RFID Signal Acquisition and Identification

A Thesis report submitted in partial fulfilment of the requirement for the degree of

Master of Technology

In

Electronics and Instrumentation

By

VIKRAMADITYA JAVRE

Roll no: 212EC3152

Department of Electronics and Communication Engineering
National Institute of Technology, Rourkela-769008,
Odisha, India
2014

RFID Signal Acquisition and Identification

A Thesis report submitted in partial fulfilment of the requirement for the degree of

Master of Technology

In

Electronics and Instrumentation

By

VIKRAMADITYA JAVRE

Roll no: 212EC3152

UNDER THE GUIDANCE OF

Dr. Samit Ari

Department of Electronics and Communication Engineering
National Institute of Technology, Rourkela-769008,
Odisha, India
2014

DECLARATION

I hereby declare that the work presented in the thesis entitled as "**RFID Signal Acquisition and Identification**" is a bona fide record of the systematic research work done by me under the guidance of **Prof. Samit Ari**, Department of Electronics & Communication, National Institute of Technology, Rourkela, India and that no part thereof has been presented for the award of any other degree.

VIKRAMADITYA JAVRE

(Roll no. 212Ec3152)

DEPARTMENT OF ELECTRONICS AND COMMUNICATION ENGINEERING

NATIONAL INSTITUTE OF TECHNOLOGY

ROURKELA-769 008, ODISHA, INDIA.

Certificate

This is to certify that the work in the thesis entitled "**RFID Signal Acquisition and Identification"** by **Vikramaditya Javre** is a record of an original research work carried out by him during 2013 - 2014 under my supervision and guidance in partial fulfilment of the requirements for the award of the degree of Master of Technology with the specialization of Electronics and Instrumentation Engineering in the department of Electronics and Communication Engineering, National Institute of Technology Rourkela. Neither this thesis nor any part of it has been submitted for any degree or academic award elsewhere.

Place: NIT Rourkela

Date: 1 June 2014

Dr. Samit Ari

Asst. Professor, ECE Department

NIT Rourkela, Odisha

Acknowledgments

Completion of this project and thesis would not have been possible without the help of many people, to whom I am very thankful. First of all, I would like to express my sincere gratitude to my supervisor, **Prof. Samit Ari**. His constant motivation, guidance and support helped me a great deal to achieve this feat.

I would like to thank Prof. S. K. Patra, Prof. K. K. Mahapatra, Prof. S. Meher, Prof. S. K. Behera, Prof. Poonam Singh , Prof U.C. Pati, Prof T.K. Dan and Prof. A. K. Sahoo for guiding and inspiring me in many ways. I am also thankful to other faculty and staﬀ of Electronics and Communication department for their support.

I would like to mention the names of Manab, Dipak, Manu and Subhamoy and all other members of Computer Vision Lab for their constant support and co-operation throughout the course of the project. I would also like to thank all my friends within and outside the department for all their encouragement, motivation and the experiences that they shared with me.

I am deeply indebted to my parents who always had their belief in me and gave all their support for all the choices that I have made.

Finally, I humbly bow my head with utmost gratitude before the God Almighty who always showed me the path to go and without whom I could not have done any of these.

Vikramaditya Javre
212EC3152

Table of Content

List of Figure

List of Tables

Abstract

RFID is one of the fastest growing technologies grouped under Automatic Identification (auto ID). RFID tags are very low cost and used for identification of objects. RFID is a global technology that is used in industries, medical, wall mart, airport baggage, Libraries, Smart cards, even in every transported object has its own RFID tag. Therefore, concern of security and privacy should be there to prevent unauthorized access. A method is proposed to prevent cloning and counterfeiting of tags based on RF Fingerprinting. RF fingerprinting of a tag is based upon physical attributed such as an electromagnetic (EM) signal of the tag. By capturing the EM signal of RFID tags a method known as Dynamic wavelet fingerprinting is applied to generate fingerprint images of signals. Our proposed method consists of four stages: Namely Real time data acquiring by use of a CRO, Dynamic wavelet fingerprinting (DWFP) of the signal, Feature extraction, and Classification. Feature is extracted such as Eccentricity, perimeter, centroid , extent, area and orientation. Ann classifier is used which is a one vs. One classifier. To improve the performance of classification multi-feature based serial feature fusion technique has been proposed, which shows a significant improvement in classification performance. RF fingerprint allows prevention of unauthorized access, identification and detecting cloning of sensitive devices. To identify tags and to detect counterfeit RF fingerprinting can be used. The cost of the tag does not increase and can be used in existing tag with only requirement of software.

Chapter 1

INTRODUCTION

1.1 Introduction

RFID is defined as an automatic identification technology or automatic identification method which used radio waves to identify tags are used for retrieving or storing data. A tag is attached to objects and identify when come close to the reader. Because of its advantages over other identification methods RFID has been getting attention from many industries in recent years [2]. However, RFID technology is not a new technology; it has been first used in 1948. Technologies like barcode are totally replaced by RFID technology. There are different standards used in RFID that is Low, high and ultra-high frequencies. All this gives better performance and detectability with respect to barcode and any other technology and have different applications [5]. The RFID application depends on its code that is present in the RFID tag. There are different types of code present for writing on a tag like Electronic Product code (EPC) or Unique Item Identifier (UII). Once the code is written in tag, then it cannot be changed. So precaution and perfection should be taken while the code. Generally EPC is mainly used and code is given wisely to every manufacturing tag company. There are different codes, standards available for different applications [9]. From a certain distance reader scanned the tag information such as physical dimensions, prices, product attributes, unique serial number or laundering requirements. This scanning is done from a distance of several meters and wirelessly. Requirement of feature, limitations and the process of communication of tag is an essential aspect in term of security. Ann classifier has shown promise in this area and we had used Ann classifier for classification. Classification shows that each tag can be identified uniquely with 82.27% accuracy. Using this method the cost of tag is not increased can be applied to any type of tag. So without use of other encryption techniques a tag can be uniquely identified.

RFID tags are existing every in the modern world so concern of security of RFID tag is essential. Proposed RFID security involves encryption of code, restricting RFID devices to physical contact to tag such as passport wallet, which block RF field, public key cryptography. But if a tag is cloned then possibility of security breaches is high and more problem to come. Security of RFID tag is essential, some tag gives strong encryption so that is cannot be breached easily beat the cost of this tag is very high [13]. A method is proposed in his research where RFID tag can be encrypted and identify easily with any use of the encryption code.

1.2 Objective

In this research, we will focus on how to acquire real time data from RFID Tags using CRO, and applying signal and image processing techniques to obtained features of specific data. Using wavelet based methods we apply RF fingerprinting.

RF fingerprinting gives us a better and low cost identification without any use of other encryption code. For this proposed method and in our research, we had taken real time RFID signal with the use of Cathode ray oscilloscope (CRO) and save this signal in the MATLAB form. In MATLAB we had applied signal processing techniques followed by a method known as Dynamic Wavelet Fingerprinting (DWFP). DWFP gives nonlinear characteristics of the signal. Characteristics or features of signals apply for classification. Using this method, the cost of the tag is not increased can be applied to any type of tag. So without use of other encryption techniques a tag can be uniquely identified.

AN OVERVIEW OF RFID TECHNOLOGY

RFID uses radio waves to identify an object or tag. It can be utilized in counterfeiting detection, tracing, surveillance and checking for objects in industries generally in construction and manufacturing. Every field today is using RFID technology with large supplements [18]. Even in college's library RFID tags are used to check and identify tagged books and articles

1.3 History of RFID

In 1600 to 1800s observation, knowledge of optics, electricity and magnetism are introduced. The 1800s is the beginning of electromagnetic energy. The first transmission of radio waves is shown by Hertz. In 1845 Michael Faraday identifies the relation between light and radio waves. RFID technology is one of them.

In World War II RFID technology was first used. A Radar which was discovered in 1935 Sir Robert Alexander was used in World War II by Germans, Japanese, British and Americans warn any sigh of aircrafts. The RFID technology is used to determine whether the aircraft friend or foe. The reflected radio signals from the aircrafts identify planes. Watson-watt, who is the head and developed first active identify friend and foe (IFF) system [6]. THE RFID works on the same principle, a signal is sent to transponder which reflects back a signal or broadcast a signal. Since the capabilities of RFID have expanded and now it can be used in many business applications. RFID tracking technology is used every day in the modern world by single click information of the object is viewed.

