
Bit rate (br)= 1/bp= 10^6

Type of modulation= BPSK
Number of samples per bit period= 100
Sampling frequency= bp/100
Carrier signal= cos(2*pi*f*t +phase)

4.2 Phase II

In phase II we got the recorded signals from different type of transmitters and played them in Matlab. Our aim was to find the features i.e. phase changing pattern, which can help us in the emitter recognition or possible SEI. Rest all operations for radio fingerprinting are being done in this phase. All Operations in the form of block diagram are given below.

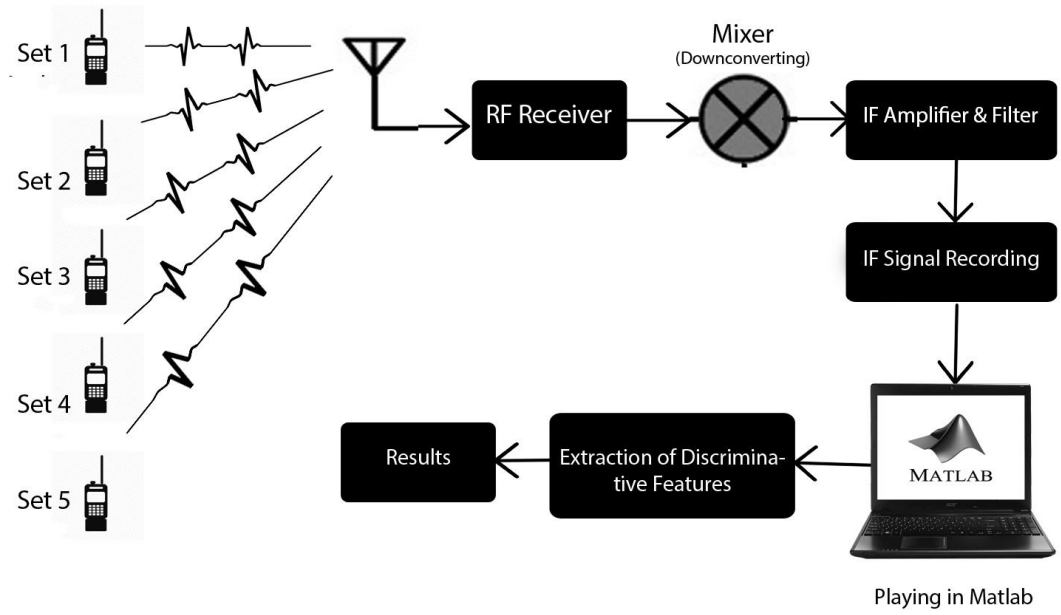

Figure 4.2 Phase II

4.2.1 Standard Receiver

We have gathered the different signals recorded in open environment. Signals are recorded after down converting the signals in advanced receiver. Details in the form of

standard receiver architecture are as shown in the diagram. The purpose of down converting is to translate the frequency of the signal so that it is compatible with the data collection system.

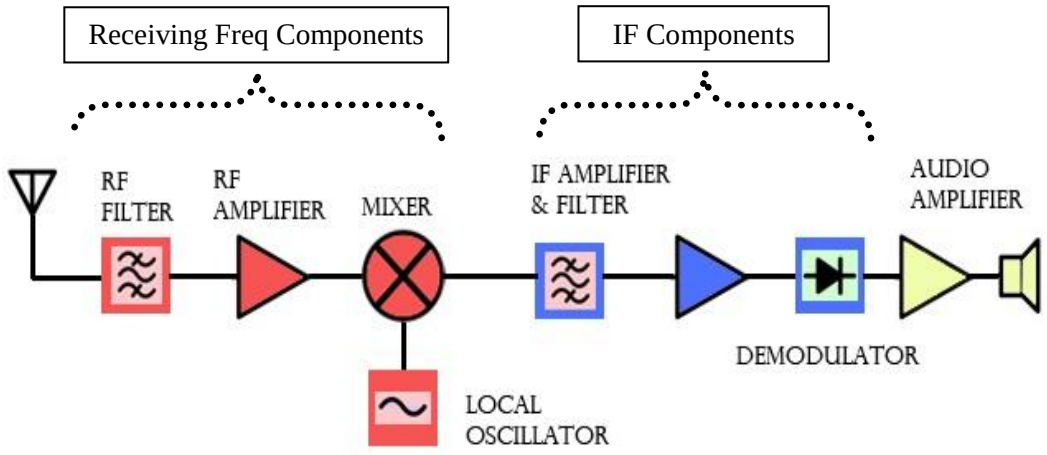

Figure 4.2.1 Standard Receiver

Signals were recorded in *.wave* file format. After recording was done the signals were played in Matlab and the key features were observed. We have recorded different set of signals from different type of transmitters.

4.2.2 Playing in Maltab

Using the Matlab tools we read the recorded signals from the *.wave* file. Then we extracted phase information from the recorded signals using Hilbert transform. We started analyzing the phase of signals and based on it, we started categorizing them.

4.2.3 Reading Signal and Extraction of Phase

First we read the signal in Matlab from the *.wav* recorded files of signal. After that we extracted phase of the signal using the Hilbert transform function.

