RADIO FREQUENCY-BASED DEVICE DISCRIMINATION OF MIXED-SIGNAL INTEGRATED CIRCUITS AND COUNTERFEIT DETECTION

THESIS

Sean O'Neill, Capt, USAF

AFIT-ENG-MS-17-M-055

DEPARTMENT OF THE AIR FORCE
AIR UNIVERSITY

AIR FORCE INSTITUTE OF TECHNOLOGY

Wright-Patterson Air Force Base, Ohio

AFIT-ENG-MS-17-M-055

RADIO FREQUENCY-BASED DEVICE DISCRIMINATION OF MIXED-SIGNAL INTEGRATED CIRCUITS AND COUNTERFEIT DETECTION

THESIS

Presented to the Faculty

Department of Electrical and Computer Engineering

Graduate School of Engineering and Management

Air Force Institute of Technology

Air University

Air Education and Training Command

in Partial Fulfillment of the Requirements for the

Degree of Master of Science in Electrical Engineering

Sean O'Neill, B.S.E.E.

Capt, USAF

March 2017

AFIT-ENG-MS-17-M-055

RADIO FREQUENCY-BASED DEVICE DISCRIMINATION OF MIXED-SIGNAL INTEGRATED CIRCUITS AND COUNTERFEIT DETECTION

THESIS

Sean O'Neill, B.S.E.E.
Capt, USAF

Committee Membership:

Maj J. Addison Betances, PhD
Chair

Maj Samuel J. Stone, PhD
Member

Dr. Michael A. Temple
Member

AFIT-ENG-MS-17-M-055

Abstract

The research presented here focused on applying Radio-Frequency (RF)-based feature extraction combined with various types of machine learning such as: Multiple Discriminant Analysis/Maximum Likelihood (MDA/ML), Generalized Relevance Learning Vector Quantized-Improved (GRLVQI), Quadratic Discriminate Analysis (QDA), and Random Forest (RndF) to discriminate mixed-signal Integrated Circuit (IC) devices and perform counterfeit detection. Unintentional RF Emissions (URE) were collected from the Device Under Test (DUT), Maxim MAX526CCWG Digital-to-Analog Converter (DAC), that were independently screened into two categories of authentic and counterfeit. A subset of these devices were used to generate a model and new collections from all devices were used to verify the model. These techniques were considered to determine if RF Distinct Native Attribute (RF-DNA) fingerprinting is an acceptable feature extraction technique for use as a form of counterfeit detection.

RF-DNA fingerprinting with MDA/ML classification achieved the best classification performance within the *simulated* Signal-to-Noise Ratio (SNR) range defined as $\text{SNR}_S \in [-30, 30]$ in $\text{SNR}_{\Delta S} = 3$ dB intervals when compared to the models generated by GRLVQI, QDA, and RndF. All models produced at least an average percent correct classification ($\%C$) of $\%C = 99\%$ at some SNR within SNR_S. Verification of devices was accomplished and evaluated using Receiver Operating Characteristics (ROC) curves against an arbitrary benchmark of True Verification Rate (TVR) $\geq 90\%$ while False Verification Rate (FVR) $\leq 10\%$ which is consistent with previous Air Force Institute of Technology (AFIT) research. In all counterfeit assessments, the devices used in this research achieved the benchmark at SNR $\geq$ -3 dB.

RF-DNA fingerprinting with MDA/ML classification was used to develop a model to discriminate between the MAX526CCWG and an update device MAX526CCWG+ which is a lead free version of the MAX526CCWG. Maximum average $\%C = 99.7\%$ occurred at SNR = 27 dB. Verification results showed all except one device classifying into the correct categories. Additional feature dimensional reduction and sampling rate reduction was accomplished under this research. Feature reduction can accomplish and achieve desired results with as few as 1% of the total number of features used within the original assessment; however, it is recommended to be reduced to 33% of the original set. The sampling rate can be reduced from 10 GSps (Giga-samples per second) to 200 MSps and achieve similar results.

Acknowledgements

I would like to thank my wonderful wife for her love, encouragement, and patience with me while I focused and labored over this research. Thank you for watching the children, managing the household, and still finding the time to bring me dinner on the nights I worked late. Without her, none of this would have been possible.

I would also like to acknowledge my parents for encouraging me to pursue any career I felt passionate about in my life. Thank you for instilling in me a desire to learn and grow.

Sean O'Neill

Table of Contents

Page

List of Figures

List of Tables

List of Acronyms

AC Alternating Current

ADEC Advanced Detection of Electronic Counterfeits

AFIT Air Force Institute of Technology

ANN Artificial Neural Network

AWGN Additive White Gaussian Noise

BPF Band Pass Filter

CI Confidence Interval

CMOS Complementary Metal-Oxide-Semiconductor

COTS Commercial Off the Shelf

CV Cross-Validation

DAC Digital-to-Analog Converter

DARPA Defense Advanced Research Projects Agency

DC Direct Current

DFARS Defense Federal Acquisition Regulation Supplement

DFT Discrete Fourier Transform

DIP Dual In-line Package

DMS Diminishing Manufacturing Sources

DOD Department of Defense

DRA Dimensional Reduction Analysis

DSP Digital Signal Processing

DUT Device Under Test

EDS Energy Dispersive X-Ray Spectroscopy

EER Equal Error Rate

EM Electro-Magnetic

FADR False Anomaly Detection Rate

FBI Federal Bureau of Investigation

FCC Federal Communications Commission

FPGA Field-Programmable Gate Array

FRR False Rejection Rate

FSS Forward Stepwise Selection

FVR False Verification Rate

GPIO General Purpose Input/Output

GRLVQI Generalized Relevance Learning Vector Quantized-Improved

HSMC High Speed Mezzanine Card

IC Integrated Circuit

IQ In-phase and Quadrature-phase

IRE Intentional RF Emissions

IT Information Technology

LDA Linear Discriminant Analysis

LDAC Load Digital-to-Analog Converter

LOOCV Leave-One-Out Cross-Validation

LPF Low Pass Filter

MDA/ML Multiple Discriminant Analysis/Maximum Likelihood

MDA Multiple Discriminant Analysis

ML Maximum Likelihood

NSA National Security Agency

OEM Original Equipment Manufacturer

OOB Out-of-Bag

OPM Officer of Personnel Management

PCB Printed Circuit Board

PFP Power Fingerprinting

PII Personal Identifiable Information

PMF Probability Mass Function

QDA Quadratic Discriminate Analysis

RAR Rogue Accept Rate

RF Radio-Frequency

RF-DNA RF Distinct Native Attribute

RFINT Radio Frequency Intelligence

RndF Random Forest

ROC Receiver Operating Characteristics

ROI Region of Interest

RRR Rogue Rejection Rate

RSS Residual Sum of Squares

SCA Side Channel Analysis

SCADA Supervisory Control and Data Acquisition

SEM Scanning Electron Microscopy

SHIELD Supply Chain Hardware Integrity for Electronics Defense

SNR Signal-to-Noise Ratio

SoC System on Chip

SOIC Small Outline Integrated Circuit

TD Time Domain

TRR True Rejection Rate

TRUST Trusted Integrated Circuits

TTL Transistor-Transistor Logic

TVR True Verification Rate

URE Unintentional RF Emission

US United States

USA United States of America

USAF United States Air Force

US-CERT United States Computer Emergency Readiness Team

VHDL Very High Speed Integrated Circuit Hardware Description Language

XRF X-Ray Fluorescence

ZIF Zero-Insertion Force

RADIO FREQUENCY-BASED DEVICE DISCRIMINATION OF MIXED-SIGNAL INTEGRATED CIRCUITS AND COUNTERFEIT DETECTION

I. Introduction

This research was largely a work to demonstrate a non-contact, non-destructive means of combating the ever present problem of aging advanced weapon systems and diminishing manufacturing sources. This chapter describes the operational motivation in Section 1.1 and the technical motivation in Section 1.2. Section 1.3 describes the overall goal of this research and how it can help provide a proven methodology to a new application. Lastly, Section 1.4 summarizes the overall flow and organization of this research paper.

1.1 Operational Motivation

As technology advances, our capabilities increase. Over the past 100 years, our society has evolved from human power mechanized devices into electrical powered devices. This change in society has shown an increase in efficiency, capabilities, cost, and complexity while simultaneously reducing size. As society rapidly changes, the military must help defend against an ever changing and complex threat. The Department of Defense (DOD) has evolved into a highly electrical based dependent department. Computing hardware and software now encompass a large portion of the chain of command within the DOD. Policies and orders are communicated down to the lower echelons via a complex network of servers, satellites, and computers. Within the United States Air Force (USAF), the aircraft weapon systems currently in production such as the F-35, KC-46, and B-21 have more electri-

cal technology on them than the aging aircraft that they are designed to replace. Indeed there are many advantages to digital electrical systems. However, as digital systems become the norm within our society, infrastructure and weapon systems hold new vulnerabilities that have yet to be acknowledged and addressed.

As the DOD becomes more dependent on the commercial industry to design, develop, and build the weapon systems that are used to defend the United States of America (USA), the parts that are integrated into our weapon systems might not be produced by the original design company anymore. This is referred to as Diminishing Manufacturing Sources (DMS). As more Integrated Circuit (IC) devices fall victim to DMS, the commercial industry and the government have seen a rise in counterfeit ICs. In 2011, IHS reported that the global reports of counterfeit parts increased to 1,363 from 324 in 2009 [1]. The counterfeiting issue had become so large, that the National Defense Authorization Act for Fiscal Year 2012 mandated processes and systems to analyze, assess, and act on counterfeit electronic parts within the defense supply chain [2, 3]. The following sections describe the types of vulnerabilities in the DOD that could present itself in current and future government systems.

1.1.1 Software Vulnerabilities.

Reports of malicious actions against Information Technology (IT), digital processing, and networked devices have seen a significant increase in numbers recently. From 2006 to 2012, the number of cyber incidents reported by federal agencies to the United States Computer Emergency Readiness Team (US-CERT) increased by 782 percent [4, 5]. The US-CERT was also responsible for correcting one of the largest known breaches of sensitive information within the government. In June 2015, the Officer of Personnel Management (OPM) announced that millions of cur-

rent, former, and perspective background investigation records for federal and contractor employees had been stolen in a cyber intrusion which began in early 2014 [6]. It was later determined that the advanced persistent threat on the OPM was caused by a well known modified PlugX malware remote-access tool commonly deployed by Chinese-speaking hacking units [7]. Another well publicized cyberattack was performed on an Iranian Supervisory Control and Data Acquisition (SCADA) system. The Stuxnet virus infected the programmable logic controls used to control the nuclear centrifuges [8]. Cyberattacks are not limited to United States (US) government agencies. In February 2015, the health insurance company Anthem had over 80 million Personal Identifiable Information (PII) records accessed [9] and in 2013, the commercial company Target acknowledged up to 70 million credit and debit cards of its shoppers were stolen via a installed malware on the point of sale systems at retail locations across the country [10, 11].

One potentially under-appreciated type of software vulnerability is a firmware attack. For example, a hard drive has firmware associated with the controller used to access the different parts of the disk. A counterfeit or untrusted hard drive might have Trojan firmware that would allow an adversary to maintain a persistent presence on a system even through re-imaging the hard drive. Even more troubling, hard drive firmware in particular was never designed with security in mind [12], leaving it particularly vulnerable with no means of monitoring for malicious activity. While cyberattacks continue to present a serious threat to the government as a whole, the focus of this research will closely analyze the hardware vulnerabilities of counterfeit materiel within the defense supply chain.

Table 1.1. Top-5 most counterfeited semiconductors in 2011 (percentage of counterfeit part reports) [2, 5].

Rank	Commodity Type	% of Reported Incidents
#1	Analog IC	25.2%
#2	Microprocessor IC	13.4%
#3	Memory IC	13.1%
#4	Programmable Logic IC	8.3%
#5	Transistor	7.6%

1.1.2 Hardware Vulnerabilities.

As production of semiconductor devices has shifted to overseas manufacturing plants, there has been growing concern with authenticity of the devices as they are shipped back to the US [13]. This concern has compounded with the rise of counterfeit parts being reported. Table 1.1 displays the different types of electronic devices that were reported as counterfeit in 2011 according to IHS [2]. The presence of counterfeit hardware in the supply chain is a serious threat to the reliability of systems performing critical functions [5, 13]. High risk suppliers have increased their sales to federal agencies by 63% in 2012. In September 2010, the Missile Defense Agency found that the memory in a high-altitude missile's mission computer was counterfeit. Total cost of fixing the problem was $2.7 million [14]. In 2008, the Federal Bureau of Investigation (FBI) seized counterfeit Cisco routers worth $76 million that could have provided Chinese hackers a back-door into US government networks [14].

To counteract the rise in counterfeit technology in addition to the Defense Authorization Act for Fiscal Year 2012, the US government had released several Defense Federal Acquisition Regulation Supplement (DFARS) to further clarify and expand upon regulations. These changes pertain to the definitions of a trusted supplier as well as what must be done in the absence of a trusted supply and how to certify

or validate components from the new supplier [15]. Multiple commercial companies have begun providing capabilities that could combat the rise of counterfeits or at least the rise in detection of counterfeits and will be further expanded upon in Chapter II. Defense Advanced Research Projects Agency (DARPA) created a program, Trusted Integrated Circuits (TRUST), which defines that any change to the device, such as providing power to the device, in now considered the signal of interest [16]. This new definition confirms that an Unintentional RF Emission (URE) is a valid measurement for IC devices. A second program enacted by DARPA, Supply Chain Hardware Integrity for Electronics Defense (SHIELD), aims to design National Security Agency (NSA)-level encryption, sensors, near-field power and communications into a microscopic-scale chip capable of being inserted into the packaging of an integrated circuit [17]. SHIELD will hopefully provide relief in the future; however, current counterfeit parts must still be identified prior to placement in any weapon system.

The focus of this research will be to use a *non-contact*, *non-destructive* method for determining authenticity of parts. In particular, this research will show the ability to discriminate between authentic and counterfeit devices by extraction of unique characteristics from URE collected from mixed-signal devices.

1.2 Technical Motivation

Aside from the operational motivation, the following section outlines the technical motivation for this research. Current Air Force Institute of Technology (AFIT) research has been involved in discriminating between semiconductor devices based upon Radio-Frequency (RF) emissions. This research builds on previous efforts and extends the application to the detection of counterfeit electronic devices.