1.4 Fundamental Components in an RFID System

An RFID system largely consists of tags (transponder), readers (transceiver) and Middle ware (software).

1.4.1 RFID Tag

RFID stored unique information in form of EPC (Electronic product key). These Tags are attached to products and then communicate via RFID Readers. Tags can categorize as Passive tags and Active tags. Passive tags are cheaper, smaller, unlimited life span because they never use power source. Reading range is 10cm up to a few meters. Outside electromagnetic field these tags do not work because these passive tags, generate power from a scattered radio signal [2]. Whereas active tags can have a reading range around 100 meters, but they use a power source and thus life span is short and also cost is high. However, because of because active tags can temperature, humidity and brightness so can be used more in industries purposes. Active tags are larger is size and having circuitry disadvantages over passive tags. RFID tags may be classified as sub classes

Passive Tags

- They generate from Interrogator field
- Low storage capability
- Shorter range (4-15 ft.)
- Have Read- Only tag's memory
- Low cost

Active Tags

- Battery required
- Higher storage capacities (512 KB)
- High Storage capability
- Long range (up to 300ft.)
- Rewritten by RF Interrogators
- High cost

1.4.2 RFID Reader

RFID readers connect the tags with the host computer. The tag sends information to the reader, it receives information and send it to host computer via standard interfaces. It creates a reading zone between tags and readers. The antenna in the reader receives radio waves coming from the tag's antenna. The Read zone depends on frequency used for communication and also reader's power. Mainly in industries and also in other application there are three kinds of readers installed namely: handheld, fixed reader installed in areas and fixed reader installed at choke point.

(A) Handheld Reader

It is lightweight and small used to find targets quickly and conveniently. It can be grabbed in our hand and carry easily from one place to another. Detection through the reader is very simple and generally uses in complicated areas. Through received signal strength user can now the distance between desired tags [31].

(B) Fixed Reader Installed in Area

It is a fixed reader installed in some place like ceiling or any other place to read movement, location and other internal data of the object. The information coming from the object is collected continuously. The range depends upon the reader's antenna power. The accuracy is greater than hand-held readers. Antenna size of reader and tag is important for range consideration. Mainly Active tags are used in fixed readers.

(C) Fixed Reader Installed at Chokepoint

It is the most common application of RFID. When a tagged object is arriving or departing it reads a signal and easily sees the flow of assets. It generally uses where the tagged object is moving quickly like in airport baggage or in manufacturing goods. Mainly Passive RFID tags are used in this application.

Fig 1.1: RFID Reader

1.4.3 Middleware

Middle is the software part of readers it receives several integrated data and it connects this data to host computer. Middleware is used as a communicator for passing data to the host computer and also it displays the data on the host computer. EPC, Sales, inventory, etc. is such data which displayed and easily viewed by the user. Data filtering, reader coordination, data routing, and process management is generally done be middleware [4][3].

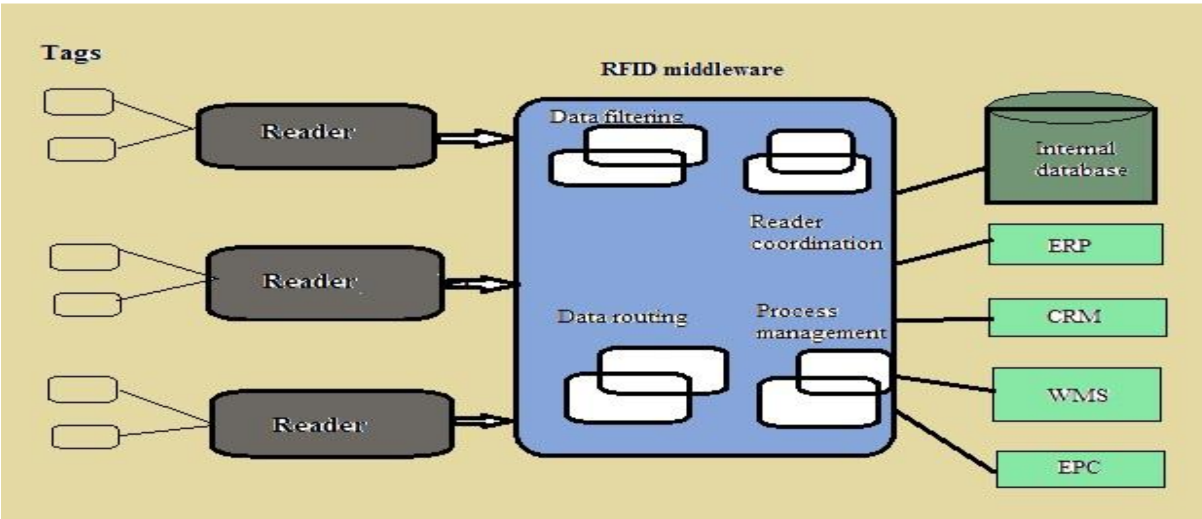


Fig 1.2: *RFID middleware*

1.5 RFID communication

In RFID communication host manages readers and issues commands. Tag and reader communicate via RF signal. The reader generates a carrier signal which sent out through the antennas and hits tags. Tags receives and modify the carrier signal and sends back this modulated signal [3]. This modulated signal received via reader's antenna which is decoded and returned to the host computer. This process of reflecting signal is also known as Passive Backscatter or Field disturbance device.

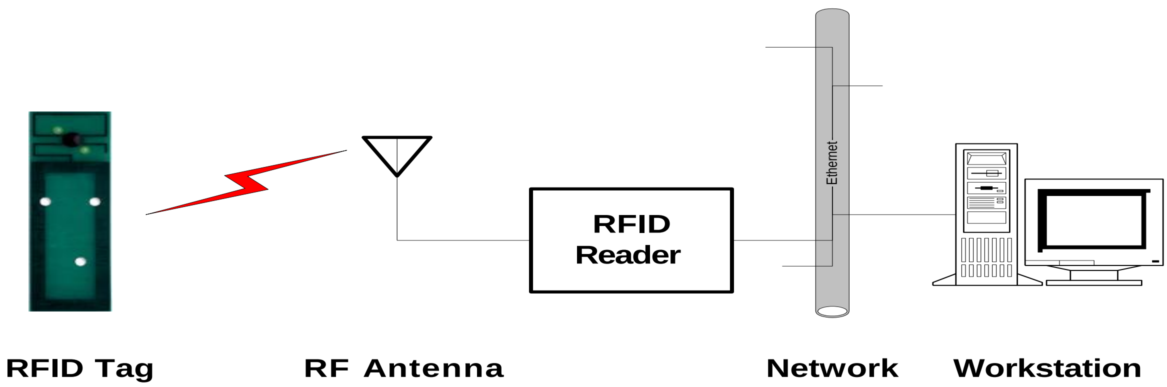


Fig 1.2: RFID Communication

RFID communication can be classified as Far-field and near-field communication. All data is transferred through this far-field and near-field communication.

1. Near -field Coupling/communication-

Near-field coupling is based on magnetic induction which proposed by Faraday. A reader generates a current which results in a magnetic field near by its region. If a tag placed near this region a voltage will appear on its region. On near-field coupling using load modulation tags sends data back to the reader [4]. Tag has its own magnetic field to opposes the reader's field and hence the reader senses small flow of current in it. In most homes today this principle is used in power transformers. For implementing a passive RFID tag near-field coupling is a better approach.