After getting phase, the plot for phase zoomed is as below: -

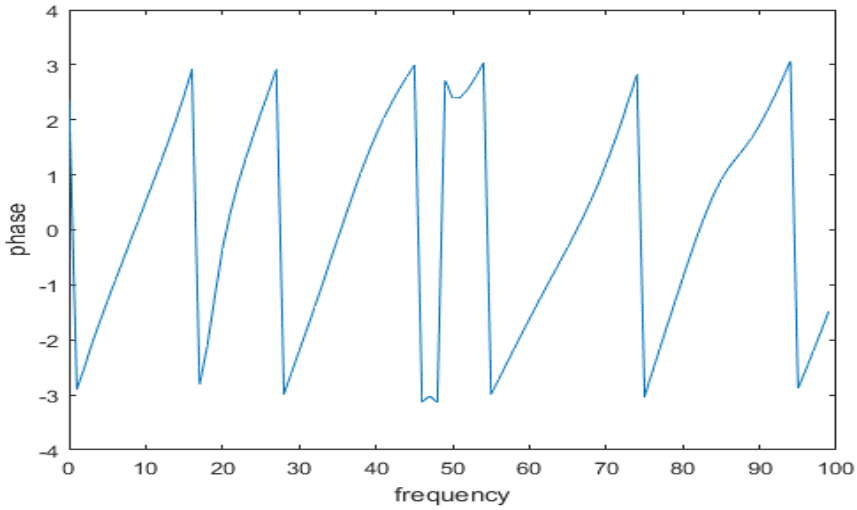

Figure 4.2.3 Reading Signal and Extraction of Phase

4.2.4 Finding Difference in Phase

After reading and extraction of phase of the recorded signal we found the difference in the phase information between two sample points. A vector has all difference values between two sample points throughout all samples.

After making a difference vector we defined a threshold value for the difference of phase. Then we found the indices of the vector have phase value above the threshold.

Now when we have a vector having the required indices, we have to find the difference of the indices, which will give us the intervals after which threshold value is achieved.

Figure below shows the indices having phase difference more than threshold.

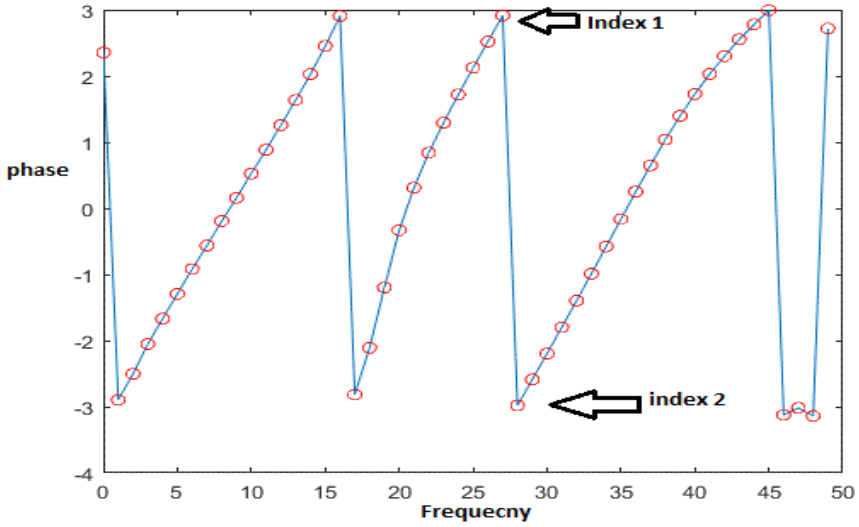

Figure 4.2.4 Finding Difference in Phase

4.2.5 Making Histogram

Now we made a bin range defined in a vector ranging from 9 to 48.

In this range we represented all the values of threshold difference vector in the form of a histogram.

Bar graph is shown below: -

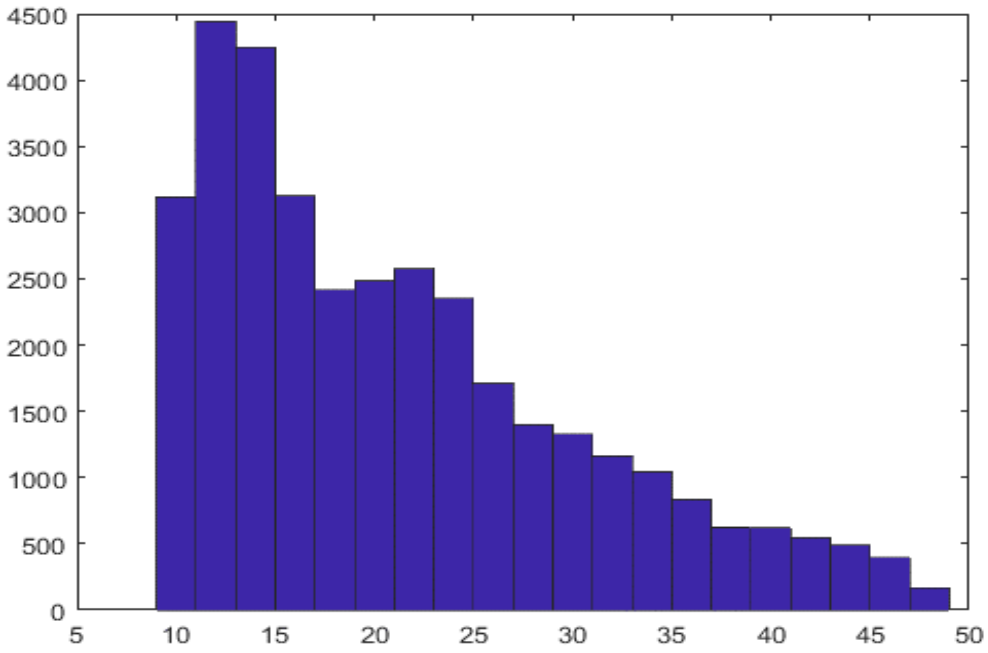

Figure 4.2.5 Making Histogram

Bar graph shows the number of phase shifts more then the threshold value after the difference of indices values.

4.2.6 Discriminating Transmitters

Based on the phase distribution on the difference values of indices we observed the patterns which are same in each signal of same radio and are different among other radios and developed the boundary between all the given set.

Based on the code explained we have developed the graphical user interface which will help us discriminate any signal from the five radio transmitters.