1.2.1 RF Emission Exploitation.

As electrical current is induced through a wire, a magnetic field is produced. As electricity flows through an IC, the same electro-magnetic phenomenon is observed. Declassified in 2006, the NSA released A History of US Communication Security [18]. This document revealed that in as early as the 1960s, the US government was aware that US security systems were vulnerable to electro-magnetic analysis. Additionally during the same time frame, the Soviets had guidelines related to RF interference. Governments were beginning to become aware of the serious possibility of exploitation via RF emissions analysis. Side Channel Analysis (SCA) seeks to extract exploitable information from these URE to gain some insight into device operation. Since each device is manufactured within a certain tolerance and no two devices are exactly similar, the collected URE could be used to uniquely identify devices.

1.2.2 RF-DNA Feature Generation.

RF Distinct Native Attribute (RF-DNA) fingerprinting process uses features extracted from RF emissions in an attempt to analyze and characterize the variance in the emissions, which are related to physical layer variances in manufactured semiconductor devices [19]. The RF-DNA features are statistical calculations on collected RF emissions, either intentionally emitted or unintentionally emitted. These features in combination with machine learning classification models can help determine authenticity of various types of ICs. Previously, AFIT has used RF-DNA features with the following classification models: Multiple Discriminant Analysis/-Maximum Likelihood (MDA/ML) [5, 19–37], Generalized Relevance Learning Vector Quantized-Improved (GRLVQI) [24–31, 38], and Random Forest (RndF) [39]. All classification techniques were successful in discriminating various types of devices.

This research seeks to expand RF-DNA research efforts to distinguish authentic parts from counterfeit parts of mixed-signal ICs.

1.3 Research Contributions

This research was primarily focused on the application of RF-DNA features in combination with machine learning classification algorithms to classify various mixed-signal ICs. The goal was to use URE emitted from the device to determine authenticity based upon a small subset of certified authentic parts and parts which have failed the certification process. The Device Under Test (DUT) was the MAX-526CCWG Digital-to-Analog Converter (DAC). Four classification models were evaluated: MDA/ML, GRLVQI, Quadratic Discriminate Analysis (QDA), and RndF. Once a suitable model was chosen, a series of feature reduction techniques and reduced sampling rates were explored to improve the time effectiveness of performing the classification. Additional classification and verification was conducted on the MAX526CCWG and the lead free updated part, MAX526CCWG+.

1.4 Document Organization

This document is organized as follows. Chapter II contains information relating to the background of RF emission exploitation, the different types of counterfeit parts, some of the current types of counterfeit detection methods, and the various types of machine learning classifiers used in this research. Chapter III provides the details of the test set up and methodology used in this research to obtain and extract the RF-DNA features and how each classification model was trained and tested. Chapter IV displays the results of percent correct classification based upon the methodology describe in Chapter III. Finally, Chapter V contains a summary of the results as well as recommendations for future research.

II. Background

This research expands on the techniques and methodology originally discovered under Side Channel Analysis (SCA). Some background information on SCA can be found in Section 2.1. Since this research seeks to discriminate counterfeit Integrated Circuit (IC) devices using Radio-Frequency (RF)-based techniques, Section 2.2 describes counterfeit types as well as current methods of determining authenticity. Section 2.3 describes the background research and supporting equations that describe the RF Distinct Native Attribute (RF-DNA) fingerprinting process and the four machine learning discrimination techniques used in this research. Section 2.4 describes some methods of previous dimensional reduction techniques and a computationally effective alternative that this research sought to utilize. Finally, Section 2.5 provides a brief description of the Device Under Test (DUT) used in this research.

2.1 Side Channel Analysis

SCA is the study of observable physical phenomena such as timing, voltage, current, and Electro-Magnetic (EM) radiation to extract information about the hardware. These phenomena are called the side channels [39, 40]. Each channel can leak information when the characteristics of the physically observable behavior, such as EM radiation, are correlated to the internal operation of the IC [19]. Previous SCA research has exploited variations in computational time [41], EM radiation [42], power consumption [43], and even optically [44]. This research primarily focused on observing the EM radiation by means of a RF emission collected from above the surface of a mixed-signal IC.

2.1.1 Intentional and Unintentional Emissions.

As stated in Section 1.2.1, when an electrical current is induced, a magnetic field is produced. There are two broad categories of EM RF emissions: Intentional RF Emissions (IRE) and Unintentional RF Emission (URE). IRE is a term to describe the intentional broadcast of RF energy to achieve a predetermined outcome. This includes but is not limited to wireless radios, cellular telephones, Bluetooth devices, Internet service providers' infrastructures, and satellite communications. Primarily, IRE are designed to intentionally broadcast a RF signal intended to convey information between two devices; however, IRE can also reveal sensitive information about the identity and/or operation of the originating device. Prior exploitation of IRE secondary information has been accomplished using RF-DNA to improve security over the following communication standards IEEE 802.11 WiFi [24–26, 32, 33, 45, 46], IEEE 802.15 ZigBee [23] and X10 [36], and IEEE 802.16 WiMAX [29, 30, 34, 35, 47].

URE are RF emissions that were not intended to broadcast a RF signal to convey information between two devices. When an IC conducts an operation such as changing a digital state or powering on a transistor, current fluctuations coupled by direct, inductive, or radiative means within the semiconductor produce URE [5, 48]. Direct coupling occurs when physical contact via a conductive medium transfers intentional currents within the same conductor [42]. Inductive coupling occurs when two wires are configured in such a way that a change in current through one wire induces a voltage across the ends of the other wire by means of EM induction. Radiative coupling or EM coupling occurs when two circuit components are separated by a large distance, typically more than a wavelength. Each circuit component acts as a RF antenna and might produce undesired affects within the circuits [49]. URE that manage to emanate out of the IC package can be observed with a near-

field probe. All devices are regulated by the Federal Communications Commission (FCC) in an attempt to mitigate IRE and URE interference on more protected forms of telecommunications [50]. Since URE are not intentionally emitted, URE tend to have significantly lower signal power compared to IRE. Previous Air Force Institute of Technology (AFIT) research has been conducted in the exploitation of URE to discriminate various devices from microcontroller units to programmable logic controllers [5, 19, 51–57].

2.1.2 Variations Between Devices.

Any manufactured product is built within a certain set of tolerances. Some examples of different type of tolerances might be rating an IC for military use as opposed to commercial use. Military-use ICs have a vastly different operating temperature range than commercial products. If a product passes all of the inspection criterion for the category it was designed for, then the IC is ready to be sold on the market. However during production, deep sub-micron small scale variations are introduced into the IC structure. The IC might still function as designed and be within the tolerances. This process enables the statement that no two ICs are exactly identical. These tiny variations within the device color the URE and make each URE unique for each device [21]. Previous RF-DNA research has been able to successfully discriminate between two "like model" devices based upon the devices URE [19–21, 51–53, 58].

2.2 Counterfeit Components

Counterfeit parts have become a large problem in government and industry supply chains. It is estimated that United States (US) semiconductor manufacturing companies are paying as high as $7.5 Billion in product replacement parts or over-

all repairs based upon counterfeit electronic components [59]. Over 66% of the reported counterfeit components in 2016 have been discontinued parts [59]. This becomes a serious problem when searching for a new type of IC that might replace a Diminishing Manufacturing Sources (DMS) component in the aging government systems.

2.2.1 Counterfeit Types.

There are various types of counterfeit components. These types can span the different applications that IC components can accomplish. Figure 2.1 displays the taxonomy of counterfeit types [60–63]. A recycled counterfeit refers to an IC that

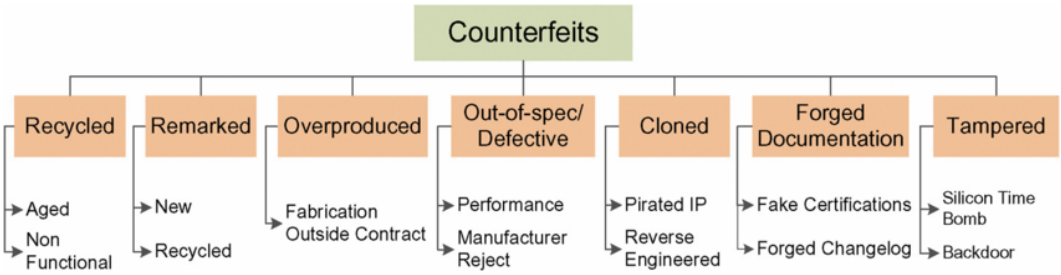


Figure 2.1. Taxonomy of counterfeit types [60–63].

has be recovered from an electrical system and is misrepresented and sold as a new component [60]. As e-waste is recycled it may end up into the hands of counterfeiters who are seeking to make a quick dollar by selling a component that might still function. The primary concern with recycled components is that as an IC ages it approaches a non-functioning state. If a part was purchased as new with an understood reliability and suddenly fails to function after a few uses, then this becomes a costly maintainability battle for the business manager of the system. Remarked counterfeit components are just as common as recycled ones. Remarked components typically are components which are designed at a lower grade, such as commercial, and remarked as a higher grade, such as military [60]. These components

might not function in the type of environment in which the grade was intended. Commercial-grade components are designed to operate within the temperature ranges of 0°C to 85°C where as a military-grade components are rated for -55°C to 125°C [64]. Overproduced counterfeit components are typically sold when a packaging company sells the components outside of the design company's contract [60]. This could become a problem with the reputation and profits for the design company. Out-of-specifications or defective counterfeit types can also infiltrate the market. These types are typically sold by an untrusted entity or a third party after the parts have knowingly failed to perform to the standard for which they were designed [60]. An example might be a packing employee attempting to make some money for themselves and selling the parts to an untrusted distributor claiming the parts are new. Cloned counterfeits are especially detrimental for the company who designed the component. Cloning is typically accomplished by reverse engineering or by illegally obtaining intellectual property [60]. Cloning could ruin the reputation of the company if the components were sold under the company's name but the manufacturing process for which the components were build produced vast differences between components. Forged documentation is similar to remarked or out-of-spec components. Forged documentation is when the components are shipped with fraudulent certifications or testing documentation that misrepresent the sold component [60]. The final type of counterfeit component is a tampered IC. Tampered components have malicious designs embedded in the package of the component or at the die level to cause undesired harm to the component or the system in which it was installed [60]. Tampered components could be a die level hardware Trojan designed to provide a back door for adversaries to access an unauthorized system [65]. This research primarily focused on the out-of-specification/defective, remarked, or tampered components as its source for counterfeit devices.

2.2.2 Counterfeit Detection.

There are several methods currently employed in an effort to detect a counterfeit component prior to installation into a system. There are positives and negatives to each approach. The following are different types of counterfeit detect methods which are non-destructive and do not provide electrical power to the device:

- External Visual Inspection
- Marking Permanency/Blacktop Examination
- X-Ray Inspection
- Energy Dispersive X-Ray Spectroscopy (EDS)
- X-Ray Fluorescence (XRF)
- Scanning Electron Microscopy (SEM)

The external visual inspection will double check that the part number matches accordingly and that the package and leads appear to be an authentic component. This type of inspection might catch counterfeit components but, as counterfeiting technology becomes increasingly sophisticated, it is unlikely that a external visual inspection will detect all counterfeits. Marking permanency or blacktop testing is a method for determining if a component has been remarked [66]. This process will dissolve the top layer of the IC package though the internal components remain operational. Component X-Rays can be used to verify the die within the component matches specifications of an authentic component. This does not however provide a fool proof method to ensure the die is in fact the correct die. This method merely ensures that there is a die and it matches dimensions. EDS can be used on suspected components to observe the chemical characteristics or elements which encompass a packaged component. EDS can be used when blacktops are composed of

different material than the underlying layers below. XRF is another non-destructive counterfeit identification technique which conducts a chemical elemental analysis of materials. XRF can be used to determine if a component with lead has be remarked as lead free. This is a huge concern since the European Union has enacted the Restriction of Hazardous Substances Directive and continues to enforce it [67]. In SEM the images of die, package, or leads are taken by scanning it with a focused beam of electrons similarly to EDS. SEM is excellent at identifying an anomaly present within the package [63]. All of the physical inspection methods can verify that the part looks like it should but cannot verify that the part behaves as it should.

One step closer to identifying a counterfeit part is to perform electrical tests on the component. There are other various types of electrical tests that can be conducted on suspected parts to verify authenticity. These types include:

- Direct Current (DC) testing
- Alternating Current (AC) testing
- Functionality testing
- RF-based signature detection

In DC testing, the voltage and current of the input/output pins are measured and compared to a known authentic. Typically this method only characterizes the input/output protection diodes near the pins. This method does not verify full functionality. AC testing involves observing the rise and fall times, set-up, hold, and release times, as well as propagation delay times [63]. AC testing can help verify that a component does in fact operate as the datasheet described. Functionality testing takes AC testing one step further and verifies that the component meets the operating characteristics described in the datasheet and that the function it is supposed

to perform is accurate through the ranges it is designed to operate. These three types of electrical testing can fully verify that a component can authentically operate as it is intended; however, to perform a full functionality test requires a large amount of time to conduct, especially if the part is a complex IC such as a Field-Programmable Gate Array (FPGA) IC.

A final emerging method to perform electrical testing is RF-based signature detection. This involves a process of extracting unique identifiable information from a type of RF-based signal. Commercial companies such as Power Fingerprinting, Inc., Battelle, and Nokomis, Inc. seek to create devices which can conduct RF-based or contact power on pin discrimination techniques. Battelle has developed a device referred to as Barricade which involves steady state information allowing characterization to be successful at a relatively low sampling rate and without requiring the component to be executing a pre-specified instruction [68]. The Battelle process requires contact on the pins. Power Fingerprinting, Inc. does not require access to the pins, but uses a course current probe that utilizes physical side channels to assess the integrity of an electronic device [69]. Nokomis, Inc. has developed the Advanced Detection of Electronic Counterfeits (ADEC) system which analyzes URE using non-contact methods to detect counterfeits. Patent filings suggest that the system may use a signal generator to stimulate a electrical component and then collect emitted RF energy using an antenna array [5, 70, 71]. The ADEC system is similar to what this research seeks to accomplish which is a non-contact, non-destructive approach for discriminating between authentic and counterfeit IC devices using RF-based techniques. RF-based signature analysis does not perform a full functionality test and is not a replacement for that type of testing. Merely, RF-based signature analysis seeks to provide a method of quickly classifying a component for a lower price than full functionality test. This research investigates the

use of RF-DNA combined with machine learning as a discrimination technique for such devices.