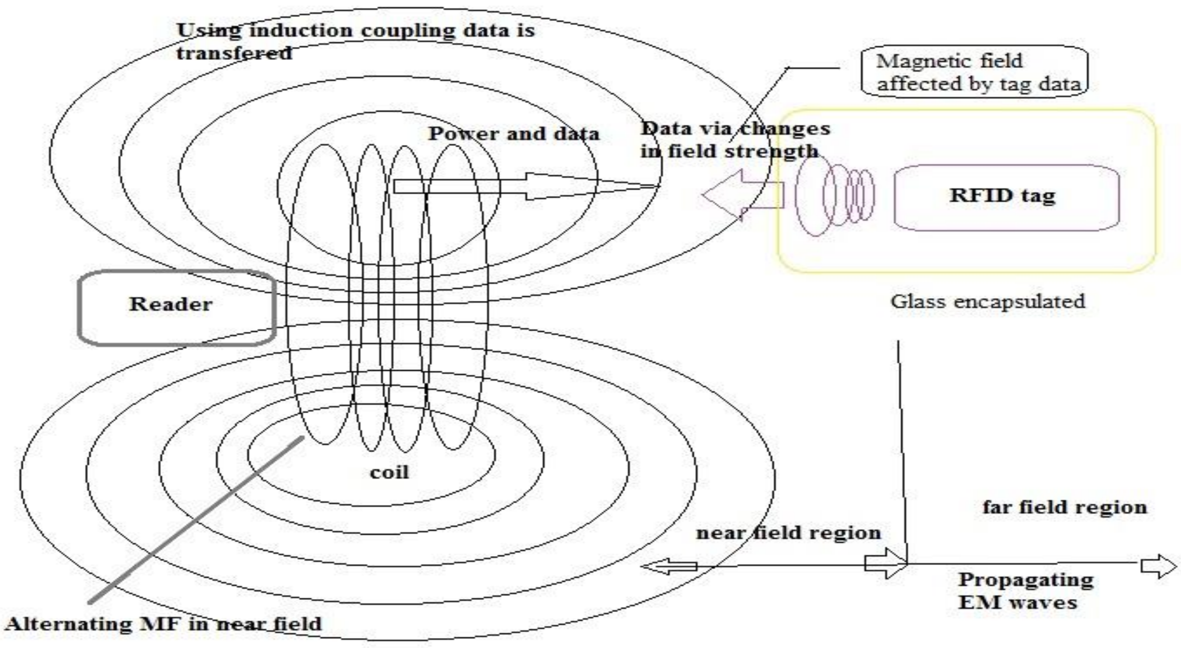


Fig 1.3:. Near-field coupling.

However, there are some physical limitations of near –field coupling. The range is limited and depends upon a range of magnetic induction, which is c/2πf. If the frequency is increased distance of the near – field region is decreased. Energy is an also a limitation of the near - field region because it acts as a function of distance.

2. Far -field Coupling/communication-

The dipole antenna of reader propagates EM waves which captured by the RFID tag. A smaller dipole antenna of tag generates a potential difference across the arm of its dipole [5] [6]. It is then rectifies and limed to capacitor which accumulated power in circuitry. Information is passed via load modulation. If a particular frequency is used and antenna is designed with precise dimension, then tag absorbs most of energy flowing through the reader. Antenna reflects back some energy because of the impedance mismatch of frequency. This energy is detected by a radio receiver [4].

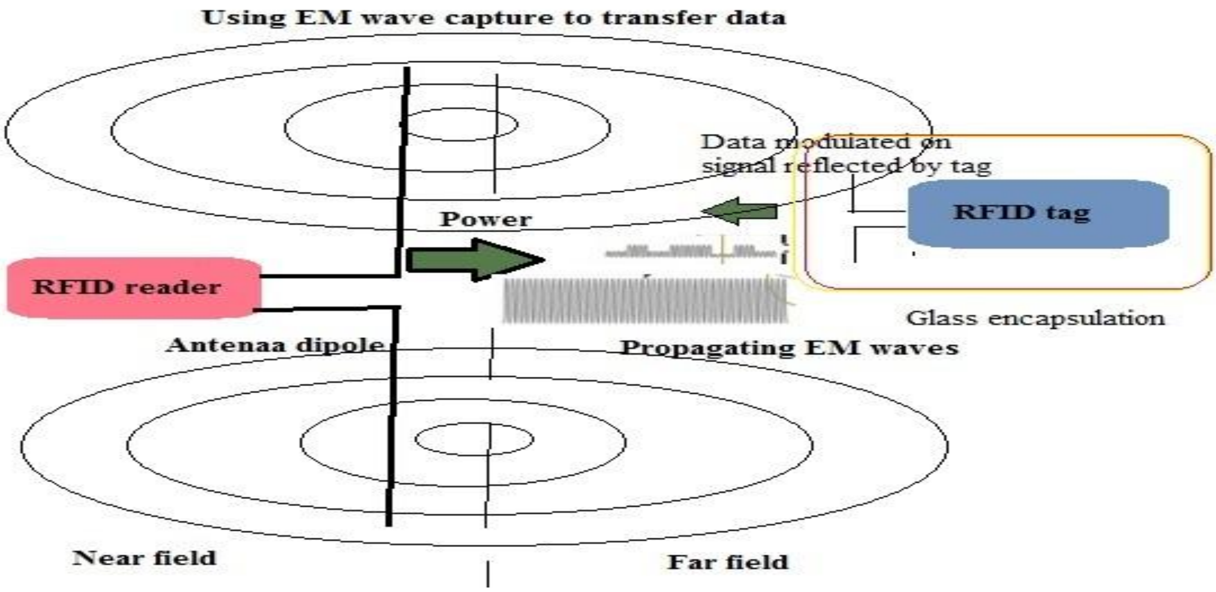


Fig 1.4:. Far-field coupling

In the far - field the operational frequency is more than 100 MHz and comes in the range of the ultrahigh - frequency band (UHF). The far-field range is depends upon the amount of energy from the tag and the sensitivity of radio receivers. The reflected energy is very small and by using Moore's law tags with larger distance can be read. The range of far-field reader is varied from 3 m to 6 m, depending upon the type of reader used.

1.5.1 RFID Frequencies

RFID technology is based on radio waves of electromagnetic fields. Understanding the frequency gives knowledge about RFID applications. 30 to 300 KHz is referred as Low frequencies in which 125 to 134 KHz generally uses for RFID applications. This RFID frequency has short range typically less than 2 m. 3 to 3 MHz comes under high frequency and range is less than 1 m. Both LF and HF can pass through water, but only HF penetrates water more easily. Transfer rate of HF is about 25 Kbits/s. 3000 MHz to 3 GHz comes under Ultra high frequency (UHF) in which 868 MHz generally used and the range is up to 100 m having a transfer rate of 1kbits/s. 2.45 GHz is microwave frequency and its uses for longer distance with high transfer rate.

TABLE I RFID Frequencies

Frequency Ranges	**LF** **125 KHz**	**HF** **13.56 MHz**	**UHF** **868-915 MHz**	**Microwave** **2.5 &5.8 GHz**
Read range	Shortest 1”-12”	Short 2”-24”	Medium 1”-10”	Longest 1’-15’
Power source of Tag	Inductive coupling	Inductive or capacitive coupling	Integral battery	Integral battery
Data rate	Slower	Moderate	Fast	Faster
Reading ability	Better	Moderate	Poor	Worse
Applications	Control and security, manufacturing, identification	Library books, laundry, employee ID’s	Supply chain, highway tracking	Highway tracking for private vehicles, asset tracking

An application under frequency range is differing in characteristics such as for liquid products, HF is used, for supply chain management UHF is used, for access control LF is used and in the toll booths microwave is used. Table I shows different frequencies with different applications

1.5.2 RFID Standards

RFID standards are important in industries. RFID is rapid application, but it’s not easy to install on different items or locations. Data and Technology standard are two types of RFID standards. EPC comes under Data standard and provide unique information about the tag. This code is invented by MIT Auto-ID centre and divided into four partitions [5]. First two digit numbers identify the structure, type and length also its. Identify the manufacturing company of tag. This is generally used in the retail sector. EPC for different items is different. EPC is a 64-bit or 96-bit code

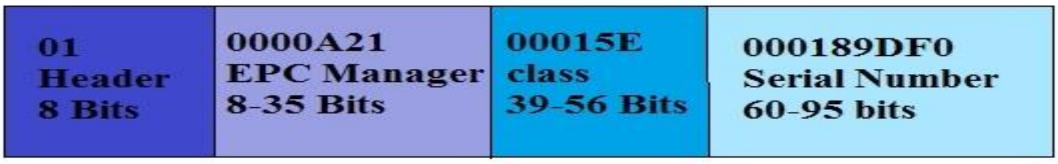


Fig 1.5: RFID Electronic Product Key code

Technology standards show the air interface between RFID readers and tags and are different from the EPC data structure. Different standards are shown below.

• ISO 18000-4 (Microwave): 2.45 GHz

• ISO 18000-7: 433 MHz

• ISO 18000-3 (HF): 13.56 MHz

1.6.3 RFID vs. Barcode

- Tag have unlimited lifespan.
- Distance is greater in active tag
- It can be merge with barcode technology

- Data size is large
- A single individual item can be identified.
- No line of sight required
- With single scan multiple objects can be read.

1.6 Security and Privacy in RFID devices

Today one of the major concerns is Privacy and security of RFID applications. Eavesdropping, cloning, contamination attacks and clandestine scanning are such concern that weakens the RFID technology. Encryption and common cryptographic operations are there to enhance the security and privacy of RFID technologies. But none of these techniques, giving perfect counter attacks to privacy and security. A RF Fingerprinting is proposed in this paper which leads to secure the RFID data with the use of any other encryption or cryptography techniques

.