GUI has following buttons: -

(1) First button showing **"Enter a Signal"** will read a signal from our personal computer.

(2) **"Press to Discriminate"** will give us three answers i.e. 'Type of Radio',

‘Mode of Operation’ and ‘Threat Data Library’.

(3) **“Press for phase distribution”** button will show the bar graph for phase distribution.

(4) Press **“sound”** to play the signal sound.

(5) Press **“Stop”** to stop the signal.

The general appearance of the GUI is as shown below in fig 4.2.6

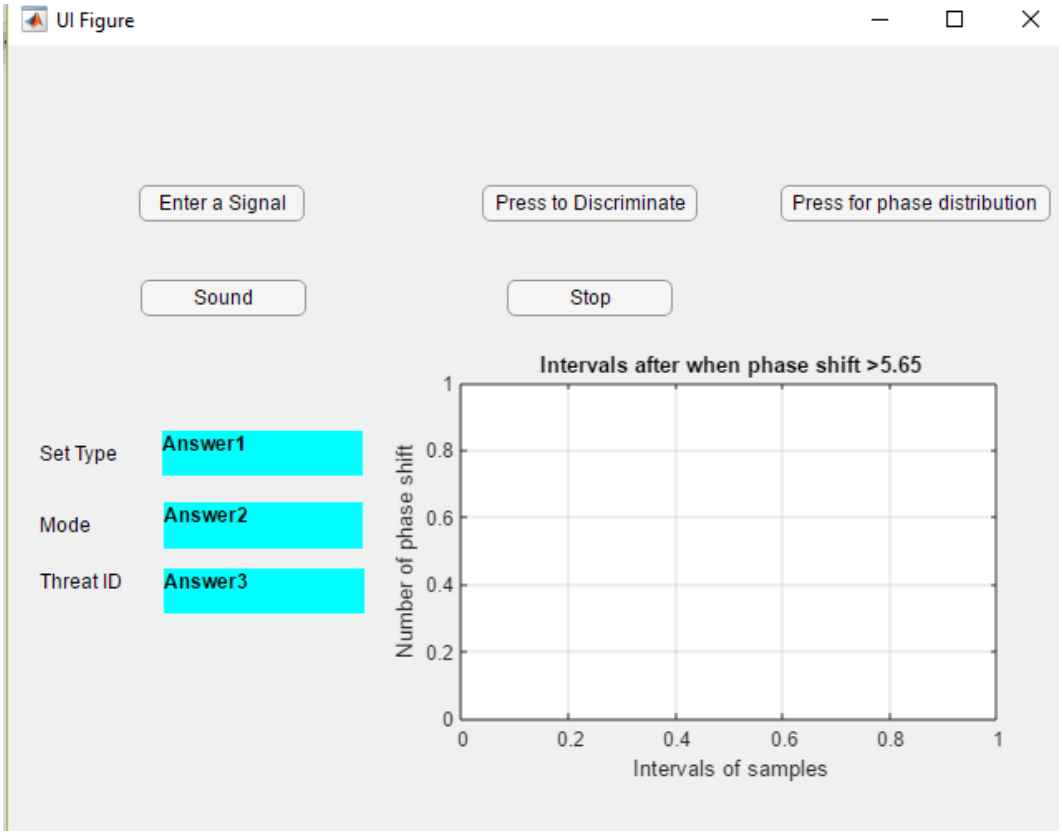

Figure 4.2.6 Discriminating Transmitters

CHAPTER: 5
RESULTS

We have analyzed signals from all five sets. The GUI will give us the required results. Our results were good with 95% accuracy and we were able to discriminate the signals from all 5 different type of radio sets. Results of phase distribution, radio type and its operation mode from all five sets are given below: -

5.1 Radio set 1

Figure given below gives us the results for radio set 1. It is giving us information on type of radio and phase distribution for the given signal and with this we gave the library ID 101 to radio set 1. Phase distribution is shown on bar only.

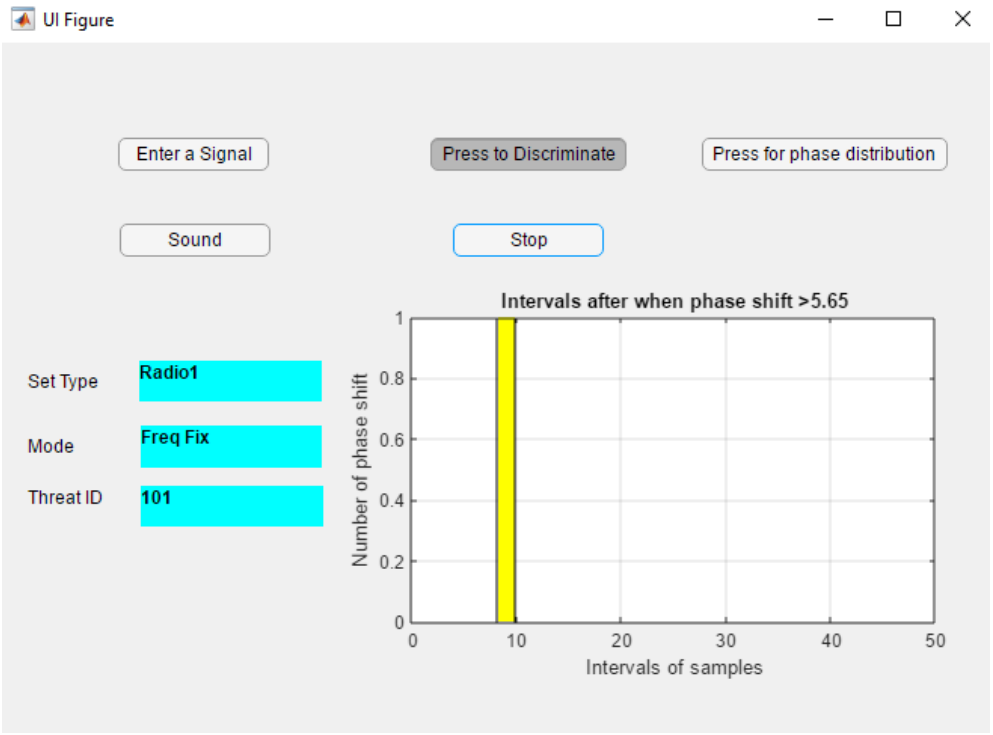

Figure 5.1 Radio Set 1

5.2 Radio set 2

Below figure gives us the details about radio set 2. Library ID for set 2 is 102 and phase distribution is much different then radio set 1 and others and has different pattern.