2.3 RF-Based Classification

Any type of machine learning classification algorithm requires a feature set or vector for each type of class considered. In the case of RF-DNA fingerprinting classification, these features are extracted from RF emissions and contain unique coloration attributable to the fabrication variance. This research utilizes the feature set of RF-DNA based upon collected URE from the DUT. Section 2.3.1 describes a few examples of RF-DNA's applications as well as what the RF-DNA features are attempting to describe about the DUTs. Section 2.3.2 provides information about the Multiple Discriminant Analysis/Maximum Likelihood (MDA/ML) classification process. Section 2.3.3 provides information about the Generalized Relevance Learning Vector Quantized-Improved (GRLVQI) classification process. Section 2.3.4 provides information about the Quadratic Discriminate Analysis (QDA) classification process. Section 2.3.5 provides information about the Random Forest (RndF) classification process.

2.3.1 RF-DNA Fingerprinting.

RF-DNA fingerprinting features are statistical features generated from time domain sampled RF emissions from any given type of device. As described in Section 2.1.1, the RF emission could be intentionally emitted such as a frequency modulated radio station signal or unintentionally emitted such as the RF emission directly above an operating IC. It is believed that the manufacturing process introduces variations in devices during die fabrication and packaging [19, 72]. These variations might be subtle and well within given tolerance such that the devices still

functions as intended. Since each device is unique, this information can be used to identify the devices.

Previous work at AFIT has successfully demonstrated the usability of RF-DNA in correctly classifying devices based upon their RF emissions. While various classification models were used, the feature set of RF-DNA remained consistent within the research. Some examples of past successful RF-DNA feature classification have been microcontroller units [5, 19], power-line communications devices [36], programmable logic controls [31], and wireless devices such as ZigBee [39] and WiFi routers [30].

The hypothesis proposed by this research is that since the physical layer characteristics that RF-DNA attempts to extract are inherently different from the manufacturing processes, then counterfeit devices which are manufactured differently than the part of which they are assuming the identity of would be physically different as well. Section 3.4.2 describes the RF-DNA feature generation used in this research.

2.3.2 MDA/ML Classifier.

Several different research topics produced at AFIT have paired MDA/ML with RF-DNA features [5, 19–37]. Multiple Discriminant Analysis (MDA) is defined as a generalized multi-class form of Fisher's Linear Discriminant Analysis (LDA). MDA relies upon the underlying assumption that each of the N_C classes can be described by a Gaussian distribution with equivalent covariance matrices, $\mathbf{\Sigma_i}$. Assuming each of the N_C classes has its own mean $\mu_\mathbf{i}$ and that the prior probabilities of each class is equivalent $\left(P(c_i) = \frac{1}{N_C}\right)$, then (2.1) describes the intraclass scatter matrix within each class and (2.2) describes the interclass scatter matrix between

each class [73].

$$\mathbb{S}_{\mathbb{W}} = \frac{1}{N_C} \sum_{i=1}^{N_C} \mathbf{\Sigma_i} \tag{2.1}$$

$$\mathbb{S}_{\mathbb{B}} = \frac{1}{N_C} \sum_{i=1}^{N_C} (\mu_\mathbf{i} - \mu)(\mu_\mathbf{i} - \mu)^T \tag{2.2}$$

If ${\mathbb{S}_{\mathbb{W}}}^{-1}\mathbb{S}_{\mathbb{B}}$ is diagonalizable, the variability between features will be contained in the subspace spanned by the eigenvectors corresponding to the N_C-1 largest eigenvalues. This produces a projection matrix $\mathbb{W}$ which maximizes interclass distance while minimizing intraclass variance [19, 73]. Figure 2.2 displays a pictorial representation of a $\mathbb{W}$ matrix for a three class classification example. If the RF-DNA features are formed into a N_{Feats}-dimensional vector $\mathbf{F}$, the individual RF-DNA features can be projected into the MDA space by (2.3).

$$\mathbf{F}_\mathbf{i}^{\mathbb{W}} = \mathbb{W}^T \mathbf{F} \tag{2.3}$$

Each of the features in the RF-DNA training set are used to determine a mean

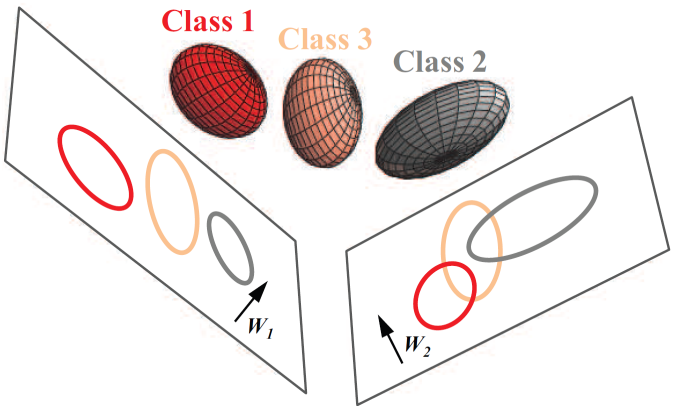


Figure 2.2. Representative MDA projection of $N_C = 3$ class inputs onto two possible $N_C - 1 = 2$-dimensional subspaces [74].

vector, $\hat{\mu}_\mathbf{i}^{\mathbb{W}}$, and covariance matrix for each of the classes, $\hat{\mathbf{\Sigma}}_\mathbf{i}^{\mathbb{W}}$. As stated earlier the covariance matrices of the classes are considered equivalent, therefore, the covari-

ance matrix is a pooled estimate in lieu of individual covariance matrices for each class, $\hat{\mathbf{\Sigma}}^{\mathbb{W}}$ [19, 73].

A RF-DNA feature vector from an unknown class is classified by MDA by first projecting the feature vector into the $\mathbb{W}$ matrix. A Maximum Likelihood (ML) comparison of each similarity score is conducted and the best match is selected. For each of the N_C classes, a $\mathbf{F}^{\mathbb{W}}$ is assigned a class c_i, where $i \in \{1, 2, \ldots, N_C\}$ and (2.4) is true.

$$P(c_i|\mathbf{F}^{\mathbb{W}}) > P(c_j|\mathbf{F}^{\mathbb{W}}) \quad \forall j \neq i \tag{2.4}$$

According to Bayes' Rule [75], the conditional probability is described by

$$P(c_i|\mathbf{F}^{\mathbb{W}}) = \frac{P(\mathbf{F}^{\mathbb{W}}|c_i)P(c_i)}{P(\mathbf{F}^{\mathbb{W}})}. \tag{2.5}$$

For any given RF-DNA feature vector, the probability $P(\mathbf{F}^{\mathbb{W}})$ is constant for every class, c_i, and can be neglected. Additionally, since the prior probabilities were assumed to be constant for all classes, $P(c_i) = \frac{1}{N_C}$, then $P(c_i)$ can be neglected in the final assessment as well [19]. Using (2.4) and (2.5), the decision criterion is reduced to maximizing $P(\mathbf{F}^{\mathbb{W}}|c_i)$. Formally, (2.6) describes the multivariate Gaussian distribution for each class.

$$P(\mathbf{F}^{\mathbb{W}}|c_i) = \frac{1}{(2\pi)^{\frac{(N_C-1)}{2}} \left|\hat{\mathbf{\Sigma}}^{\mathbb{W}}\right|^{\frac{1}{2}}} \exp\left(-\frac{1}{2}\left(\mathbf{F}^{\mathbb{W}} - \hat{\mu}_{\mathbf{i}}^{\mathbb{W}}\right)^T \hat{\mathbf{\Sigma}}^{\mathbb{W}-1}\left(\mathbf{F}^{\mathbb{W}} - \hat{\mu}_{\mathbf{i}}^{\mathbb{W}}\right)\right) \tag{2.6}$$

By plugging the density function into (2.5) and using (2.4), the Bayesian classifier assigns an observation to the class for which (2.7) is true [76].

$$c_i : \underset{i}{\operatorname{argmax}} \left\{ \mathbf{F}^{\mathbb{W}T} \hat{\mathbf{\Sigma}}^{\mathbb{W}-1} \hat{\mu}_{\mathbf{i}}^{\mathbb{W}} - \frac{1}{2} \hat{\mu}_{\mathbf{i}}^{\mathbb{W}T} \hat{\mathbf{\Sigma}}^{\mathbb{W}-1} \hat{\mu}_{\mathbf{i}}^{\mathbb{W}} + \log \frac{1}{N_C} \right\} \tag{2.7}$$

This MDA/ML process is the same process used in previous AFIT research con-

ducted with the DUT [56, 57].

2.3.3 GRLVQI Classifier.

Previous AFIT research has used the Artificial Neural Network (ANN)-based classification process of GRLVQI [24–31, 38]. GRLVQI refers to a self-organizing, supervised neural learning approach which learns input relevance weights for each data feature while conducting classification via a sigmoid cost function injunction with gradient descent [77–79]. Where MDA/ML assumes the input observations originate from a Gaussian distribution, GRLVQI has no inherent assumption or requirement for the input data distribution. Additionally, GRLVQI is not limited by linear algebra constraints such as the number of observations or the number of features.

A GRLVQI classification model is trained using a predefined number of prototype vectors, N_P, each comprised of the N_{Feats} features to represent each of the N_C classes [30]. Training begins by randomly generating a set of $\mathbf{p}^n$ prototype vectors used to form a matrix $\mathbf{P}$ of dimension $(N_C \cdot N_P) \times N_{Feats}$. GRLVQI iteratively minimizes Bayes risk by differentially shifting the best in-class and out-of-class prototype vectors by the distortion described in (2.8) where F_n is a randomly selected RF-DNA feature vector consisting of $n \in \{1, 2, \ldots, N_{Feats}\}$ features, $\mathbf{p}_n \in \mathbf{P}$ prototype vectors, and λ_n is the relevance of the n^{th} feature [30].

$$d_\lambda^j = \sum_{n=1}^{N_f} \lambda_n (\mathbf{F}_n - \mathbf{p}_n^j)^2 \tag{2.8}$$

The updating process continues for a predetermined number of iterations, N_I, or until the predetermined termination criteria is met. Upon completion, (2.9) describes the *best* relevance vector for the RF-DNA features and can be used to conduct future dimensional reduction of the RF-DNA feature vector. The *best* proto-

type vector matrix is given by $\mathbf{P}_B$.

$$\boldsymbol{\lambda}_B = [\lambda_1, \lambda_2, \ldots, \lambda_{N_{Feats}}] \tag{2.9}$$

Classification of an unknown RF-DNA feature vector, $\hat{\mathbf{F}}$ is accomplished by calculating the distance between the feature vector and each of the prototype vectors $\mathbf{p}_{i,n} \in \mathbf{P}_B$ where $i \in \{1, 2, \ldots, N_C\}$ classes and $j \in \{1, 2, \ldots, N_P\}$ prototype vectors. Equation (2.10) describes the calculation required to classify an unknown RF-DNA feature vector.

$$c_i : \underset{ij}{\operatorname{argmin}} \left(d_\lambda \left(\mathbf{p}_{i,j}, \hat{\mathbf{F}} \right) \right) \tag{2.10}$$

Figure 2.3 displays a representative example of classifying an unknown feature vector to class c_3 based upon minimum Euclidean distance to prototype vectors. This

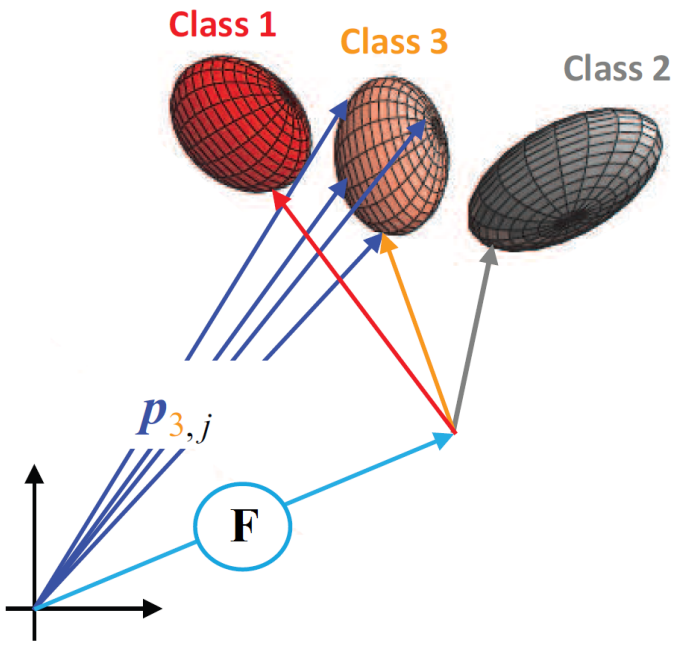


Figure 2.3. Representative GRLVQI classification assigning unknown feature vector, F, to class c_3 based upon the minimum Euclidean distance to prototype vectors [74].

GRLVQI process is the same process used in previous AFIT research conducted using the DUT [57].

2.3.4 QDA Classifier.

QDA is very similar to LDA where the classification process assumes that each observation originates from a multivariate Gaussian distribution. QDA differs in that it assumes that each class has its own covariance matrix and does not pool the estimates into a singular covariance matrix for all classes. Equation (2.11) displays an updated multivariate Gaussian distribution equation with the covariance matrix for the class given instead of the pooled estimate.

$$P(\mathbf{F}^{\mathbb{W}}|c_i) = \frac{1}{(2\pi)^{\frac{(N_C-1)}{2}}\left|\hat{\mathbf{\Sigma}}_i^{\mathbb{W}}\right|^{\frac{1}{2}}}\exp\left(-\frac{1}{2}\left(\mathbf{F}^{\mathbb{W}}-\hat{\mu}_{\mathbf{i}}^{\mathbb{W}}\right)^T\hat{\mathbf{\Sigma}}_i^{\mathbb{W}-1}\left(\mathbf{F}^{\mathbb{W}}-\hat{\mu}_{\mathbf{i}}^{\mathbb{W}}\right)\right) \tag{2.11}$$

By plugging the updated density function into (2.5) and using (2.4), the Bayesian classifier assigns an observation to the class for which (2.12) is true [76].

$$c_i : \underset{i}{\text{argmax}}\left\{-\frac{1}{2}\mathbf{F}^{\mathbb{W}T}\hat{\mathbf{\Sigma}}_i^{\mathbb{W}-1}\mathbf{F}^{\mathbb{W}}+\mathbf{F}^{\mathbb{W}T}\hat{\mathbf{\Sigma}}_i^{\mathbb{W}-1}\hat{\mu}_{\mathbf{i}}^{\mathbb{W}}-\frac{1}{2}\hat{\mu}_{\mathbf{i}}^{\mathbb{W}T}\hat{\mathbf{\Sigma}}_i^{\mathbb{W}-1}\hat{\mu}_{\mathbf{i}}^{\mathbb{W}}-\frac{1}{2}\log|\hat{\mathbf{\Sigma}}_i^{\mathbb{W}}|+\log\frac{1}{N_C}\right\} \tag{2.12}$$

Unlike the linear decision criteria, the term $\mathbf{F}^{\mathbb{W}T}\hat{\mathbf{\Sigma}}_i^{\mathbb{W}-1}\mathbf{F}^{\mathbb{W}}$ has a quadratic component associate with it hence quadratic in lieu of linear discriminate analysis. Figure 2.4 displays the decision boundary differences between linear and quadratic when both LDA and QDA are conducted on a scatter plot of two different classes with a comparison using two RF-DNA features. This QDA process is the same process used in previous AFIT research conducted using the DUT [57].