1.6.2 Privacy:

RFID tags without the owner's knowledge always respond to queries from readers and thus lead to problems and making privacy more challenging. RFID privacy involves illegal interaction of tags with the reader. His problem can be solved if the public key data of tag are available, so the reader's authentication protocol is established. But this installing this protocol is challenging as it depends upon no of tags, range and power used. Tracking, Eavesdropping and clandestine scanning is a privacy concern if RFID devices.

1. Clandestine Scanning:

Use of Faraday cages prevents such attacks as without he use of user input RFID tags respond queries from readers, so it is possible to interrogate such tags. These attacks can go undetected for a certain distance [19]. A Faradays cage shields the tags and opposes any other electromagnetic waves and prevents such attacks.

2. Clandestine Tracking:

It is possible for unauthorized parties to track h movement of tag queries even when the queries are unique. Even if the tag is encrypted tracking is possible. So Faraday cages can be used to counterfeit and prevents clandestine scanning.

3. Eavesdropping:

Eavesdropping means to listen the private conservation or data secretly and data streaming may be recorded. This attack cannot be prevented by a Faraday cage since legitimate of tag is already taken part. Distance plays an important role here since they can carry out from a certain distance from the adversarial reader to tag data is not invaded and wrong doing alert is passed to the owner.

1.6.3 Security:

Legitimated false information of reader and problem of cloning, faking is the main concern in RFID security. Before any data taken out from the tag it is necessary to harvest data for authentication protocol. Data integrity and forgery via tag cloning are the main attacks arise from security concern of RFID devices.

1. Data Integrity:

Modifying the data of RFID is very dangerous and should be in control. For example, if any, known terrorist modifies this data and he easily able to cross the border by using a passport because today every passport uses RFID encryption [24]. Providing private key to tag prevents such attacks. But key should be passed to every verification senator and miss-match of key cause some other damages. Writing only registries also an alternative approach to prevent such attacks, but this lead to such disadvantages like data correction, appends impossible and updates.

2. Tag Cloning:

Using Digital signature may avoid tag cloning and easily verify data integrity of tags, but they prevent forgery but not copying. Unique numbering of tag can prevent tag cloning and read only registry is also used authentication with tag inventorying.

3. Denial of Service:

In RFID environments, DOS attacks may cause major harm. This attack very easy and unsophisticated and very cheap to carry out. The tag is free, using high temperature and using string electromagnetic pulses and makes them useless [22]. These attacks can curb using Faraday cages. The tag can be crashed by overloading of reader with more data.

All these attacks may weaken or damaging the use of RFID devices. For any device or application security is a primary concern. Here, all these methods of preventing attacks need encryption or any other process like shielding. But here on this thesis a method is proposed known as RF fingerprinting; by using it tag can be encrypted by means of its feature which is the characteristics of electromagnetic signals [26]. By taking feature of tags and applying some pattern recognition techniques unique identification of tags can be established. Detail of RFID fingerprinting is given in the next topic.

1.7 Thesis Outline

Introduction – In this chapter the introduction of RFID technology is shown like where it used first what is its hardware part, communication protocol, RFID vs. Other techniques. What are its software requirements, its limitation and security and privacy issues.

The second chapter deals with the methodologies used, in which a real time RFID signal is extracted using CRO and processed in MATLAB to form A binary fingerprint like Pattern. Further different feature and are extracted by applying some methods and features are fused together to give better accuracy in classification.

Third Chapter introduced the method of Feature fusion. This is done by applying Multi serial feature fusion technique and an input data is generated for the classifier. The use of Ann classifier is shown with its back propagation algorithm which describes the auto learning of the network. The result of various features is shown in this chapter.

Chapter four gives the conclusion of our work and tell the future work on this RFID system.

Chapter 2

Pre-processing and Data Acquisition

2.1 Introduction

RFID tags are different in design and here we used RFID passive tags. Name and configuration of tags are listed as follows.

*Avery-Dennison tag

In this work, we will focus on how to acquire real time data from RFID Tags using CRO, and applying signal and image processing techniques to obtained features of specific data. Using wavelet based methods we apply RF fingerprinting. RF fingerprinting gives us a better and low cost identification without any use of other encryption code. For this proposed method and in our research, we had taken real time RFID signal with the use of Cathode ray oscilloscope (CRO) and save this signal in the MATLAB form. In MATLAB we had applied signal processing techniques followed by a method known as Dynamic Wavelet Fingerprinting (DWFP). DWFP gives nonlinear characteristics of the signal. Characteristics or features of signals are applied for classification.

2.2 Methodologies

There were 2 tags purchased for this study. First real time signals of here are acquired by using CRO.As shown in fig reader's circuitry connection is connected to CRO terminals. A sinusoidal signal is displayed in CRO. When a tough place near a reader's antenna small power is reflected and amplitude of a sinusoidal signal is decreased. Decreasing of amplitude shows loss in energy. This energy is absorbed by a tag which is utilized to power the tag circuitry (antenna). This signal is saved in CRO in CVR format. This CVR format is open in

MATLAB and saved in Excel format. We have extracted 50 data's from each tag and saved it. Each tag, a unique name is given like for first tag it is given by V and 50 s data is given by v1, v2, v3, v4,………….. v50 and similarly for other tag. Two tags with 100 data was recorded. The operating frequency of reader is 11.56 MHz, which comes under high Frequency (HF).

Tag sent a demodulated signal (EPC) to the reader and general application, it is also a demodulated signal. For same EPC code the aim is to identify each unique tag. This EPC (data) is observed in pattern classifier

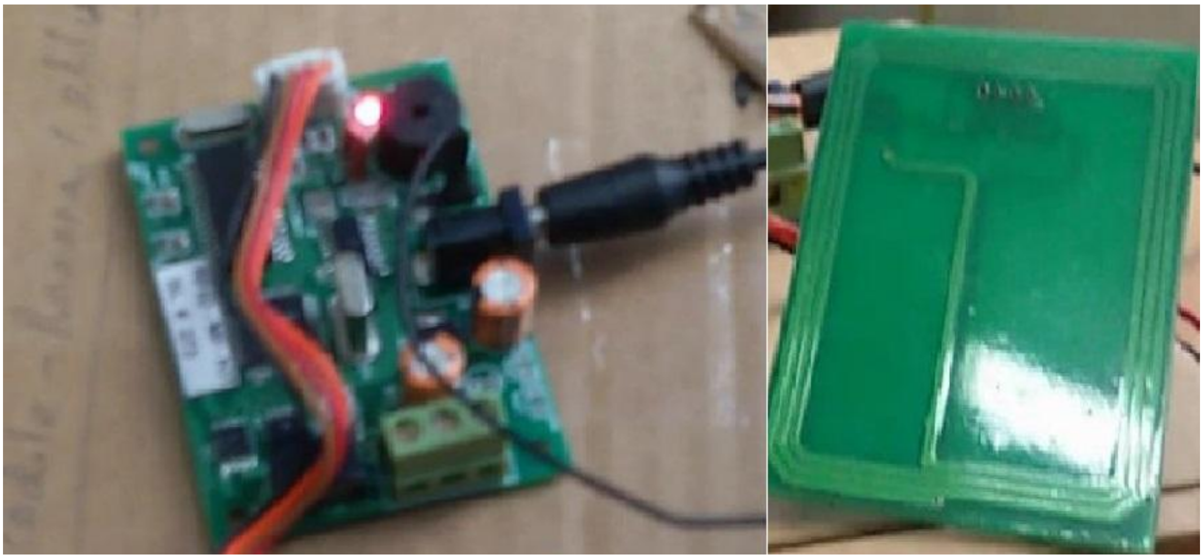


Fig 2.1.RFID reader with an antenna used in the study

2.3 RF FINGERPRINTING

Experiments by Lofstromet al shows unintentional modulation of circuits lead to identify the unique parameters of tags and theory is also coming under phantom circuits. RFID tags prevents counterfeiting by measuring nonlinear characteristics of electromagnetic waves .

This was studied by Romeroet al [1]. This experiment not works into low SNR . His first application was RFID was introduced by Danevet al in which 50 RFID cards were used for generating RFID fingerprints. Same EPC was written on each card to identify the fingerprint of RFID signal.