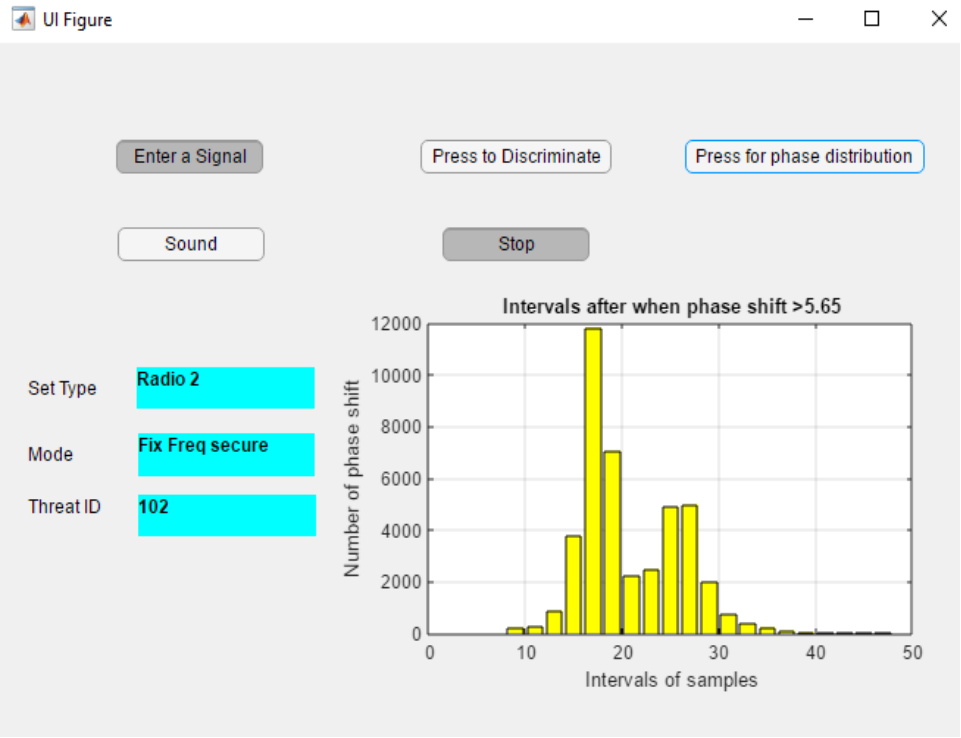

Figure 5.2 Radio Set 2

5.3 Radio set 3

Figure for the radio set 3 is different from the rest of figures. It tells us that the signal is from radio set 3 and its phase distribution.

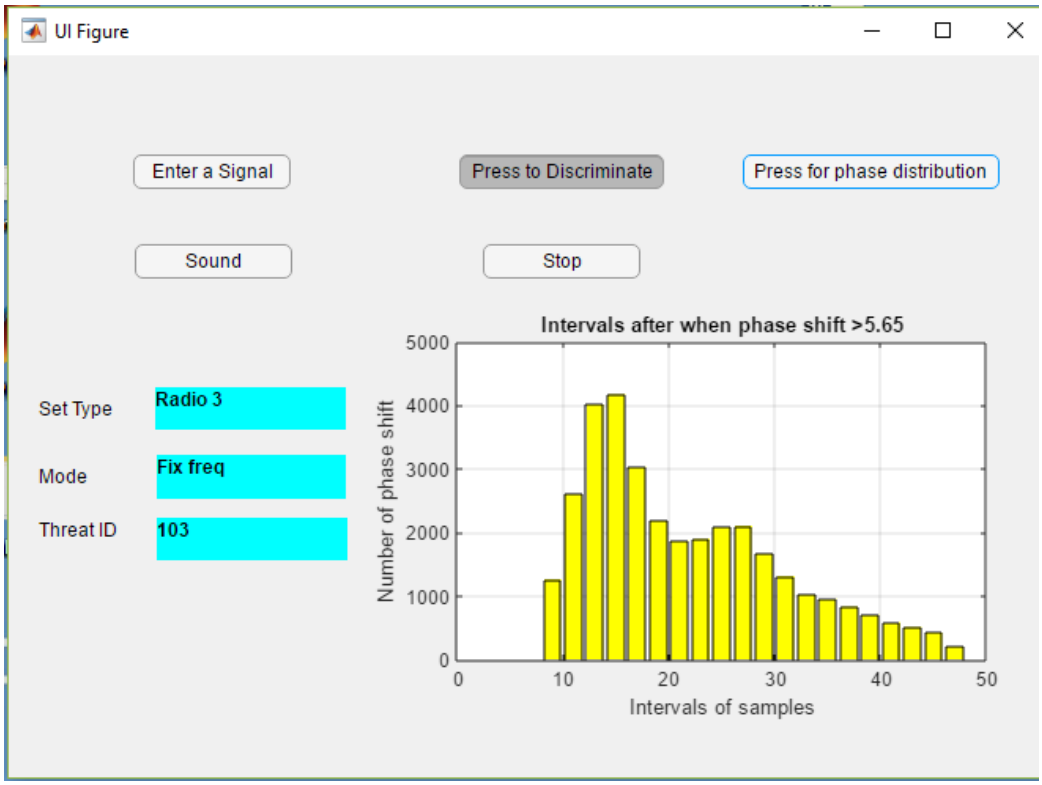

Figure 5.3 Radio Set 3

5.4 Radio set 4

Figure for the radio set 4 is different from the rest of figures. It tells us the signal is from the set 4 and its phase distribution. Its phase bars are in decreasing order and different from others.