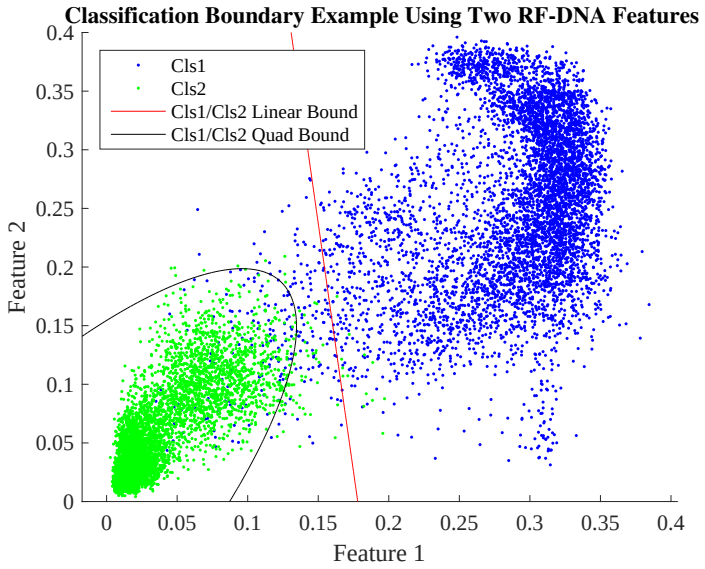


Figure 2.4. Representative example of linear and quadratic boundaries on a scatter plot of two classes with two RF-DNA features.

2.3.5 Random Forest Classifier.

Classification can be accomplished by using a decision tree based approach. Previous AFIT research has combined RF-DNA features and decision tree based classification [39, 80]. A single decision tree involves segmenting the feature space into a number of regions by conducting a decision on the RF-DNA features which generate nodes. The nodes are split on a set of criterion. To accomplish this, the decision tree calculates the weighted impurity, I_t, of a node t using the Gini impurity index [81]. The Gini impurity, I_t, of node t is calculated by (2.13) where the sum is over all the classes, $i \in \{1, 2, \ldots, N_C\}$, and the observed fraction of classes, $h(i)$, with class i that reach the node. A *pure* node has only one class associated with it and an associated Gini impurity index of $I_t = 0$.

$$I_t = 1 - \sum_{i=1}^{N_C} h^2(i) \tag{2.13}$$

An estimate of the probability that an observation is in node t is accomplished using (2.14) where T is a the set of all observations in node t and the number of observations within the node is defined as $N_{\text{Node Sample Size}}$.

$$P(T) = \sum_{k \in T} \frac{1}{N_{\text{Node Sample Size}}} \tag{2.14}$$

The single decision tree determines the best way to split a node t by maximizing the impurity gain ΔI over all splitting candidates which are the RF-DNA features. A node is split into left, t_L, and right, t_R, child nodes each containing a set of observations T_L and T_R respectively. The impurity gain, δI, is calculated using [39, 80]:

$$\Delta I = P(T)I_t - P(T_L)I_{t_L} - P(T_R)I_{t_R}. \tag{2.15}$$

A decision is made to split the node based on the candidate which yields the maximum impurity gain [82]. A single decision tree is not a robust decision making process. A small change in input data can cause a large delta in the final estimated tree. This is referred to as a high variance model [76].

To combat high variance, several methods have been expanded upon using the RndF process. RndF grows an ensemble of N_{Trees} and the final prediction is the majority vote of the ensemble's class choice. Additionally in single decision trees, each node is split using the best split among all of the N_{Feats} RF-DNA features. In a random forest, each node is split using the best among a subset of features randomly chosen at that node [83]. The split is only allowed to use one of the m predictors that were randomly selected from the original feature set with replacement where m is limited by $m \approx \sqrt{N_{Feats}}$ [76]. Using a random selection of features to split each node yields low error rates that are more robust with respect to noise, decorrelates the decision trees within the ensemble, and due to the Law of Large

Numbers they do not overfit to noise [84]. This RndF process is the same process used in previous AFIT research conducted using the DUT [57].

2.4 Dimensional Reduction of RF-DNA Features

The ability to determine which RF-DNA features greatly affect the discrimination process can be beneficial when conducting dimensional reduction analysis. If a majority of the classification can be accomplished with a smaller subset of the features, then the computational complexity can be reduced. Previous research has used the best relevance vector developed during the GRLVQI classification process [30, 31]. This research seeks to accomplish a qualitative feature set dimensional reduction by conducting model development on the strict subsets of instantaneous amplitude, frequency, and phase RF-DNA features. Additionally, this research explored an additional method of reduction by use of Forward Stepwise Selection (FSS). FSS is a computationally efficient version of best subset selection. Best subset selection fits a least squares linear regression model for each possible combination of the N_{Feats} RF-DNA features [76]. This generates $2^{N_{Feats}}$ different models for each combination of features. Best subset selects the best model for each of the M_n where $n \in \{1, 2, \ldots, N_{Feats}\}$ based upon having the smallest Residual Sum of Squares (RSS). This orders the best subsets of models based upon number of features used $\{M_1, M_2, \ldots, M_{N_{Feats}}\}$. $M_{N_{Feats}}$ has all of the features ordered by smallest RSS. FSS is different compared to best subset selection in that FSS adds predictors to a model one at a time instead of searching the entire $2^{N_{Feats}}$ combinations. This reduces the computational component from $2^{N_{Feats}}$ combinations to $\frac{N_{Feats}(N_{Feats}+1)}{2}$ combinations [76]. However, RSS is a better metric for regression instead of classification and it can overfit to noise. For the purpose of this research, FSS is used to observe what would happen in classification as the features are re-

duced to a subset of the features ordered in $M_{N_{Feats}}$.

2.5 MAX526CCWG Device Description

The DUT for this research is the MAX526CCWG Digital-to-Analog Converter (DAC) which are manufactured by Maxim Integrated. The DUT contains four double-buffered interface digital logic components with a 12-bit input register and a 12-bit voltage-output DAC. Data are loaded into the one of the four input registers using two write operations with an 8-bit least significant bit write load signal and a 4-bit most significant bit write load signal. An asynchronous Load Digital-to-Analog Converter (LDAC) input transfers data from the input register to the DAC register. All logic inputs are Transistor-Transistor Logic (TTL) and Complementary Metal-Oxide-Semiconductor (CMOS) compatible [85].

The MAX526CCWG can be used for many applications: minimum component count analog systems, digital offset/gain adjustment, arbitrary function generators, industrial process controls, and automatic test equipment [85]. As reported in 2016 by IHS Markit, counterfeit converters make up around 5% of the reported counterfeit parts with memory and programmable logic IC devices contributing to the top two types of 31% of the overall reports [59]. The MAX526CCWG was selected for this research as a representation of a mixed-signal IC and an example of a converter IC. Additionally, this component is of interest to the US Government and Department of Defense (DOD) organizations.

III. Methodology

In order to extract relevant Unintentional RF Emission (URE) from the Device Under Test (DUT), power and digital timing logic must be applied to the Integrated Circuit (IC). This chapter outlines the methodology used in this research to generate the results presented in Chapter IV. Section 3.1 describes the operating conditions used to generate the URE that were collected. Section 3.2 details the configuration of the URE collection system. Section 3.4 outlines the process used to generate the necessary statistical RF Distinct Native Attribute (RF-DNA) features from the collected URE. Section 3.5 provides an overview of the model generation process for each classifier. Section 3.6 describes the methods and processes used to classify and evaluate devices to generate the results presented in Chapter IV. Section 3.7 provides the method in which various subsets of features were selected as a method of dimensional reduction. Section 3.8 describes the various reduced sample rates evaluated by this research. Section 3.9 provides the classification and verification process used on the DUT and the updated device MAX526CCWG+.

3.1 MAX526CCWG Operating Conditions

This section provides details about the conditions in which the MAX526CCWG devices were operated during URE acquisitions. The devices were mounted onto a custom designed Printed Circuit Board (PCB). A Field-Programmable Gate Array (FPGA) was used to generate the test vectors needed to exercise the DUT functions.

3.1.1 Custom Printed Circuit Board.

A custom PCB was designed to provide the necessary digital logic, Direct Current (DC) power, and representative output loads to the devices. The PCB was designed according to information determined from the datasheet provided by Maxim Integrated [85]. The DUT was exchanged on the PCB using a Small Outline Integrated Circuit (SOIC) to Dual In-line Package (DIP) adapter [86] and a 24-pin Zero-Insertion Force (ZIF) DIP test socket [87]. This process ensured that the Radio-Frequency (RF) emissions from the PCB were held constant as a control so that the URE collected from devices can be contributed to the devices themselves and not the PCB. A BK Precision 9130 Triple Output Programmable DC Power Supply [88] provided DC power to the DUT via header pins on the PCB. Table 3.1 displays the voltage and current limitations as determined by the datasheet [85], as well as the power supply values used in this research. If a current value was maxed out, the voltage dropped to match the impedance of the circuit. A picture of the PCB is displayed in Figure 3.1.

Table 3.1. Voltage and current limits and power supply values as determined by DUT's datasheet [85].

Designated Pin	**Voltage**			**Current**		
	Min	Max	Set Value	Min	Max	Set Value
V_{DD}	10.8V	16.5V	15.0V	-	28mA	28mA
V_{SS}	-4.5V	-5.5V	-5.0V	-	26mA	26mA
V_{REF}	0V	(V_{DD}-4)V	10V	-	-	50mA

3.1.2 FPGA.

The digital timing logic was accomplished via a custom made state machine written in Very High Speed Integrated Circuit Hardware Description Language (VHDL). The VHDL state machine was loaded onto the Altera Cyclone V System on Chip (SoC) FPGA. The FPGA utilized a High Speed Mezzanine Card (HSMC)

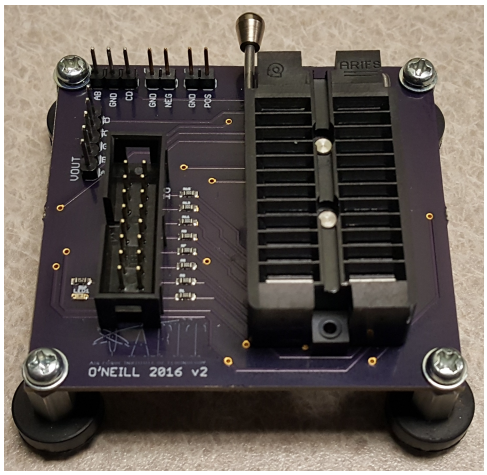


Figure 3.1. Custom PCB used to provide power, digital logic, and output loads to the DUT.

connector in combination with a General Purpose Input/Output (GPIO) daughter board to output the digital pins. Figure 3.2 displays the FPGA and Daughter Board used in this research. The digital pins were connected to the PCB via a ribbon cable. Figure 3.3 displays the digital timing logic of the state machine,

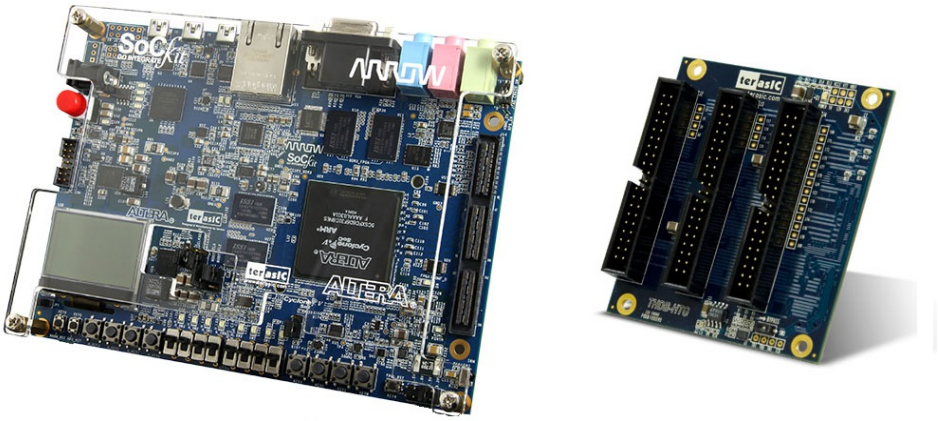


Figure 3.2. Altera Cyclone V SoC FPGA [89] and GPIO Daughter Board Attachment [90].

which was designed in accordance with timing limits specified in the datasheet [85] and loaded onto the FPGA. The state machine initialized all output registers to zero. After initialization, the address control bits were assigned to output 'A' and

data pins were held constant at zero for the duration of URE collections. The Load Digital-to-Analog Converter (LDAC) signal displayed in Figure 3.3 refers to the digital logic provided to the Load Digital-to-Analog Converter (DAC) pin on the DUT, which shall be referred to as the DUT clock. The DUT clock has a frequency of $f_{DUTclk} \approx 0.7353\ MHz$.

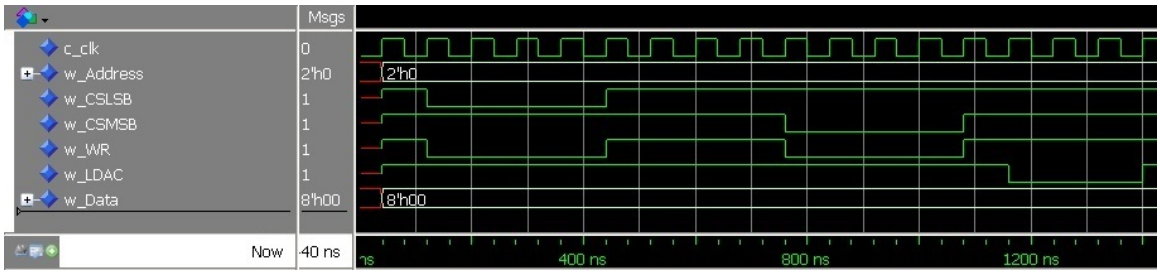


Figure 3.3. Model-Sim simulation of the digital timing logic within the limits specified by the datasheet. The signal names correlate to the pin names as determined by the MAX526 datasheet [85]. The FPGA clock is f_clk = 25 MHz or t_clk = 40 ns.