The feature is measured by using wavelet techniques and pattern classification technique are applied in individual tags. Simple RFID fingerprinting is based on signal's relevant feature. When a radio transmission is established transmitter generates its own property for transmission. RFID fingerprinting is a process which measure or identify this properties or features. Based on configuration, each signal generates its own fingerprint [2]. This radio frequency fingerprinting creates question around privacy, is they are reliable and safe. But after use of this method led more development of RFID tags. Many experts looking different uses for these technologies, such as tracking of humans and animals by using small RFID chips, in retail for product scanning. Today RFID becomes a topic of debate whether theses technologies should be implemented or to be used in its current form and is more protection is required. The main aim of radio fingerprinting is to detect signal's feature and to form a fingerprint pattern [8]. This pattern is measured and analysis by using pattern classification techniques so that it gives a unique identification. In his work we acquire real time signals of RFID readers and generate fingerprint patterns of these signals by using wavelets. After different features is extracted and combined with feature fusion technique. Ann classifier is used for pattern classification.

The application of pattern classification includes.

1) Sensing the element: RFID tags are read from certain distance and different EPC signals of these tags are gathered.

2) Feature extraction: These EPC signals are extracted and measurement is done for each signal.

3) Feature selection: There are different feature to be extracted, but here we choose a subset of this feature in other words feature is reduced. Efficient features are selected and irrelevant features are removed. Some of these features are combined together by a process known as feature fusion

4) Classification: Training and testing subsets are created of these data signals by resembling algorithm. The Ann classifier is trained and tested. For this application the classifier is discriminating in nature [1].

5) Decision making: Class is finalized through classifier.

2.4 Experimental Results

When a tough place near a reader's antenna small power is reflected and amplitude of a sinusoidal signal is decreased. Decreasing of amplitude shows loss in energy. This energy is absorbed by a tag which is utilized to power the tag circuitry (antenna) [4]. This signal is saved in CRO in CVR format as shown in fig 2.2 and fig 2.3

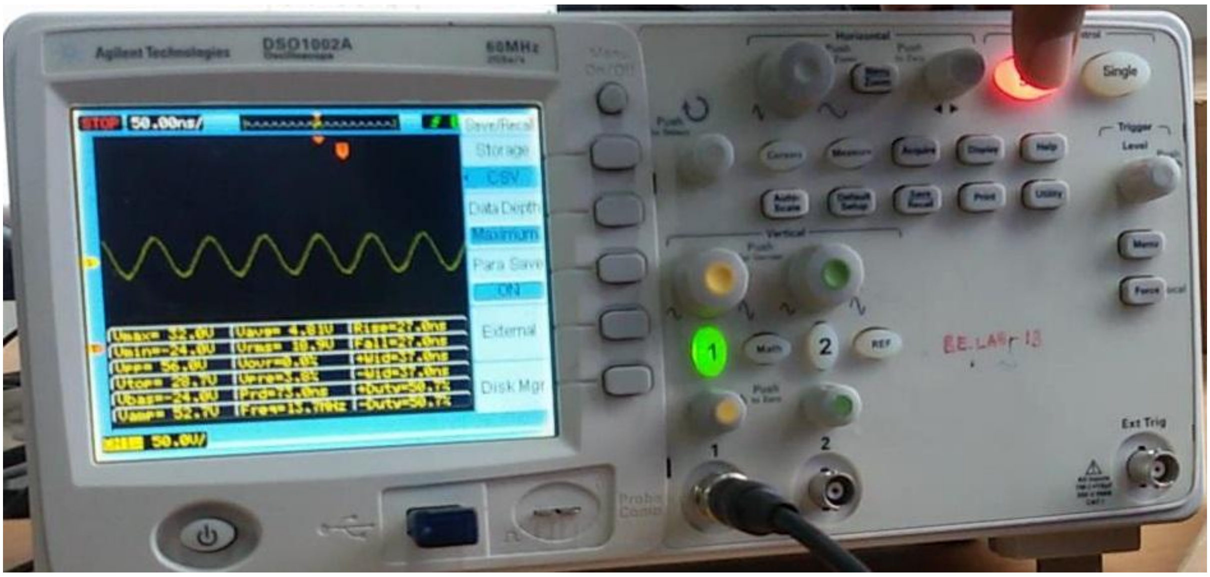


Fig 2.2 RFID signal acquiring by CRO

Fig 2.3 Signal saving in CVR format

The saved signal in MATLAB format is pre processed in MATLAB. Amplitude labelling, x and y axis naming and Frequency samples are calculated. Here the Shannon frequency algorithm is used to describe frequency samples. This theorem says that for a signal to reconstruct a frequency equal to, greater than the operating frequency is needed. Here operating frequency is 13.56 MHz and overall sample are 10240. This signal is shown in fig

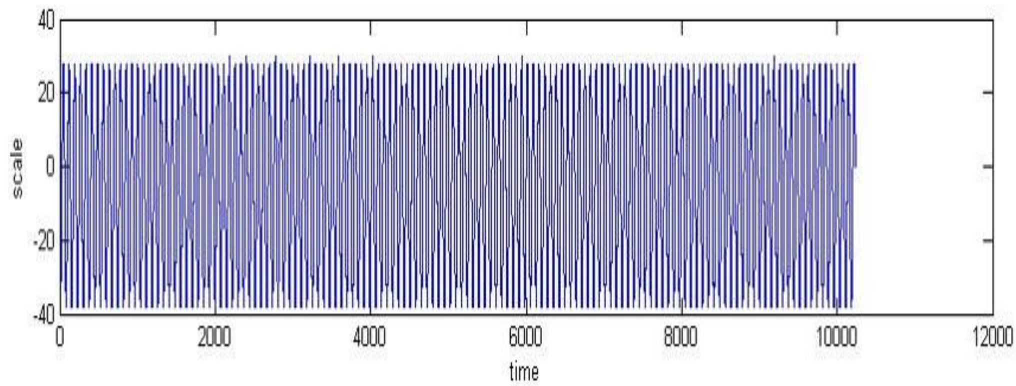


Fig 2.4 RFID signal in MATLAB after pre-processing

2.5 Conclusion

The RFID signal is acquired by using CRO and Mifare RFID kit operating in high frequency of 13.56 MHz The signal is very Low in level that is very low SNR which has to be processed. Signal is processed in MATLAB and a signal of high level with frequency samples is processed in to obtain Binary fingerprints Pattern is shown in next chapter.

CHAPTER 3

Feature Extraction and Classification

3.1 Feature Extraction

3.1.1 Introduction

Collection of relevant information from the signal is known as feature extraction. Signals are insufficient to answer and unable to distinct because of high transitions of signals. There are different tools used to extract features and characteristics of signal such as digital signal processing [6]. Different no of methods are there to extract feature for RFID signals. Dynamic wavelet transform is used to extract the feature because of its ability to characterize the time-frequency information which is very important for extracting efficient feature. This research work demonstrated this Dynamic wavelet transform and using multi feature fusion based techniques [25]. For a short segment of signal with good statically stability are the benefits for using these techniques.

This chapter introduced various aspects of feature extraction. First use of Dynamic wavelet transform is shown which generates RF fingerprints. Section2 describes the feature selection from these fingerprints. Section 3 describes the use of higher order statics to reduce the length of these features. Lastly, multi feature fusion technique is applied on this feature.

For tag t v and so, the signal extraction gives W-many different EPCs, tag(1) = 1,2 where j = 1,2,........................ W. Next feature is extracted and select W of them so that feature vectors will denote by SJ, k, k=1, 2.... W. Here in this work Dynamic wavelet fingerprint (DWFP) is used because it gives important and relevant information about RFID features. Higher order statics that are mean, variance Shannon entropy, Skewness, Kurtosis are used to reduce the size of features so that efficient classification is established [14]. DWFP and higher order statics are combined to yield a feature vector for classification with high accuracy.

3.1.2 DWFP

To extract features of original time-domain waveform of RFID signals wavelet transform applied this termed as DWFP technique. Here After applying DWFP a finger print like shape is generated of signal so termed as RF fingerprinting [1]. Before applying DWFT each signal is first low passed by low pass filter simply by applying a stationary wavelet transform. AS this a signal to be analytic in wavelet there are two parts for a signal that is approximation coefficients and detail coefficients. Detail coefficient represents high frequencies where as approximation coefficient represents low frequencies.

So first five details of signal are removed in other words high frequencies are removed from signal to minimize noise. Then a wavelet transform is applied in each signal (as shown in the figure below). Before applying DWFO each signal is low pass filtered and then a stationary wavelet transform is applied. The first five detail coefficient of signal is removed because this detail shows high frequencies of the signal.