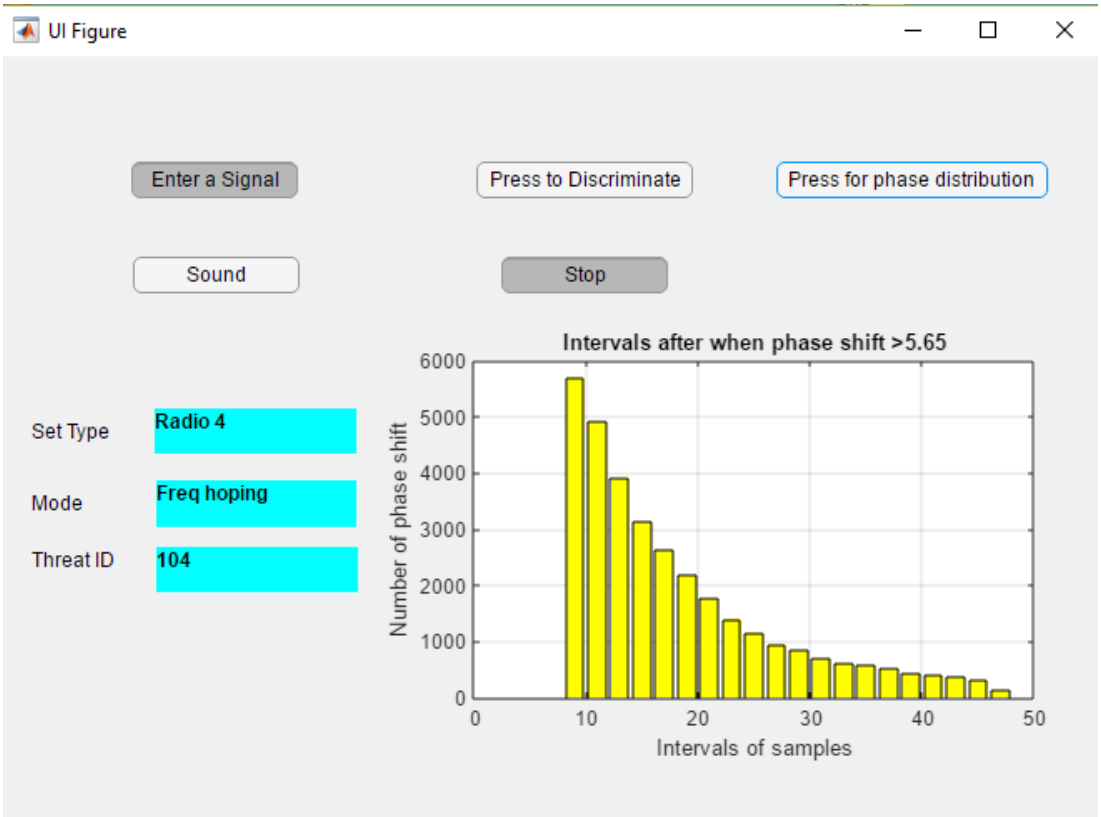

Figure 5.4 Radio Set 4

5.5 Radio set 5

Figure for the radio set 5 is different from the rest of figures. It tells us the signal is from the set 5 and its phase distribution is different from others as it has numerous small peaks with few larger peaks.