3.1.3 Evaluated Devices.

To effectively conduct research concerning counterfeits, two classes of ICs were considered: a set that passed tests and were determined to be authentic (suspected authentic) and those that failed the tests are were determined to be counterfeit or non-authentic in some manner (suspect counterfeit). $N_{SC} = 9$ suspected counterfeit devices and $N_{SA} = 9$ suspected authentic devices were purchased from an independent organization after an extensive counterfeit detection process was conducted. The counterfeit detection process encompassed such procedures as visual inspection, Scanning Electron Microscopy (SEM), elemental analysis, and decapsulation of one sample from the lot. The $N_{SA} = 9$ suspected authentic devices passed the company's counterfeit detection process; conversely, the $N_{SC} = 9$ devices failed the process. To verify the authenticity and counterfeit nature of the devices, a functionality test was conducted on each device where output 'A' of the device was mea-

sured when the device was operated to full value of the reference voltage (V_{OUTA} $\approx$ 10.0 V). The DUTs outputs are based off of operational amplifiers with negative feedback [85]. To account for variations in output loads and possible floating point values, all outputs were loaded with a 5 kΩ resistor and a 100 pF capacitor in parallel. Additionally, the voltage and current supplied from the power supply was recorded for each device when the device was given the digital data inputs to output V_{OUTA} $\approx$ 0.0 V

Table 3.2. The N_{SA} = 9 suspected authentic devices with their respective power values. The part number labeled on all devices is MAX526CCWG. The text appears as red if the current value was maxed out or if it failed a functionality test.

Name	Date Code	V_{DD} (Volts)	I_{DD} (mA)	V_{REF} (Volts)	I_{REF} (mA)	V_{SS} (Volts)	I_{SS} (mA)	Function Test
G1	9433	14.998	14	9.999	0	-4.999	4	Pass
G2	9433	14.998	15	9.999	0	-4.999	4	Pass
G3	9433	14.998	11	9.999	0	-4.999	5	Pass
G4	9433	14.998	10	9.999	0	-4.999	7	Pass
G5	9433	15.000	10	9.999	0	-4.999	5	Pass
G6	9433	15.000	14	9.999	0	-4.999	4	Pass
G7	9433	14.999	10	9.999	0	-4.999	6	Pass
G8	9433	15.000	12	9.999	0	-4.999	3	Pass
G9	9433	15.000	13	9.999	0	-4.999	4	Pass

Table 3.3. The N_{SC} = 9 suspected counterfeit devices with their respective power values. The part number labeled on all devices is MAX526CCWG. The text appears as red if the current value was maxed out or if it failed a functionality test.

Name	Date Code	V_{DD} (Volts)	I_{DD} (mA)	V_{REF} (Volts)	I_{REF} (mA)	V_{SS} (Volts)	I_{SS} (mA)	Function Test
C1	0437	1.190	29	2.815	50	-0.104	26	Fail
C2	0437	2.959	29	3.197	50	-0.146	26	Fail
C3	0437	14.997	2	6.165	50	-0.233	25	Fail
C4	0437	15.000	2	9.999	0	-4.999	2	Fail
C5	0437	14.999	1	9.999	0	-4.999	12	Fail
C6	0437	2.551	29	2.513	50	-0.141	25	Fail
C7	0437	14.999	27	9.999	29	-0.343	25	Fail
C8	0437	14.999	0	9.999	0	-4.999	0	Fail
C9	0437	1.504	28	1.620	49	-0.011	25	Fail

Table 3.2 displays the following information for each authentic DUT labeled as

part number MAX526CCWG: power values, the date code, whether or not the device passed the functionality test, and the designated name used in this research. All of the authentic devices were manufactured in 1994 and all appeared to be functioning as expected. Table 3.3 displays the following information for each counterfeit DUT labeled as part number MAX526CCWG: power values, the date code, whether or not the device passed the functionality test, and the designated name used in this research. All of the counterfeit devices failed the functionality test and the power was not within specification on most devices. This confirmed that the devices are in fact not authentic. The counterfeit devices of "C4" and "C5" had power values within operating limits but failed to function. "C8" did not draw any current through any of the pins. It is expected that "C8" is an open circuit such that the die is not connected to the pins within the package.

In addition to the certified devices, 19 MAX526CCWG+ devices were purchased from two separate distributors. The current part number MAX526CCWG is obsolete and was replaced with MAX526CCWG+. The '+' symbol denotes the lead free version of the MAX526CCWG. Table 3.4 displays the following information for each open market device labeled as part number MAX526CCWG+: power values, the date code, whether or not the device passed the functionality test, and the designated name used in this research. Devices with the "D" preface were purchased from one distributor and devices with the "M" preface were purchased from a different distributor.

Table 3.4. Open Market devices with their respective power values. The part number labeled on all devices is MAX526CCWG+. The text appears as red if the current value was maxed out or if it failed a functionality test. These devices were purchased from two separate distributors.

Name	Date Code	V_{DD} (Volts)	I_{DD} (mA)	V_{REF} (Volts)	I_{REF} (mA)	V_{SS} (Volts)	I_{SS} (mA)	Function Test
D1	1537	14.999	11	9.999	0	-4.999	8	Pass
D2	1537	14.998	14	9.997	0	-4.999	5	Pass
D3	1537	14.999	10	9.999	0	-4.999	6	Pass
D4	1537	14.999	10	9.999	0	-4.999	6	Pass
D5	1537	14.999	10	9.999	0	-4.999	8	Pass
D6	1537	15.000	10	9.999	0	-4.999	7	Pass
D7	1537	14.999	10	9.999	0	-4.999	6	Pass
D8	1441	14.999	10	9.999	0	-4.999	6	Pass
D9	1537	14.999	11	9.999	0	-4.999	5	Pass
D10	1537	15.000	10	9.999	0	-4.999	5	Pass
M2	1512	14.999	9	9.999	0	-4.999	4	Pass
M3	1512	14.998	9	9.997	0	-4.999	5	Pass
M4	1512	14.999	9	9.999	0	-4.999	5	Pass
M5	1512	14.999	11	9.999	0	-4.999	7	Pass
M6	1512	14.998	9	9.997	0	-4.999	5	Pass
M7	1512	14.999	9	9.999	0	-4.999	5	Pass
M8	1512	14.998	10	9.999	0	-4.999	6	Pass
M9	1512	14.999	10	9.999	0	-4.999	6	Pass
M10	1512	14.999	9	9.999	0	-4.999	5	Pass

3.2 RF Signal Collection

This section provides details of the hardware collection system used to collect the URE from a grid scan above each device.

3.2.1 Acquisition System.

A computer controlled XYZ table was used to secure a Riscure high-sensitivity RF near-field probe positioned above the DUT [91]. The near-field probe was lowered upon the surface of the DUT package and a metal shroud was lowered around the probe tip to mitigate the effects from the surrounding environment. The PCB was secured in place via a custom printed mount shown in Figure 3.4. This acqui-

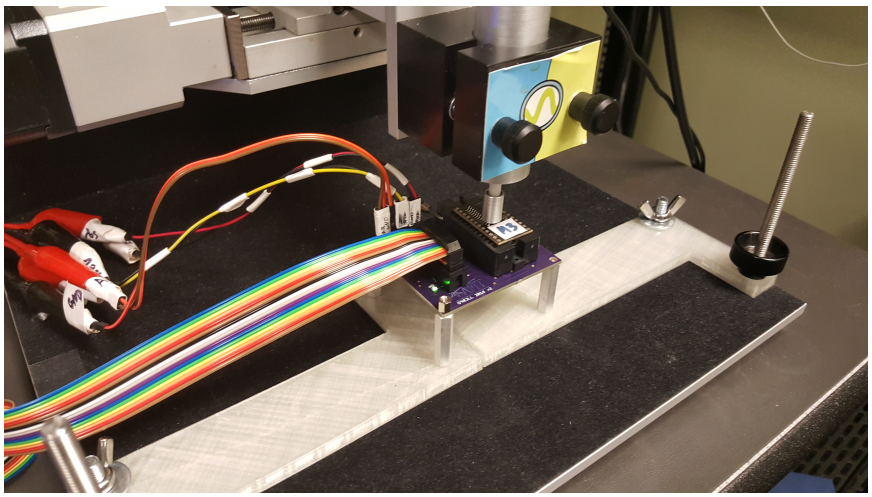


Figure 3.4. XYZ table, RF near-field probe, and DUT in custom mount used for URE collection. This is the same acquisition system used in [56, 57].

sition system is the same system used in previous Air Force Institute of Technology (AFIT) research [56, 57] and remained constant for all collections, only the DUT was exchanged on the PCB.

The RF near-field probe was sampled using a Teledyne LeCroy WavePro® 760Zi-A oscilloscope with 8-bits of resolution at a sample rate of $f_S = 10$ Giga-samples per second (GSps). The LeCroy WavePro® 760Zi-A oscilloscope is capable of sample rates up to $f_{Smax} = 40$ GSps and a bandwidth of $\mathrm{W_{Max}} = 6$ GHz [92]. A coaxial Mini-Circuits BLP-90+ Low Pass Filter (LPF) with a designed passband of $\mathrm{W_{LPF}} = [\mathrm{DC}, 81\mathrm{MHz}]$ and a nominal -3 dB cutoff frequency of $f_{CO} = 90$ MHz was used to prevent aliasing by placing the filter in-line between the RF near-field probe and the oscilloscope [93]. The measured frequency response of Mini-Circuits BLP-90+ Coaxial LPF with nominal -3 dB cutoff frequency is $f_{CO} \approx 96.8$ MHz [5, 93] using a network analyzer under previous AFIT research [5, 94]. All collections and signal processing were accomplished using MATLAB® software. In order to maintain consistency, the DUT clock was used as the trigger to initiate collections.

3.2.2 RF Near-Field Probe Placement.

To begin each collection, the near-field probe was placed on the bottom left corner of the DUT. An arbitrary grid of 30 spaces horizontally by 50 spaces vertically was overlaid on top of each device. Each grid scan consisted of $N_{DUT} = 30 \times 50 =$ 1,500 emissions per device. Figure 3.5 displays the arbitrary grid of a DUT. The near-field probe is mechanically moved to each location via the XYZ table shown in Figure 3.4. Each square represents the average power of a single collected URE using the trigger as a collection start and stop operation to maintain consistence between collections. The colormap displayed in Figure 3.5 is a visual representation of the average power of each URE. The maximum average power is found and the entire grid is normalized to that value seen in Figure 3.5 as the bright yellow section.

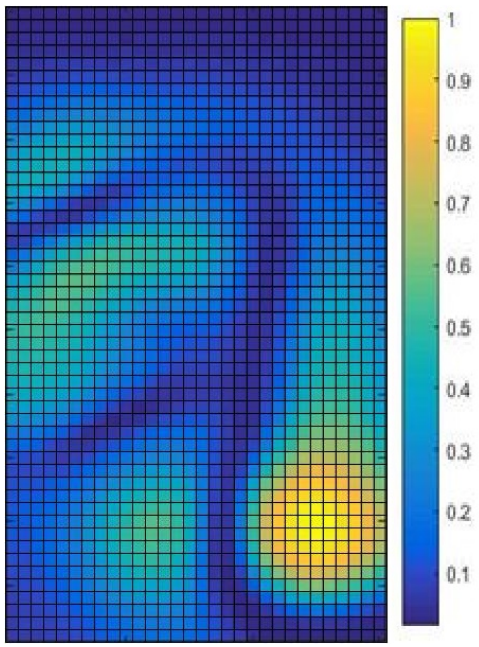


Figure 3.5. A representative 30×50 grid scan overlaid on a colormap of normalized average power emitted from the DUT.

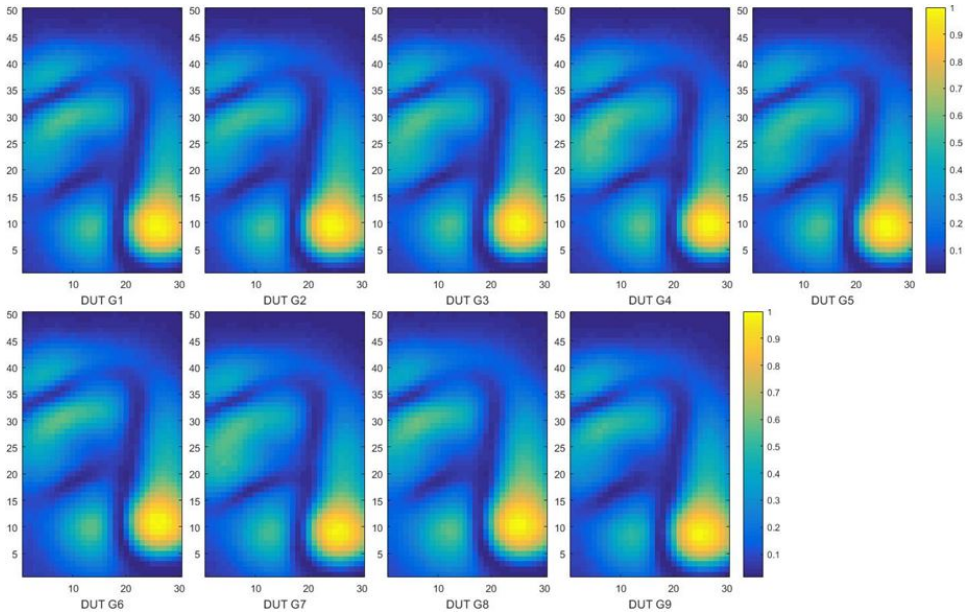


Figure 3.6. Normalized average power colormaps for each of the $N_{SA} = 9$ suspected authentic DUTs based on a 30×50 grid scan of acquisitions.