1) Image Processing:

RF fingerprinting gives fingerprints of the waveform and next steps to apply image processing routines in each waveform. Fingerprints pattern is having different objects in a region. A different number of objects are found in each fingerprint. Thus the image processing of each object gives different properties (features). But fist eight – connected objects have to apply in each waveform to separate each object. Some of these measured properties in this work are Eccentricity of object, area of an object, boundaries of object, counting on – off pixels in a region, solidity, perimeter and centroid.

Image processing routine results in fingerprint properties. The values of these properties are matched they are discrete in time. For a smooth array of these properties linear interpolation is applied. Short description of these properties is given below.

(i) Solidity: It is convex hull in that region or defined as Area/Convex Area.

(ii) Orientation: It is the angle between a-axis and the major axis of the ellipse.

(III). Extent: It is the ratio of pixels in the pixel region to the total bounding box or area divided by the area of bounding box.

(iv) Perimeter: It is the circumference of the boundary or total boundary length.

(v) Area: Total numbers of pixels in the region are defined as Area.

(vi) Eccentricity: It is defined as distance between major axis and centroid [5] [7][6].

2) Fingerprint Feature Selection.

:

The main aim to apply DWFO is to find the features Uj, k, k=1,....... W, which is used to classify tags. Here the classification is one vs.. For this Euclidean distance metric is used to compare the Euclidean distances of different images [1].

As there are a number of objects in a fingerprint and after image processing routine each object gives number of features. So the size of a feature in one waveform is large and for better accuracy in classifier feature size should be less. Here in this work Ann classifier is used which gives better efficiency if there is minimum no. of feature present. For this purpose higher order statistics are applied in each feature length of single waveform [3]. This will decrease the feature length and efficient features are selected in a single waveform. This method is applied in all waveform

3.1.3 Experimental Results

This signal is proceeds in MATLAB and a method known as Dynamic wavelet finger printing is applied. First high frequency component is removed by applying stationary wavelet transform and wavelet coefficient is formed which is shown in fig 3.2.

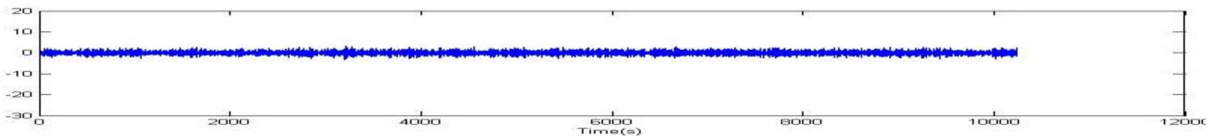


Fig 3.1: wavelet coefficient of waveform

This wavelet coefficient is sliced in Time – Scale axis and a result gives a Binary Fingerprint Pattern This pattern is shown is fig

Fig.3.2: Binary fingerprint image of waveform

This Binary pattern is connected together meant Binary number of this image is not separated . To separate different regions of object a Eight connected technique is applied and the result give a Separate objects of this binary Image.

Fig. 3.3 Binary fingerprint image after labelling with eight connected object

3.1.4 Conclusion

The Signal is converted into Binary pattern and eight connected technique is applied to separate the objects in this Finger print image. Then features are extracted from each objects .This features includes Eccentricity, Extent, Orientation, Centroid, perimeter and Solidity. This features are stored in Excel format for further use and for classification.

3.2 Classification

3.2.1 Introduction

Artificial neural networks are based on neural networks, which is based on biological structure of neurons. The artificial neural network is generally used as a classifier. ANN is discriminating in the state nature that's why generally used. It is implemented easily on hardware platform has the ability to generalization properties of automatic similarity based function and approximate functions [6]. it can mapped complex class distributed features very easily. During the learning phase it changes its structure of adaptive system based on external or inter information. Ann can be related to the human brain. As neuron is a main processing unit of the human brain so work identically in ANN. A neural network is formed by connecting neurons by using synaptic weight. Learning phase is used to acquire knowledge in networks. According desired design perspective synaptic weights and number of neurons is changed. Information is flowing through neuron in neural networks. There are three basic elements present in neural networks.

1. A synaptic weight w_{kj} is multiplied by the input of synapse j which is connected to neuron k of a signal x_{j}. *If he associated synapse is excitatory, then weight is positive and if the synapse is inhibitory then weight is negative [8].*

2. In summing the input signals an adder is there which is weighted according to the synapse of neuron.

3. For limiting the amplitude of the output an activation function is there. Typically the normal range of amplitude of neuron is [0, 1}] or [-1, 1].

An applied bias or threshold w_{k0} = *book* is also included in a neuron model which is used to increase or decrease the effect of activation function. A neural k is defined by a set of equations

3.2.2 Multilayer feed forward network

The first layer is called an input layer which goes towards second layer also called hidden layer. The second layer output passed through third layer and acts as an input of the second layer and this hierarchy keeps going on this till the output layer. As at each node the layer acts as its first input. The final output layer shows the overall response of the network and activation pattern is supplied in each node. The figure shows the feed forward network with p source nodes [19]. The first node of a hidden layer is denoted by h1 and with second layer it is denoted by h2, output layer is denoted by q so a p-h1-h2-q network is shown.

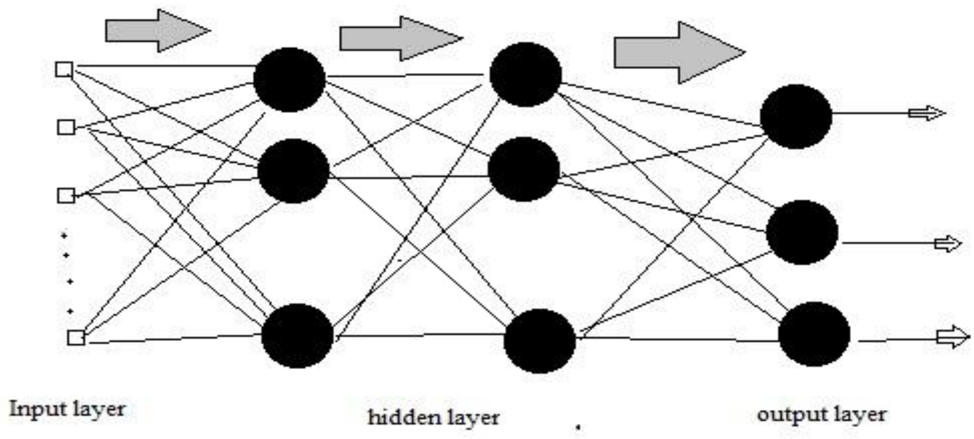


Fig 3.4 Multilayer feed forward neural networks

If every node is connected to its adjacent layer, then the network is said to be fully connected. Is some connection are missed then it's said to be partially connected.

3.2.3 Learning process

Neural network automatically learns from its environment and its properties makes interest in neural network and also by this property neural network improve its performance over each learning stage.[21] [24] Through an iterative process neural network learns about its environment this iteration is applied to its thresholds (base) and synaptic weight. Type Parameter changes shoes type of learning.

Let at a time n the synaptic weight w_{kj} is the value of $w_{kj}(n)$. An adjustable weight $\Delta w_{kj}(n)$ is applied to synaptic weight $w_{kj}(n)$, at time n and new update value is [8].

$$Week\ (n + 1) = w_{kj}\ (n) + \Delta w_{kj}\ (n) \qquad (9)$$

A solution of learning problem with well defines rules is called learning algorithm. Adjustment of the synaptic weight is carried out by learning algorithm.

3.2.4 Perceptron networks

For classification of linearly separable pattern perception is the simplest form of neural network. The single neuron consists of bias and synaptic weight [9]. Perceptron is used to train the linearly separable classes. Positions of decision surface are converges by Perceptron algorithm. This theorem is called a Perceptron convergence theorem [12]. The single layer Perceptron network is shown and it has limited to classify only two classes. Other Perceptron is able to compute more complex classes.

3.2.5 Back-propagation networks

Training a network with supervised manner and an algorithm is known as error back propagation algorithm. Learning error rule is used in this algorithm [6]. This algorithm has two steps, first forward and second backward [10]. In forward pass, feature pattern is applied to the input layer his inputs to perform and compete in each input layer. At output layer an actual response is produced. This phenomenon is based on gradient descent and delta rule. In delta rule, the learning rate parameter and gradient function is proportional to the weight of the neuron. In forward pass the synaptic weight is same. At the output layer error is measured by computing between target values and resulting output. Then this error is sent towards the backward direction to change the weights for a desired response [17]. This process of the forward pass and backward pass is repeated till the final aim is achieved.