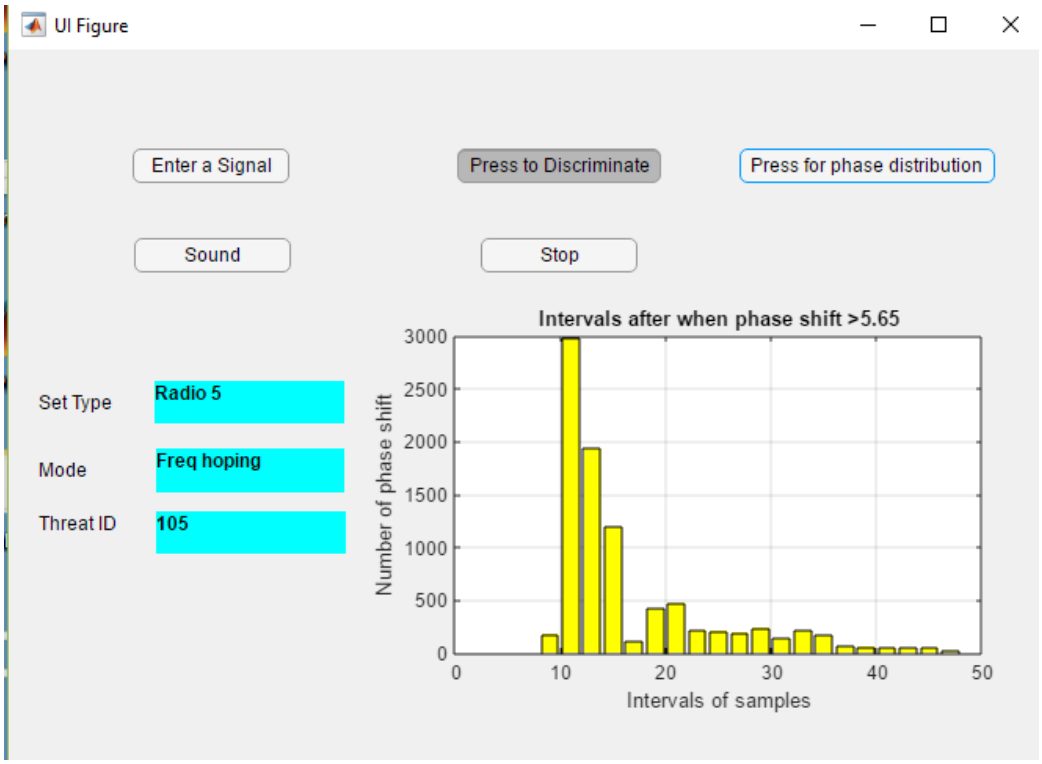

Figure 5.5 Radio Set 5

CHAPTER: 6
Future Plan

6.1 Future Recommendations

There is a vast domain of research in radio fingerprinting and much in future can be achieved. Some of works which can be carried forward are listed.

- Use the power spectrum information of the signals and based on that do the extraction of key features and distinguish the transmitters. Power spectrum information is very helpful both in transient state analysis and in the steady state analysis.
- Development of large data base with all the features extracted is a new task in itself. Work on the library development will help extend the project.
- When available with high sampling rate receivers and software tools, an effort can be made to extend this steady state analysis with a transient state analysis and extraction of features from both ways.
- Same work can also be performed by using same type of transmitters, operating in same mode and environment. Similarly by replacing the power source the transmitters have, we can also perform the fingerprinting as power source is often changed in transmitters.
- Scope of this project can be enhanced by using transmitters with different frequency range, we used communication radio transmitters in this project. We could use other electromagnetic emitters using different frequencies other than telecommunication frequencies.
- In furthering the analysis the pattern recognition algorithms can be applied to the extracted data and by using statistical study we can discriminate the emitters.

CHAPTER: 7
CONCLUSIONS AND REFRENCES

Conclusions

Radio Fingerprinting is the requirement of modern days, in government, private sectors or in military. With this work, foundation is laid to pave the way for area of research which has a good scope a head. We have achieved the following goals using the phase of the signal.

- We were able to understand on how to perform the reception of the signal, the down conversion and how to do IF recording. We recorded the modulated signal and then applied the Matlab tools available at our hands to get the job done.
- We were able to distinguish the given five transmitters of different types and operating in different modes based on phase changing patterns with 95% accuracy.
- We were able to propose the future work to extend the scope of project.
- We have started implementing the idea of data library but comprehensive development is required to be done in the future plans.
- With more stakeholders taking interest in this area, we are confident to see this research getting vast and much popular, as it requires more resources.

References

[1] Talbot, K., Duley, P., & Hyatt, M. (2003). Specific emitter identification and verification. Technology Review Journal, Spring/Summer, 113–133.

[2] Yonggiang Jia Shengli Zhu Lu Gan. Specific Emitter Identification Based on Natural Measure Published in Entropy 2017 DOI : 10.3390/E19030117.

[3] Dulek, B.; Ozdemir, O.; Varshney, P.K.; Su, W. Distributed maximum likelihood classification of linear modulations over nonidentical flat block-fading Gaussian channels. IEEE Trans. Wirel. Commun. **2015**, 14, 724–737.

[4] Suski, W.C., II; Temple, M.A.; Mendenhall, M.J.; Mills, R.F. Radio frequency fingerprinting commercial communication devices to enhance electronic security. Int. J. Electron. Secur. Digit. Forensics **2008**, 1, 301–322.

[5] B.P lathi, modern digital and analogue communication systems fourth edition.

[6] Oppenheim, Signal and systems second edition.

[7] K. Ellis and N. Serinken. Characteristics of radio transmitter fingerprints. Journal of Radio Science, pages 585–597, 2001.

[8] O. Ureten and N. Serinken. Bayesian detection of transmitter turn-on transients. Proceedings NSIP99, pages 830–834, 1999.

[9] O. Ureten and N. Serinken. Detections of radio transmitter turn-on transients. Electronic Letters, pages 1996–1997, 1999.

[10] J. Hall, J. Barbeau, and E. Kranakis. Detection of Transient in Radio Frequency Fingerprinting using Signal Phase. Proceedings Wireless and Optical Communications, 2003.]

[11] Jeyanthi Hall Detection of Transient in Radio Frequency Fingerprinting using signal Phase. Proceedings of IASTED International Conference on Wireless and Optical Communications (WOC), Banff, Alberta, 2003.

[12] Vladimir Brik Wireless device identification with radiometric signatures. Proceedings of the 14th ACM international conference on Mobile computing networking. Pages 116-127.

[13] Scanlon, P.; Kennedy, I.O.; Liu, Y. Feature extraction approaches to RF fingerprinting for device identification in femtocells. Bell Labs Tech. J. **2010**, 15, 141–151.

[14] Carroll, T. A nonlinear dynamics method for signal identification. Chaos Interdiscip. J. Nonlinear Sci. **2007**, 17, 023109.

[15] Polak, A.C.; Dolatshahi, S.; Goeckel, D.L. Identifying wireless users via transmitter imperfections. IEEE J. Sel. Areas Commun. **2011**, 29, 1469–1479.

[16] Huang, G.; Yuan, Y.; Wang, X.; Huang, Z. Specific Emitter Identification Based on Nonlinear Dynamical Characteristics. Can. J. Electr. Comput. Eng. **2016**, 39, 34–41.

[17] Zhang, J.; Wang, F.; Dobre, O.A.; Zhong, Z. Specific Emitter Identification via Hilbert-Huang Transform in Single-Hop and Relaying Scenarios. IEEE Trans. Inf. Forensics Secur. **2016**, 11, 1192–1205.