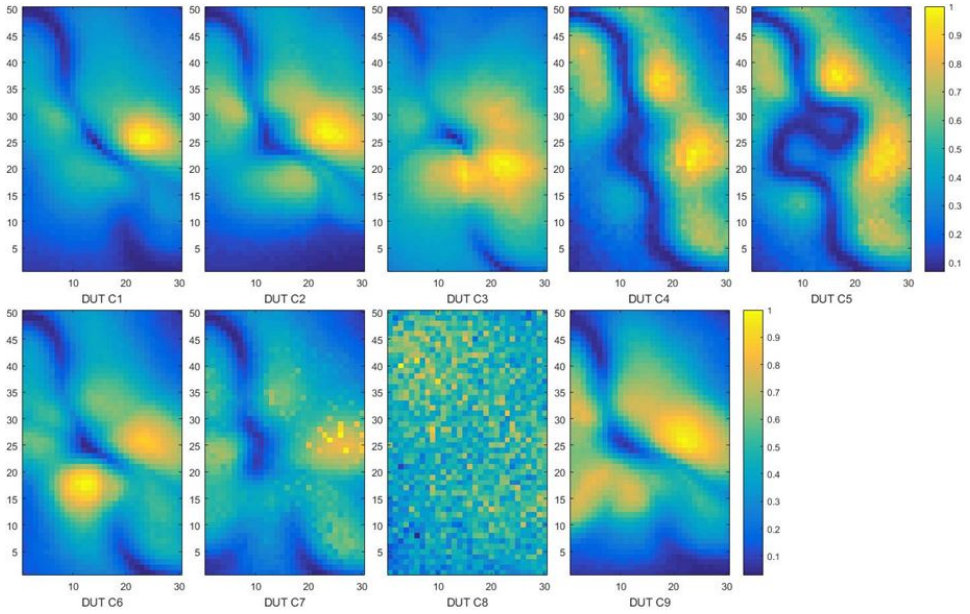


Figure 3.7. Normalized average power colormaps for each of the $N_{SC} = 9$ suspected counterfeit DUTs based upon a 30×50 grid scan of acquisitions.

The colormap visual representation was accomplished on all authentic and counterfeit devices. Figure 3.6 displays the nine authentic devices and their colormap

grid scans. Visually, all of the devices appear similar. Figure 3.7 displays the nine counterfeit devices and their colormap grid scans. Each device appears different especially when compared to the authentic devices. Device "C8" appears to not have a defined RF emission output pattern which further justifies that the device might be an open circuit.

3.3 Class Selection

To help mitigate the uniqueness created by each individual device, a subset of four devices were selected from the available authentic and counterfeit devices. The entire set was not used as this would not allow evaluation of the model on device that were not used in the model development process. The subset "Class 1" consists of the devices "G6", "G7", "G8", and "G9". The subset "Class 2" consists of the corresponding counterfeit devices "C6", "C7", "C8", and "C9". Figure 3.8 displays the subset selection of devices for each class.

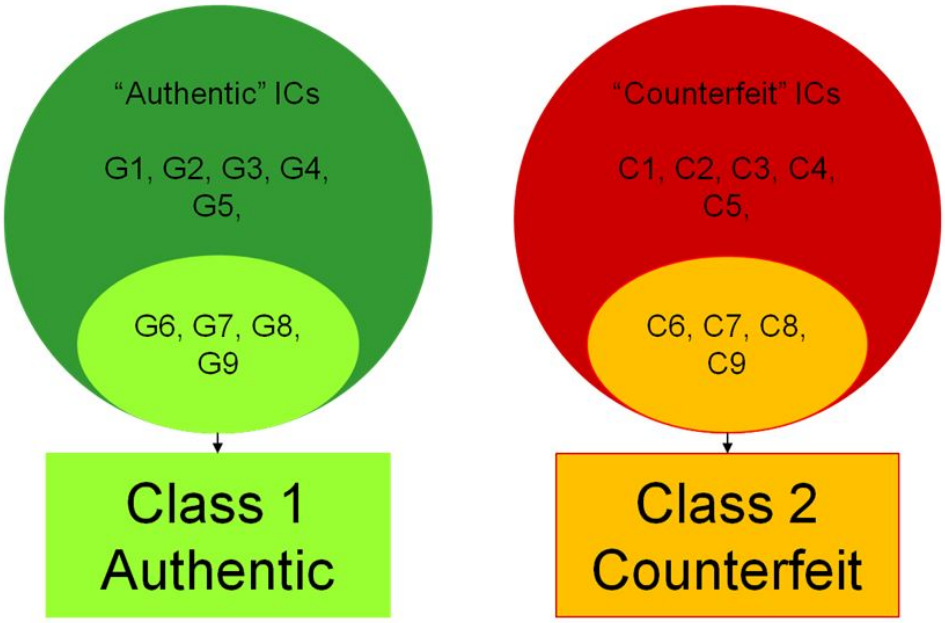


Figure 3.8. Visual representation of the subset selection into separate classes.

These devices were X-Rayed in an attempt to observe the die and pin layout to help distinguish the devices and help confirm authenticity. Figure 3.9 displays the different devices used in the classes and their respective die layouts. The suspected authentic devices {"G1", "G2", ..., "G9"} with a date code of 9433 have a significantly different die layout than the suspected counterfeit devices {"C1", "C2", ..., "C9"} marked with the date code of 0437.

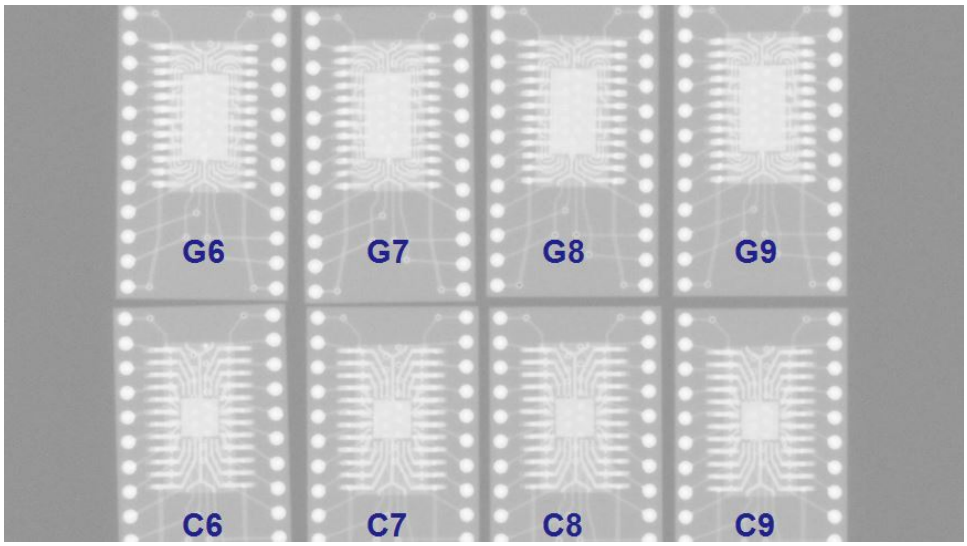


Figure 3.9. X-Ray of the four "G" devices used for the authentic class, Class 1, and the four "C" devices used for the counterfeit class, Class 2.

3.4 Post-Collection Processing

This section provides the details of how collected emissions were manipulated to observe the effect of Signal-to-Noise Ratio (SNR) on the classification and verification process. Additionally, this section elaborates on the generation of the RF-DNA features that are used in the classification and verification process.

3.4.1 SNR Scaling.

Each collected URE was isolated using the trigger waveform, the DUT clock, as a reference. The collected SNR of the devices was approximated by selecting the maximum power within the 30×50 grid, and dividing by an equivalent amount of like-filtered background noise without DC power or digital logic signals applied to the DUT. Equation (3.1) shows the calculation of the collected SNR. The background noise power, P_{Bkd} was calculated by taking the average of 1,000 independent collections of the same sample size as the collected URE, $P_{Bkd} \approx 1.33$ mW. Figure 3.10 displays the various background noise powers to generate the average background noise power. The maximum power of the collected signals within the 30×50 for a given device was $P_{Collected+Noise} = 162.3$ mW. The collected SNR was calculated as $\text{SNR}_\text{C} \approx 20$ dB using (3.1).

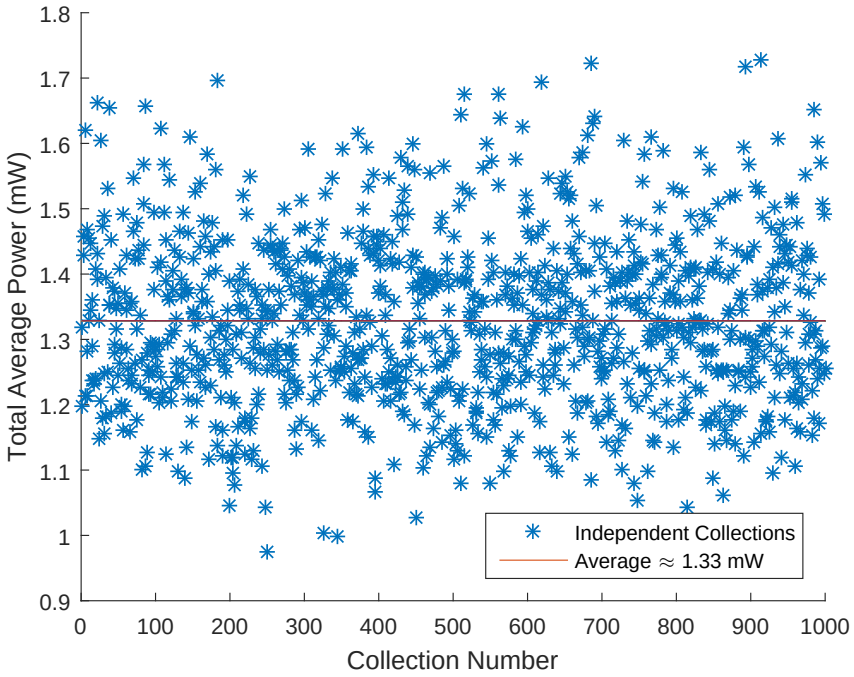


Figure 3.10. Total average power values for 1,000 background collections with the average of $P_{Bkd} \approx 1.33$ mW

$$SNR_C = \frac{max_{ingrid}(P_{Collect+Noise}) - P_{Bkd}}{P_{Bkd}} \tag{3.1}$$

Simulated SNRs were used to evaluate the impact of SNR on the classification and

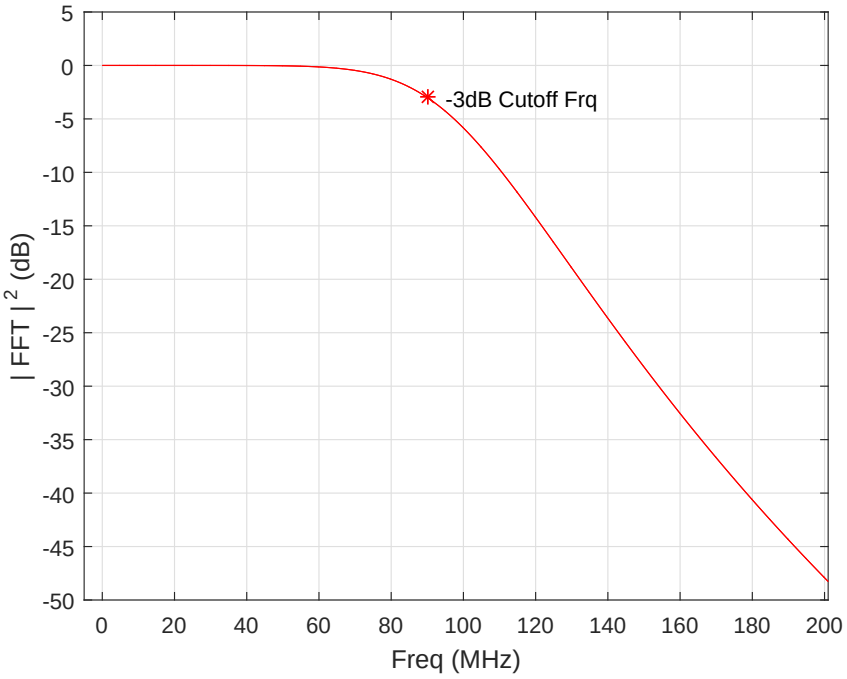


Figure 3.11. Simulated frequency response of 8th-order Butterworth LPF with cutoff frequency designed for f_{CO} = 90 MHz.

verification process. Previous work has shown a Gaussian distribution to be an appropriate model to use in this research [95]. The signal power was estimated then one instance of like-filtered Additive White Gaussian Noise (AWGN), $N_{Nz} = 1$, was generated, filtered, power scaled appropriately, and added to the isolated collected URE to achieve $\text{SNR}_S \in [-30, 30]$ dB in $\text{SNR}_{\Delta S} = 3$ dB intervals.

Each independent noise realization was drawn from a normal distribution using MATLAB's® `randn` function which independently draws a number from a uniform pseudo-random number generator. The noise was filtered using a digital LPF. Figure 3.11 displays the normalized frequency response of the 8th-order phase pre-

serving digital Butterworth LPF used to simulate the in-line, coaxial Mini-Circuits BLP-90+ LPF used during URE collections. The filtered noise power was scaled appropriately to achieve the desired SNR_S values.

3.4.2 RF-DNA Feature Generation.

The Region of Interest (ROI) for each collected URE response is the isolated samples using the DUT clock as a trigger. Consistent with prior research, the ROI was divided into $N_{Subregion} = 45$ equal length subregions [56, 57]. Subdividing the ROI into equal length, sequential subregions isolates transient regions which could show the highest variations between devices. Figure 3.12 displays a single collected URE and the corresponding subregions.

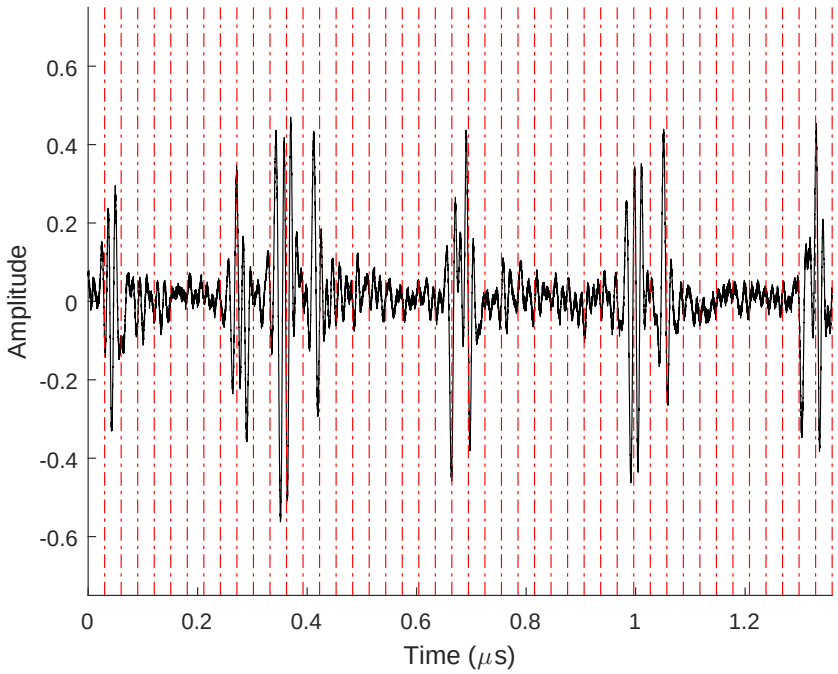


Figure 3.12. Example of one collected URE divided into $N_{Subregion} = 45$ equal duration, contiguous subregions for fingerprint.