3.2.6 Implementation of ANN and two-level CNN Classifier

The RFID signal data set performance is evaluated. Total 100 segments are obtained from each two classes. For each tag, there are 50 segments are taken which were used as training and testing data set. Each member of neural network is trained via training data set. 30 s data are taken from each tag which are used to train a neural network. Total 60 s data trained in Ann. Whereas 40 data is taken for testing purpose, 20 s data for each tag. After applying signal processing and DWFP on each data a fingerprint image is generated. These fingerprint patterns have a number of objects and for each object feature is extracted.

3.2.7 Performance matrices

Classifier performance is quantified by common matrices like accuracy, specificity, positive productivity and sensitivity. The overall accuracy is defined as [7]

$$A = 100\left\{1 - \frac{N_e}{N_b}\right\} \qquad (10)$$

A is the total number of misclassified data and also called accuracy of classifiers.

The parameter is given by following equations.

Accuracy: It is the number of correct classified segments to the number of total segments.

$$A_c = \frac{TP + TN}{TP + TN + FP + FN} \qquad (11)$$

Specificity: It is the Number of correct classified healthy segments to the number of total healthy segments [7] [8].

$$S_e = \frac{TP}{TP + FN} \tag{12}$$

Specificity: Number of correct classified seizure-free epileptogenic zone segments to the number of total seizure-free epileptogenic zone segments.

$$S_p = \frac{TN}{TN + FP} \tag{13}$$

Sensitivity: Number of correct classified epileptic seizure segments to the total number of epileptic seizure segments.

$$P_p = \frac{TP}{TP + FP} \tag{14}$$

In this equation *TP, TN, FN, FP* indicates true positive, true negative, false positive, false negative respectively. An image which has been correctly assigned to a class is true positive, whereas images which are not assigned is false positive [10]. An image which have been assigned but missed and assigned to another class is the false negative similarly opposite of false negatives is false positive. How a classifier recognizes images in a certain class without missing is called sensitivity and images which classifies exclusively is called positive productivity.

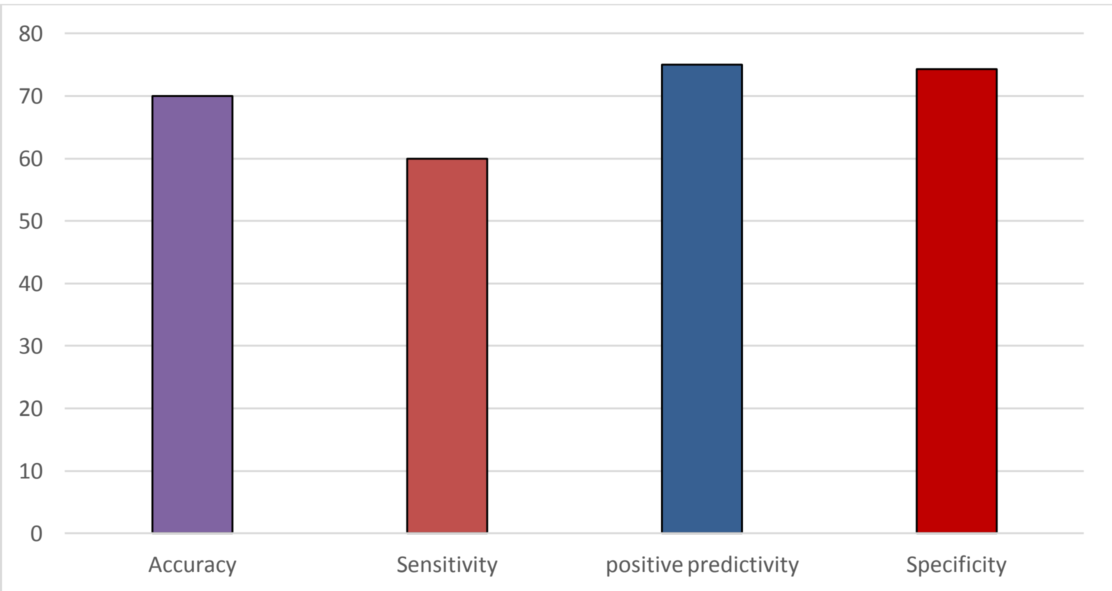
3.2.8 Result and Discussion

Using for performance metrics: accuracy, sensitivity, specificity and positive productivity, we have quantified our classifier. We have used feature fusion based technique in which features of objects in an image such as Eccentricity, equivalent diameter, perimeter, solidity, area and area is fused together. The confusion matrix of this feature fusion is shown in fig. This feature moments shown performance metrics of accuracy 70%, sensitivity 60%, positive predictivity 75% and specificity 80%.

Table II: Confusion matrix of serial fusion I

True class	Predicted Class	
	Positive	Negative
Positive	12	8
Negative	4	16

Table III: Performance comparison of six features fusion (eccentricity, orientation, perimeter, equivalent diameter and area).

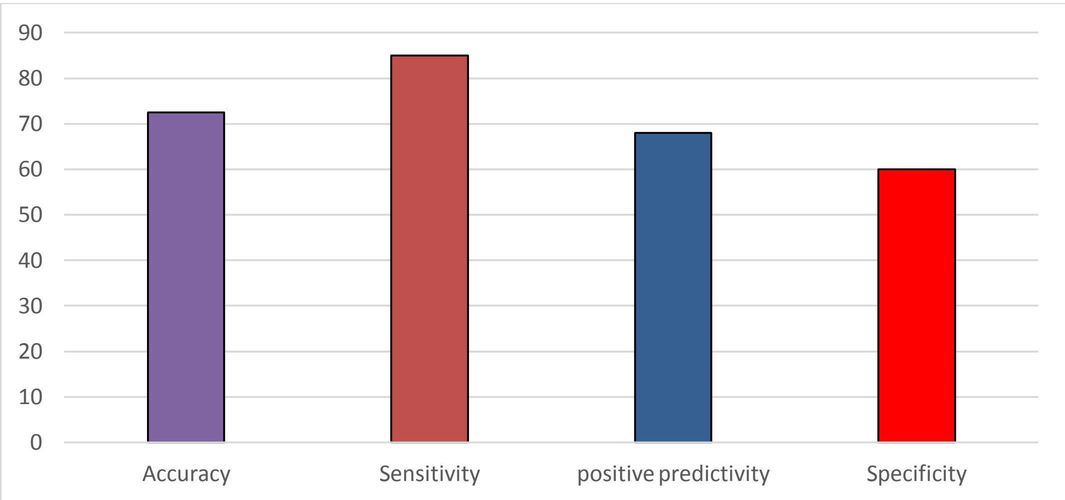


We have used other features such as centroid and angle between this centroid and distance of the boundary. His feature is fused together to get better performance and improvement of classifier. The confusion matrices are shown in fig. Here the performance metrics are accurate 72.50%, sensitivity 85%, positive predictively 68 % and specificity 60%, which show better performance than feature fusion of eccentricity and other features. This serial fusion strategy increases performance of classifier significantly.

Table IV: Confusion matrix of serial fusion II

True class	Predicted Class	
	Positive	Negative
Positive	17	3
Negative	8	12

Table V: Performance comparison of two features fusion centroid and angle between centroid and boundary).