GLOSSARY

Appendix A

```
%>>>>>>>>> Amplitude modulation >>>>>>>%
clear all;
close all;
x=[ 1 0 0 1 1 0 1];                                    % Binary
Information
```

```
bp=.000001;                                                    %
bit period
disp(' Binary information at Trans mitter :');
disp(x);
%XX representation of transmitting binary information as digital
signal XXX
bit=[];
for n=1:1:length(x)
    if x(n)==1;
       se=ones(1,100);
    else x(n)==0;
        se=zeros(1,100);
    end
     bit=[bit se];
end
t1=bp/100:bp/100:100*length(x)*(bp/100);
subplot(3,1,1);
plot(t1,bit,'lineWidth',2.5);grid on;
axis([ 0 bp*length(x) -.5 1.5]);
ylabel('amplitude(volt)');
xlabel(' time(sec)');
title('transmitting information as digital signal');
%XXXXXXXXXXXXXXXXXXXXXXX B-ASK modulation
XXXXXXXXXXXXXXXXXXXXXXXXX%
A1=10;                          % Amplitude of carrier signal for
information 1
A2=5;                           % Amplitude of carrier signal for
information 0
br=1/bp;
% bit rate
f=br*10;                                                       %
carrier frequency
t2=bp/99:bp/99:bp;
ss=length(t2);
m=[];
for (i=1:1:length(x))
    if (x(i)==1)
        y=A1*cos(2*pi*f*t2);
    else
        y=A2*cos(2*pi*f*t2);
    end
    m=[m y];
end
t3=bp/99:bp/99:bp*length(x);
subplot(3,1,2);
plot(t3,m);
xlabel('time(sec)');
ylabel('amplitude(volt)');
title('waveform for B-ASK modulation coresponding binary
information');
%XXXXXXXXXXXXXXXXXXXX B-ASK demodulation
XXXXXXXXXXXXXXXXXXXXXXXXXXXX
```

```
mn=[];
for n=ss:ss:length(m)
  t=bp/99:bp/99:bp;
  y=cos(2*pi*f*t);                                          %
carrier siignal
  mm=y.*m((n-(ss-1)):n);
  t4=bp/99:bp/99:bp;
  z=trapz(t4,mm)                                             %
intregation
  zz=round((2*z/bp))
  if(zz>7.5)                                    % logic level =
(A1+A2)/2=7.5
    a=1;
  else
    a=0;
  end
  mn=[mn a];
end
disp(' Binary information at Reciver :');
disp(mn);
%XXXXX Representation of binary information as digital signal
which achived
%after ASK demodulation
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
bit=[];
for n=1:length(mn);
    if mn(n)==1;
       se=ones(1,100);
    else mn(n)==0;
        se=zeros(1,100);
    end
     bit=[bit se];
end
t4=bp/100:bp/100:100*length(mn)*(bp/100);
subplot(3,1,3)
plot(t4,bit,'LineWidth',2.5);grid on;
axis([ 0 bp*length(mn) -.5 1.5]);
ylabel('amplitude(volt)');
xlabel(' time(sec)');
title('recived information as digital signal after binary ASK
demodulation');
%>>>>>>>>>>>>>>>>>>>>>>>>>>> fft >>>>>>>>>>>>>>>>>>>>>>>>>>>>>>%
m1=fft(m);
f=(0:length(m)-1)*br*100/length(m);
figure;
plot(f,abs(m1));
```

Appendix B

```
%B-PSK modulation
clc;
```

```
clear all;
close all;
x=[ 1 0 0 1 1 0 1];                                          % Binary
Information
bp=.000001;                                                          %
bit period
disp(' Binary information at Trans mitter :');
disp(x);
%XX representation of transmitting binary information as digital
signal XXX
bit=[];
for n=1:1:length(x)
    if x(n)==1;
       se=ones(1,100);
    else x(n)==0;
        se=zeros(1,100);
    end
     bit=[bit se];
end
t1=bp/100:bp/100:100*length(x)*(bp/100);
subplot(3,1,1);
plot(t1,bit,'lineWidth',2.5);grid on;
axis([ 0 bp*length(x) -.5 1.5]);
ylabel('amplitude(volt)');
xlabel(' time(sec)');
title('transmitting information as digital signal');
%XXXXXXXXXXXXXXXXXXXXXXX B-PSK modulation
XXXXXXXXXXXXXXXXXXXXXXXXXX%
A=5;                                                 % Amplitude of
carrier signal
br=1/bp;
% bit rate
f=br*2;                                                          % carrier
frequency
t2=bp/99:bp/99:bp;
ss=length(t2);
m=[];
for (i=1:1:length(x))
    if (x(i)==1)
        y=A*cos(2*pi*f*t2);
    else
        y=A*cos(2*pi*f*t2+pi);    %A*cos(2*pi*f*t+pi) means -
A*cos(2*pi*f*t)
    end
    m=[m y];
end
t3=bp/99:bp/99:bp*length(x);
subplot(3,1,2);
plot(t3,m);
xlabel('time(sec)');
ylabel('amplitude(volt)');
```

```
title('waveform for binary PSK modulation coresponding binary
information');
%XXXXXXXXXXXXXXXXXXXX B-PSK demodulation
XXXXXXXXXXXXXXXXXXXXXXXXXXXXX
mn=[];
for n=ss:ss:length(m)
  t=bp/99:bp/99:bp;
  y=cos(2*pi*f*t);                                          %
carrier siignal
  mm=y.*m((n-(ss-1)):n);
  t4=bp/99:bp/99:bp;
  z=trapz(t4,mm) ;                                            %
intregation
  zz=round((2*z/bp));
  if(zz>0)                                          % logic level =
(A+A)/2=0
                          %becouse A*cos(2*pi*f*t+pi) means -
A*cos(2*pi*f*t)
    a=1;
  else
    a=0;
  end
  mn=[mn a];
end
disp(' Binary information at Reciver :');
disp(mn);
%XXXXX Representation of binary information as digital signal
which achived
%after PSK demodulation
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
bit=[];
for n=1:length(mn);
    if mn(n)==1;
       se=ones(1,100);
    else mn(n)==0;
        se=zeros(1,100);
    end
     bit=[bit se];
end
t4=bp/100:bp/100:100*length(mn)*(bp/100);
subplot(3,1,3)
plot(t4,bit,'LineWidth',2.5);grid on;
axis([ 0 bp*length(mn) -.5 1.5]);
ylabel('amplitude(volt)');
xlabel(' time(sec)');
title('recived information as digital signal after binary PSK
demodulation');
%>>>>>>>>>>>>>>>>>>>>>>>>>>> fft>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>%
m1=fft(m);
f=(0:length(m)-1)*br*100/length(m);
figure;
plot(f,abs(m1));
```