In order to classify each class a set of unique features are required. RF-DNA

features were calculated for each ROI using Time Domain (TD) statistical characteristics in accordance with previous AFIT research [5, 19, 30, 31, 56, 57]. The RF-DNA feature generation technique requires complex signals having In-phase and Quadrature-phase (IQ) samples. The URE used in this research were collected as real-valued TD samples; the MATLAB® `hilbert` function was used to generate complex IQ samples from the real-valued collected URE. The `hilbert` function in MATLAB® returns a complex time analytic signal representation of the discrete Hilbert transform with In-phase components being the original input sequence and the imaginary Quadrature-phase components being the input sequence with a 90° phase shift [51, 96]. Equation (3.2) displays the nomenclature of the IQ representation for future use in this paper.

$$s_{IQ}[n] = s_{re}[n] + j s_{im}[n] \tag{3.2}$$

The instantaneous amplitude (Amp), phase (Phz), and frequency (Frq) responses were calculated for each complex signal. Equation (3.3) describes the calculation used to generate the instantaneous amplitude $a[n]$ of the complex signal $s_{IQ}[n]$. The instantaneous amplitude and phase calculations were mean centered and normalized by subtracting the mean instantaneous value and then dividing the samples by the max value within each instantaneous calculation. The instantaneous frequency was normalized but was not mean centered.

$$a[n] = \sqrt{s_{re}^2[n] + s_{im}^2[n]} \tag{3.3}$$

Equation (3.4) describes the calculation used to generate the instantaneous phase

$\phi[n]$ of the complex signal $s_{IQ}[n]$.

$$\phi[n] = \tan^{-1}\left[\frac{s_{im}[n]}{s_{re}[n]}\right], s_{re} \neq 0 \tag{3.4}$$

Equation (3.5) describes the calculation used to generate the instantaneous frequency $f[n]$ of the complex signal $s_{IQ}[n]$.

$$f[n] = \frac{1}{2\pi}\left[\frac{d\phi[n]}{dn}\right] \tag{3.5}$$

The statistical characteristics of standard deviation (σ), variance (σ^2), skewness (γ), and kurtosis (k) were calculated for each of the $N_{Subregions} = 45$ as well as the total ROI on the three instantaneous responses of ROI. Standard deviation and variance are both used as previous research has shown standard deviation to be a discriminable feature for the DUT [57]. For use in all statistical features, (3.6) displays how the mean of a region was calculated, N represents the total number of samples in that region, and A represents the values of the signal within that region. Standard deviation was calculated using (3.7). Variance was calculated using (3.8). Skewness was calculated using (3.9). Kurtosis was calculated using (3.10).

$$\mu = \frac{1}{N}\sum_{i=1}^{N} A[n] \tag{3.6}$$

$$\sigma = \sqrt{\frac{1}{N}\sum_{i=1}^{N} |A[n] - \mu|^2} \tag{3.7}$$

$$\sigma^2 = \frac{1}{N}\sum_{i=1}^{N} |A[n] - \mu|^2 \tag{3.8}$$

$$\gamma = \frac{1}{N\sigma^3}\sum_{i=1}^{N} (A[n] - \mu)^3 \tag{3.9}$$

$$k = \frac{1}{N\sigma^4}\sum_{i=1}^{N}(A[n]-\mu)^4 \tag{3.10}$$

The total number of statistical RF-DNA features is $N_{Feats} = 4$ statistical calculations $\times$ 3 instantaneous responses $\times$ ($N_{Subregions}$ + total ROI) $= 552$ RF-DNA features. The $N_{Feats} = 552$ RF-DNA features were combined in to a single vector as shown in (3.13).

$$\mathbf{F}_{Subregion} = \left[\sigma, \sigma^2, \gamma, k\right] \tag{3.11}$$

$$\mathbf{F}_{Instantaneous\ Response} = \left[\mathbf{F}_{Subregion1}, \mathbf{F}_{Subregion2}, \ldots, \mathbf{F}_{Subregion45}, \mathbf{F}_{TotalRegion}\right] \tag{3.12}$$

$$\mathbf{F}_{\mathbf{Features}} = \left[\mathbf{F}_{Instantaneous\ Amplitude}, \mathbf{F}_{Instantaneous\ Phase}, \mathbf{F}_{Instantaneous\ Frequency}\right] \tag{3.13}$$

3.5 Model Development

Each "Class" subgroup contained four DUTs as described in section 3.3 and collectively had a total number of RF-DNA feature observations, $N_{ClsObs} = 4 \times N_{DUT} = 6,000$ observations per class. The total number of observations used in classification, $N_{Total} = 2 \times N_{ClsObs} = 12,000$ observations. N_{Total} is divided into two equal sets: the training set $N_{Training} = 6,000$ observations and the testing set $N_{Testing} = 6,000$ observations. Both have an equal number of observations from each class, Class 1 and Class 2. The Multiple Discriminant Analysis/Maximum Likelihood (MDA/ML), Generalized Relevance Learning Vector Quantized-Improved (GRLVQI), Quadratic Discriminate Analysis (QDA), and Random Forest (RndF) models were generated using a K-fold Cross-Validation (CV) process with $N_{Training} = 6,000$ observations. For each of the classification techniques, a new model was developed for each of the 21 different SNR values within $\text{SNR}_S \in [-30, 30]$ in $\text{SNR}_{\Delta S} = 3$dB intervals. The testing set is held out from the model

development process and was used to validate the model.

3.5.1 K-Fold Cross Validation.

One model development CV process that is known for reducing bias is Leave-One-Out Cross-Validation (LOOCV). If $N_{Obs} = N_{Training}$ as the total number of observations available, LOOCV builds a model based off of N_{Obs}-1 observations and uses that held-out observation to test against the model. This process is repeated until all observations have been held out [76]. The model with the highest accuracy is then selected as the model. LOOCV is very computationally intensive as the model development is directly proportionate to the number of observations. An alternative to LOOCV is K-fold CV which is computationally less intensive but still provides some means of reducing model development bias.

In K-fold CV, the observations are divided into K equal groups or folds. A similar process from LOOCV is performed where the K-1 groups are used to develop a model and the held out K group is used to test against a model. The model with the highest accuracy is then selected. To maintain consistency with previous research, $K = 5$ for the K-fold CV was used in this research [56, 57]. $K = 5$ was selected in accordance with previous recommendations to use $K = 5$ or $K = 10$ when LOOCV or larger K values is not computationally efficient [97].

3.5.2 MDA/ML and QDA Generation.

As stated in Section 2.3, the MDA/ML classification process produces a projection matrix, $\mathbb{W}$, that projects the RF-DNA feature vector, $\mathbf{F}$, onto a $N_C - 1$ dimensional space [98]. For this research, the number of classes is defined as $N_C = 2$ and the length of the $\mathbf{F}$ vector is number of features used in the RF-DNA process, $N_{Feats} = 552$ features. This process is similar to previous AFIT research

[5,19,31,56,57]. Similarly, The difference between MDA/ML and QDA is the covariance matrix. Where MDA/ML creates a pooled estimate of the covariance matrix, QDA assumes that each class has its own covariance matrix [76].

3.5.3 GRLVQI Generation.

Previously described in Section 2.3, the GRLVQI model used $N_P = 10$ prototype vectors consisting of $N_{Feats} = 552$ RF-DNA features to define each of the $N_C = 2$ classes. The updating process for (2.8) used in this research is $N_I = 600$ iterations or until criteria for termination was satisfied.

3.5.4 Random Forest Generation.

The MATLAB® `TreeBagger` function was used to generate the forest model used for classification in this research. The `TreeBagger` function builds a series of decision trees based upon the criteria described in Section 2.3.5. The number of trees built for this research is $N_{Trees} = 100$ trees. A similar k-fold CV was used on the RndF in lieu of using the out-of-bag estimates of the model to maintain consistency with the other models generated for comparison purposes.

3.5.5 Model Evaluation.

As the RF-DNA feature vector, $\mathbf{F}$, is manipulated by the various classification models, a test statistic, z_V, is assigned to an observation corresponding to how much the given vector resembles each of the possible N_C classes. The class that corresponds to the highest probability is decided upon as the class the observation belongs to, correctly or incorrectly. To evaluate the various generated models, this research valued two criterion for determination of best model. The first criteria is the model that generates an average percent correct classification ($\%C$), $\%C \geq 90\%$,

at the lowest possible SNR value shall be determined as the *best* model for this criteria. The second criteria used is the model that generates the highest $\%C$ shall be determined as the *best* model for this criteria. If a single model does not have both criteria, the first criteria of determining the arbitrary $\%C \geq 90\%$ at the lowest SNR is weighted higher since this can be interpreted as better discrimination with more noise present within the evaluated observation. If none of the models achieve the $\%C \geq 90\%$ criteria, the model with the highest $\%C$ shall be chosen for this research. The model evaluation is performed on the held out testing set which consisted of $N_{Testing} = 6,000$ observations. Once a classification model was chosen, that model was used for the verification, subset feature selection, and reduced sample rate analysis presented in Chapter IV of this paper.

3.6 Verification Evaluation

Once a model development process was chosen, the first SNR value within the range SNR_S where $\%C \geq 90\%$ was selected as the model that will be used in the verification process or the model with the highest $\%C$ if the criterion in Section 3.5.5 are not met. Verification is a one-verses-one comparison of new observations. New observations were collected for all of the authentic and counterfeit devices which included the devices that were used to train and test the model. New collections from devices "G1"-"G9" and "C1"-"C9" were collected, scaled appropriately to the SNR value selected, and the RF-DNA features were calculated and placed in a '*rogue*' F vector. This research refers to these new observations as '*rogues*' to represent the observations as coming from unknown devices posing as authentic devices. To accomplish this, all '*rogue*' devices are claiming to be from "Class 1", the authentic device class. The purpose of verification is to verify the claimed identity of a device using a previously determined threshold measuring a *difference* between

a presented identity and the stored reference identity.

Model verification is performed by analyzing the metrics of True Verification Rate (TVR) and False Verification Rate (FVR) for each of the held out testing set observations claiming to be the class to which the devices originated from. TVR is the rate at which a device or class is claiming its true identity as defined within the scope of the model and the model identifies it correctly. The False Rejection Rate (FRR) corresponds to 1 - TVR. FVR is the rate at which a device or class is claiming a different identity than its own and the model incorrectly identifies it from its true identity. The True Rejection Rate (TRR) corresponds to 1 - FVR.

'*Rogue*' assessment is performed by analyzing the TVR and the Rogue Accept Rate (RAR). The RAR is the rate at which a rogue device or class is claiming to be the identity it is not and the model incorrectly identifies it as the claimed device or class. RAR is synonymous with FVR. The term used to describe the rejection rate of the '*rogue*' devices is Rogue Rejection Rate (RRR) which is equivalent to 1 - RAR. Table 3.5 elaborates on the model verification terminology.

Verification performance is documented using a Receiver Operating Characteristics (ROC) curve which is generated by comparing FVR versus TVR or RAR versus TVR. TVR is calculated based upon generating a Probability Mass Func-

Table 3.5. Combinations of actual and claimed identities for device verification with the corresponding outcomes and verification rates based on the accept/reject decision. Correct decisions are highlighted in green and incorrect decisions are highlighted in red [5].

Actual Identity	Claimed Identity	Decision	Outcome	Verification Rate
Auth$B$	Auth$B$	Accepted	True Verification	$TVR = 1 - FRR$
Auth$B$	Auth$B$	Rejected	False Rejection	$FRR = 1 - TVR$
Auth$A$	Auth$B$	Accepted	False Verification	$FVR = 1 - TRR$
Auth$A$	Auth$B$	Rejected	True Rejection	$TRR = 1 - FVR$
Rogue$C$	Auth$B$	Accepted	Rogue Acceptance	$RAR = 1 - RRR$
Rogue$C$	Auth$B$	Rejected	Rogue Rejection	$RRR = 1 - RAR$

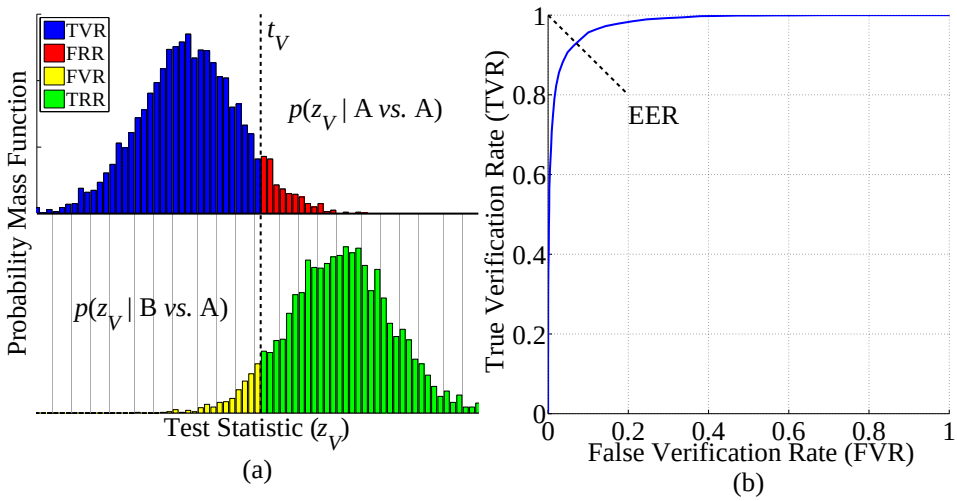


Figure 3.13. Representative (a) PMFs of test statistic, z_V, values for "A vs. A" (blue/red) and "B vs. A" (yellow/green) comparisons with (b) the corresponding ROC curve for *authorized device verification*. The verification rate regions are color coded with accepted z_V values on the left side of t_V and rejected z_V values on the right side of t_V. The shown threshold, t_V, corresponds to the EER [5].

tion (PMF) of the test statistic, z_V. Each point on the ROC is a representation of varying the verification threshold, t_V, across the PMF. Figure 3.13 displays a representative PMF and the corresponding regions described earlier in this section, as well as a ROC curve generated from those PMFs [5]. For an actual device claiming its actual identity or for this research an authentic device claiming to be in the authentic "Class 1" (A vs. A), the values for TVR and FRR can be calculated. Similarly comparing other devices against the claimed identity or for this research counterfeit devices from "Class 2" claiming to be in the authentic "Class 1" (B vs. A), the values for FVR and TRR can be calculated. t_V is varied across the range of the PMF bins and the percentage of z_V values are calculated accordingly. The Equal Error Rate (EER) t_V is class dependent for each of the N_C classes. The point at which FRR = FVR is referred to as the EER. In the case for this research effort, EER could represent the point at which the user is allowing a certain amount of devices to be mislabeled as either counterfeit or authentic.