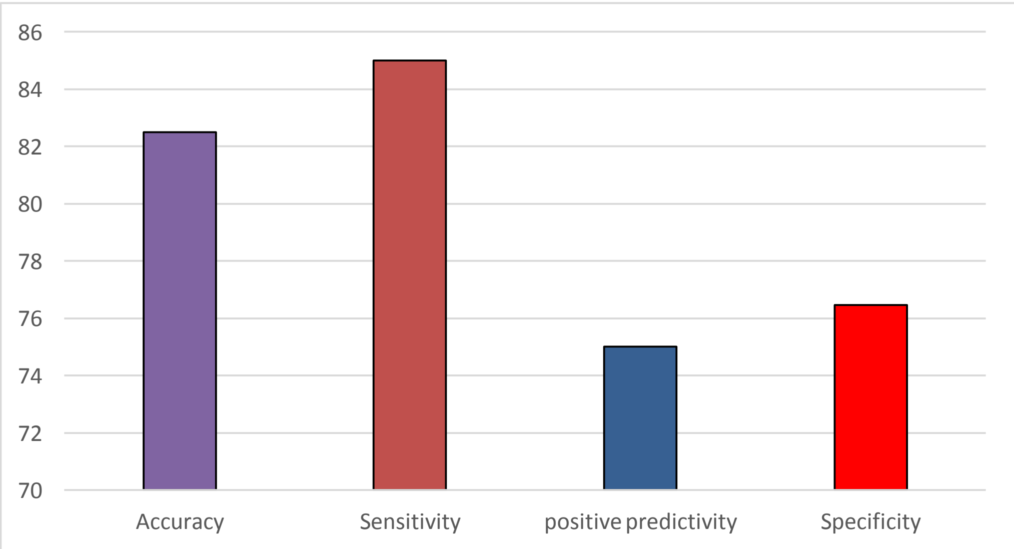


Both the serial fusion shown accuracy not larger than 72%. So here we used multi-fusion serial feature in which both the fusion of feature is fused again and apply on classifier. This multi features serial fusion technique show promise in the area and provide an accuracy of 82%, sensitivity 80.95%, positive predictively 76.47% and specificity 76.47%. The confusion matrix is shown in the table.

Table VI Confusion matrix of multi features serial fashion

True class	Predicted Class	
	Positive	Negative
Positive	18	2
Negative	5	15

Table VII: Performance comparison of multi feature serial fashion.



Chapter 4

Conclusion and Future work

4.1 Conclusion

Our proposed method consists of four stages: Namely Real time data acquiring by use of a CRO, Dynamic wavelet fingerprinting (DWFP) of the signal, Feature extraction, and Classification. To improve the performance of classification multi-feature based serial feature fusion technique has been proposed, which shows a significant improvement in classification performance. Two fusion of feature is used is overcoming the problem of mismatching. Experiment results show that multi feature serial fusion improves performance of classifier significantly. Despite the same EPC, written on tag we have created a binary classifier which can verify that tag1 is same as tag 2 with 82% accuracy. There is some limitation that it cannot determine the identification of tag 1 but can determine similarity between tag 1 and tag 2. Which were useful in ID's badge applications and application for tracking object. This method is an improvement on RFID tag which relies on encryption for security in small memory. Classifier is based on unintended qualities of signal. As approximation coefficient is removed from signal, but still, it's have higher SNR and future research to be done using these circumstances.

4.2 Future Work

RFID is a fast growing technology and in the future every product may be uses this technology. There are different applications are present in RFID technology. So security is a primary concern and for this reason we proposed this method [13]. We have taken physical attributes of signal of tag that is the unintentional modulation transmitting from it. There are lots of other characteristics present in a signal which should be studied. We have worked on high frequency RFID system that is 13.56 MHz of frequency. Work should be done on higher frequencies. We have worked on low SNR and SNR should be implemented for better understanding of RFID signals. Here on this thesis, we worked on demodulated sinusoidal signal is but work on binary signal should be implemented. Our work show that first a signal is converted in binary image and then image processing routine are applied to collect feathers. So different features to select to taken improve the accuracy and performance of classification. Selection of efficient features is should be worked on**.**

Bibliography

1. Bertoncini, Crystal, Kevin Rudd, Bryan Nousain, and Mark Hinders. "Wavelet Fingerprinting of Radio-Frequency Identification (RFID) Tags," *IEEE Transactions on Industrial Electronics*, Vol. 1, 2012.

2. Rao, Padmanabha R., and Paolo L. Siccardo. "Location determination using RF fingerprinting." *U.S. Patent No. 6269,246*. 31 Jul. 2001.

3. Zangeneh, Mondona, et al. "Surface plasmon spectral fingerprinting of adsorbed magnesium phthalocyanine by angle and wavelength modulation," Applied spectroscopy, vol. 5,no.8,,2004.

4. R. Want. "An Introduction to RFID Technology", *IEEE Pervasive Computing, vol.5, no.1*, 2006.

5. Dongre, Vikas J. and Mankar, Vijay "Devnagari Handwritten Numeral Recognition using Geometric Features and Statistical combination Classifier", *International Journal on Computer Science & Engineering, vol.5,no.10*, 2013.

6. Yu, Lei, et al. "Fingerprinting localization based on neural networks and ultra-wideband signals." *Signal Processing and Information Technology (ISSPIT), 2011 IEEE International Symposium on* IEEE, 2011.,vol.1,no.18

7. www.cs.ukzn.ac.za : last accessed June, 2014

8. Kolpakov, Roman, and Mathieu Raffinot. "New algorithms for text fingerprinting.*"Combinatorial Pattern Matching*. *Springer Berlin Heidelberg, vol.2, no.6,*2006.

9. www.slideshare.net, last accessed June, 2014

10. www.lkn.ei.tum.de : last accessed June, 2014

11. Web.cacs.louisiana.edu : last accessed June, 2014

12 . www.dfki.uni-kl.de : last accessed June, 2014

13. Periaswamy, Senthilkumar Chinnappa Gounder, Dale R. Thompson, and Jia Di. "Fingerprinting RFID tags." *Dependable and Secure Computing, IEEE Transactions on vol.8, no.6 (2011)*

14. arxiv.org : last accessed June, 2014

15. www.rfidaa.org : last accessed June, 2014

16 Gibbs, T., 2004. RFID: The Next New Thing. Intel Corporation.: last accessed June, 2014

17 O. Ureten and N. Serinken, “Wireless security through RF fingerprinting,” *Can. J. Elect. Comput. Eng., vol. 32, no. 1, pp. 27–33, 2007.*

18 Y.-J. Huang, C.-C. Yuan, M.-K. Chen, W.-C. Lin, and H.-C. Teng, “Hard-ware implementation of RFID mutual authentication protocol,” *IEEE Trans. Ind. Electron., vol. 57, no. 5*, pp. 1573–1582, May 2010.

19 A. Juels, “RFID security and privacy: A research survey,” IEEE J. Sel. Areas Commun., vol. 24, no. 2, pp. 381–395, Feb. 2006.

20 H. P. Romero, K. A. Remley, D. F. Williams, and C. Wang, “Electromagnetic measurements for counterfeit detection of radio frequency identification cards,” *IEEE Trans. Microw. Theory Tech., vol. 57, no. 5, pp*. 1383–1387, May 2009.

21 T. Fawcett, “An introduction to ROC analysis,” *Pattern Recognition. Letter. vol. 27, no. 8*, pp. 861 874, Jun. 2006

22 J. Hou and M. K. Hinders, “Dynamic wavelet fingerprint identification of ultrasound signals, ”*Mater. Eval., vol. 60, no. 9, pp*. 1089–1093, 2002.

23 D. Halperin, T. S. Heydt-Benjamin, K. Fu, T. Kohno, and W. H. Maisel. Security and privacy for implantable medical devices. *IEEE Pervasive Computing, Special Issue on Implantable Electronics,* January 2008

24 T. Fawcett, “An introduction to ROC analysis,” *Pattern Recognit. Lett., vol. 27, no. 8, pp*. 861–874, Jun. 2006

25 ISO/IEC 14443. Identification cards - Contactless integrated circuit(s) cards - Proximity cards, 2001

26 Philips Semiconductors. Mifare Standard 4 Kbyte Card IC - MF1 IC S70 – Functional Specification - Rev. 3.1, 2002.

27 Henning Richter, Wojciech Mostowski, and Erik Poll. Fingerprinting Pass-ports, NLUUG 2008 *Spring Conference on Security, Ede, the Netherlands, vol.2 no* 12, 2008

28 Tassos Dimitriou. A lightweight RFID protocol to protect against traceability and cloning attacks. In Security and Privacy for Emerging Areas in Communications Networks, 2005. Secure Comm 2005. *First International Conference on, pages 59 – 66, s*ept. 2005.

29 Josep Domingo-Ferrer, Francesc Sebé, and Agusti Solanas. A polynomial-time approximation to optimal multivariate microaggregation. Comput. *Math. Appl., vol. 1, no.*5:714–732, February 2008.

30 C. A. Bertoncini and M. K. Hinders, "Fuzzy classification of roof fall predictors in microseismic monitoring," *Measurement, vol. 43, no. 10*, pp. 1690–1701, Dec. 2010.

31 Charles H. Bennett, Gilles Brassard, Claude Cr´ epeau, and Ueli Maurer. Generalized Privacy Amplification. *IEEE Transaction on Information Theory, vol.6, no.41*:1915–1923, 1995.