Appendix C

```
%Binary FSK %

clc;

clear all;
close all;
x=[ 1 0 0 1 1 0 1];                                          %
Binary Information
bp=.000001;
% bit period
disp(' Binary information at Trans mitter :');
disp(x);
%XX representation of transmitting binary information as
digital signal XXX
bit=[];
for n=1:1:length(x)
    if x(n)==1;
       se=ones(1,100);
    else x(n)==0;
        se=zeros(1,100);
    end
     bit=[bit se];
end
t1=bp/100:bp/100:100*length(x)*(bp/100);
subplot(3,1,1);
plot(t1,bit,'lineWidth',2.5);grid on;
axis([ 0 bp*length(x) -.5 1.5]);
ylabel('amplitude(volt)');
xlabel(' time(sec)');
title('transmitting information as digital signal');
%XXXXXXXXXXXXXXXXXXXXXXX B-FSK modulation
XXXXXXXXXXXXXXXXXXXXXXXXXX%
A=5;                                                 % Amplitude of
carrier signal
br=1/bp;
% bit rate
f1=br*8;                                % carrier frequency for
information as 1
f2=br*2;                                % carrier frequency for
information as 0
t2=bp/99:bp/99:bp;
ss=length(t2);
m=[];
for (i=1:1:length(x))
    if (x(i)==1)
        y=A*cos(2*pi*f1*t2);
    else
        y=A*cos(2*pi*f2*t2);
```

```
    end
    m=[m y];
end
t3=bp/99:bp/99:bp*length(x);
subplot(3,1,2);
plot(t3,m);
xlabel('time(sec)');
ylabel('amplitude(volt)');
title('waveform for binary FSK modulation coresponding binary
information');
%XXXXXXXXXXXXXXXXXXX B-FSK demodulation
XXXXXXXXXXXXXXXXXXXXXXXXXXXX
mn=[];
for n=ss:ss:length(m)
  t=bp/99:bp/99:bp;
  y1=cos(2*pi*f1*t);                    % carrier siignal for
information 1
  y2=cos(2*pi*f2*t);                    % carrier siignal for
information 0
  mm=y1.*m((n-(ss-1)):n);
  mmm=y2.*m((n-(ss-1)):n);
  t4=bp/99:bp/99:bp;
  z1=trapz(t4,mm)
% intregation
  z2=trapz(t4,mmm)
% intregation
  zz1=round(2*z1/bp)
  zz2= round(2*z2/bp)
  if(zz1>A/2)      % logic lavel= (0+A)/2 or (A+0)/2 or 2.5 (
in this case)
    a=1;
  else(zz2>A/2)
    a=0;
  end
  mn=[mn a];
end
disp(' Binary information at Reciver :');
disp(mn);
%XXXXX Representation of binary information as digital signal
which achived
%after demodulation
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
bit=[];
for n=1:length(mn);
    if mn(n)==1;
       se=ones(1,100);
    else mn(n)==0;
        se=zeros(1,100);
    end
     bit=[bit se];
end
t4=bp/100:bp/100:100*length(mn)*(bp/100);
```

```
subplot(3,1,3)
plot(t4,bit,'LineWidth',2.5);grid on;
axis([ 0 bp*length(mn) -.5 1.5]);
ylabel('amplitude(volt)');
xlabel(' time(sec)');
title('recived information as digital signal after binary FSK
demodulation');
%>>>>>>>>>>>>>>>>>>>>>>>>> fft
>>>>>>>>>>>>>>>>>>>>>>>>>>>>%
m1=fft(m);
f=(0:length(m)-1)*br*100/length(m);
figure;
plot(f,abs(m1));
```

Appendix D

```
%Amplitude modulation

clear all;
fs=1000;
t=0:1/fs:0.1;
m=cos(2*pi*20*t);
x=cos(2*pi*200*t);
y=m.*x;
plot(t,y)
f=(0:length(y)-1)*fs/length(y);
y1=fft(y);
figure;
plot(f,abs(y1))
```

Appendix E

```
%Amplitude modulation
clear all;
fs=1000;
t=0:1/fs:0.1;
m=cos(2*pi*20*t);
x=cos(2*pi*200*t);
y=m.*x;
plot(t,y)
f=(0:length(y)-1)*fs/length(y);
y1=fft(y);
figure;
plot(f,abs(y1))
```

Appendix F

```
%Frequency modulation
clc;
clear all;
close all;
fc=input('Enter the carrier signal freq in hz,fc=');
fm=input('Enter the modulating signal freq in hz,fm =');
fs=1000;
t=0:1/fs:0.1;
x = sin(2*pi*30*t);
y = fmmod(x,fc,fs,fm);
plot(t,y)
y1=fft(y);
f=(0:length(y)-1)*fs/length(y);
figure;
plot(f,abs(y1));
```