3.7 Feature Subset Selection

Once a classification model was selected, the process of generating and testing models was repeated for various combinations of feature subsets. Classification using the best classifier process was compared with a subset of features consisting of the features from exclusively instantaneous amplitude, phase, or frequency each consisting of $N_{InstFeats} = 184$ features. This was used to observe which of the instantaneous features was most influential in classification. Additionally, a subset of features generated from the entire signal, with no subregions, was accomplished consisting of $N_{WholeRegionFeats} = 12$ features to observe the effects of not subdividing the collected URE. A subset of features was also generated which consisted of the variance (σ^2), skew (δ), and kurtosis (k) for the instantaneous amplitude for each region resulting in $N_{NoStdDevFeats} = 138$ features. Since variance is statistically the second moment, removing standard deviation (σ) will show the effect of sign change from the mean on classification. Finally, features comprised of only the four, $N_{FSS} = 4$, most relevant features extracted from Forward Stepwise Selection (FSS) when SNR = 0 dB, were compared to the other subsets of features [57]. A 95% confidence interval was used to determine statistical equivalence between the averages for each subset. The 95% Confidence Interval (CI) was calculated using (3.14) where p is defined as the mean error, or 100% minus the average between "Class 1" and "Class 2", and n is the total number of observations used to generate that value, $n = N_{Testing} = 6,000$ [99].

$$CI = p \pm \sqrt{\frac{p(1-p)}{n}} \tag{3.14}$$

3.8 Reduced Sample Rate

This research explored the option of reducing the sample rate, f_S, via post-processing decimation. The model development and testing was conducted at various decimation factors which correspond to various sampling rates. Filtering was not conducted again as all of the reduced sample rates were sampled above the cut-off frequency of the LPF. The decimation was conducted after AWGN generation and scaling to the collected URE. The feature generation was conducted on the new reduced sampled regions. Decimation was conducted in steps of 10. The reduced sampling rates which were observed were: $f_{ReducedS}$ = [1000, 500, 333, 250, 200, 166, 143] MSps. The original number of samples in each subdivided region for f_{Samp} = 10 GSps is $N_{Samples}$ = 302 samples. For the reduced sample rates, the reduced number of samples per subdivided region is $N_{ReducedS}$ = [30, 15, 10, 7, 6, 5, 4] samples.

3.9 Die Layout Classification

The robustness of the RF-DNA features are tested with a new classification model. This model compares the same devices used in the authentic class, "Class 1", to four randomly selected devices chosen from Table 3.4. The four devices were "D1", "D5", "M2", and "M7" and shall be referred to as the newer die class. The classification model was trained and tested using the same methods described in Section 3.5. This test is to observe how the classification process holds up to changes associated with the die encased within the package. Figure 3.14 displays four devices from each of the different discriminating factors associated with this research: authentic class, counterfeit class, distributor 1, and distributor 2. Both distributors devices "M6" and "D6" appear to have the same die layout; however, each device is from a separate lot production as indicated by their different date codes in Ta-

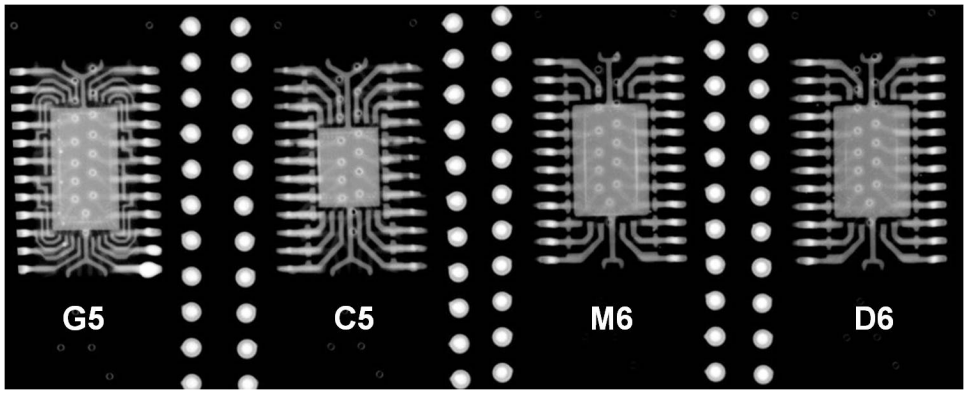


Figure 3.14. X-Ray of four devices from each of the different groups: authentic ("G5"), counterfeit ("C5"), distributor 1 ("M6"), and distributor 2 ("D6").

ble 3.4. The date codes indicate that the devices purchased from the two distributors are 20 years newer than the authentic class devices. Additionally the chemical composition has changed to a lead-free design.

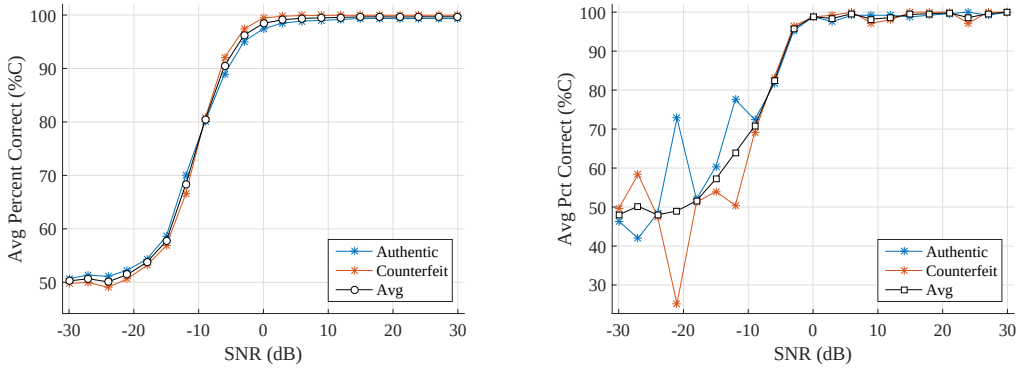
IV. Results

The results dictated within this chapter represent the culmination of previous Air Force Institute of Technology (AFIT) research conducted using the Device Under Test (DUT) [56, 57]. These results used the methodology described in Chapter III. Chapter IV provides the results for class classification in Section 4.1 using the different models described in Chapter III. Section 4.2 describes the verification of all devices against the best classification model process chosen in Section 4.1. Section 4.3 displays the results of model classification using different subsets of the features available from Chapter III. Section 4.4 presents the results of reducing the sample rate by means of post-collection decimation. Section 4.5 presents the results of part level discrimination based upon die layouts.

4.1 Class Classification

Four different models were developed and tested against using the methodology described in Chapter III. Average percent correct classification ($\%C$) across the two separate classes was used to determine the best model using the criterion described in Section 3.5. Figure 4.1 displays the held out testing set results of the $N_{Feats} = 552$ RF Distinct Native Attribute (RF-DNA) features using the (a) Multiple Discriminant Analysis/Maximum Likelihood (MDA/ML) classification process, (b) Generalized Relevance Learning Vector Quantized-Improved (GRLVQI) classification process, (c) Quadratic Discriminate Analysis (QDA) classification process, and (d) Random Forest (RndF) classification process. MDA/ML had a maximum $\%C = 99.67\%$ occurring at Signal-to-Noise Ratio (SNR) $\geq$ 18dB. The value at which $\%C \geq 90\%$ occurred when SNR = -6 dB. GRLVQI had a max $\%C = 100\%$ occurring at SNR = 30 dB. The value at which $\%C \geq 90\%$ occurred when SNR = -

3 dB. For GRLVQI when SNR = -21 dB, there is an observed variation between the two classes which can be attributed to classifier favoring the Authentic class over the Counterfeit class. However, $\%C$ between the classes still maintains an expected trend. QDA had a max $\%C = 99\%$ occurring at SNR = 9 dB. The value at which $\%C \geq 90\%$ occurred when SNR = -3 dB. RndF had a max $\%C = 99.43\%$ occurring at SNR = 30 dB. The value at which $\%C \geq 90\%$ occurred when SNR = -3 dB [57].



(a) MDA/ML (b) GRLVQI

(c) QDA (d) RndF

Figure 4.1. Classification results using all $N_{Feats} = 552$ RF-DNA features of the held out testing set at each of the SNR values within the SNR_S range for both the authentic class, "Class 1", and the counterfeit class, "Class 2", as well as the average of the two classes. The models are arranged as (a) MDA/ML, (b) GRLVQI, (c) QDA, and (d) RndF [57].

Figure 4.2 displays $\%C$ for each of the four different models. Comparing the results, MDA/ML was selected as the model of choice for this research due to hav-

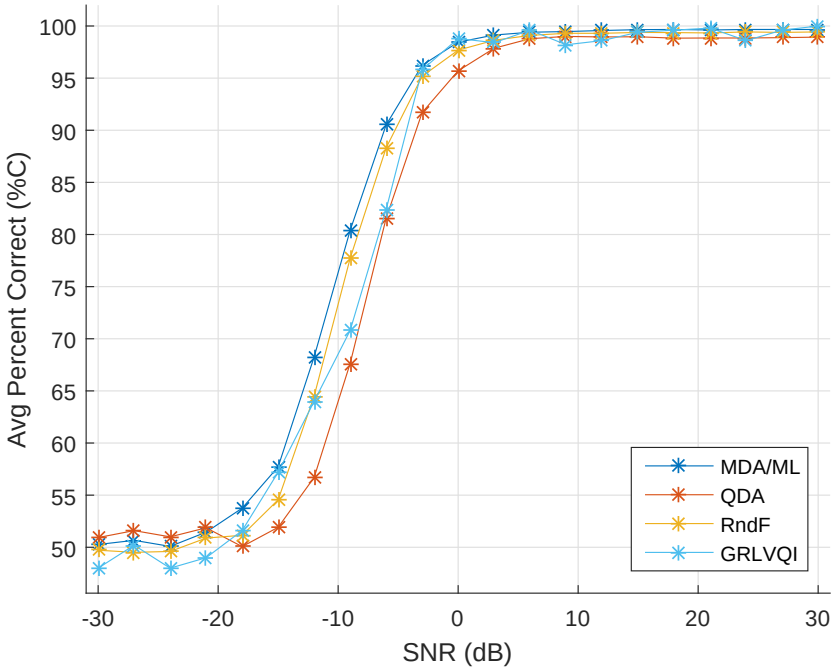


Figure 4.2. Consolidated average percent correct classification between authentic class, "Class 1", and counterfeit class, "Class 2", at each of the SNR values within the SNR$_S$ for each of the four models: MDA/ML, GRLVQI, QDA, and RndF. [57]

ing the lowest SNR value, SNR = -6 dB, where $\%C \geq 90\%$ as well as a maximum value of $\%C = 99.67\%$ occurring at SNR $\geq$ 18 dB.

4.2 Class Verification

Figure 4.3 displays the model development process that was selected in Section 4.1 as the best process. Using the SNR dependent models developed during the MDA/ML process, the model where SNR = -3dB shall be used to conduct verification on all of the devices identified in Table 3.2, Table 3.3, and Table 3.4. This model was selected since both classes achieved a $\%C \geq 90\%$ at this SNR value. The arbitrary benchmark consistent with previous AFIT research [5, 19, 31], $\%C \geq 90\%$, occurred when SNR = -6 dB; however, the authentic "Class 1" $\%C = 89\%$ when SNR = -6 dB.

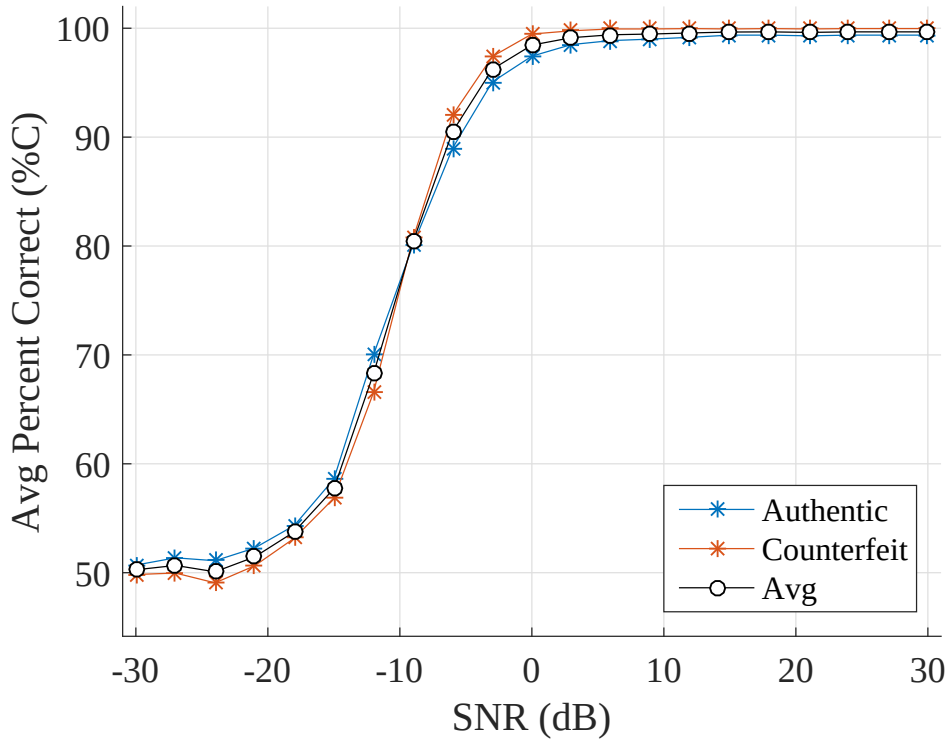


Figure 4.3. MDA/ML classification results using all $N_{Feats} = 552$ RF-DNA features of the held out testing set at each of the SNR_R values for both the authentic class, "Class 1", and the counterfeit class, "Class 2", as well as the average of the two classes.

To demonstrate verification performance for this SNR dependent model, Figure 4.4 displays the Receiver Operating Characteristics (ROC) curve for the testing and training RF-DNA features when the observations were claiming to be from the class to which the observations originated. Performance as measured by the False Verification Rate (FVR) vs True Verification Rate (TVR) ROC curve is acceptable when the Equal Error Rate (EER) is less than 10% (as indicated by the region in the dashed box). The dashed box represents the arbitrary benchmark of correct classification $\%C \geq 90\%$. The EER occurred when TVR = 0.9647 or 96.47% and FVR = 0.0353 or 3.53%. Verification was conducted upon all devices identified in this research.

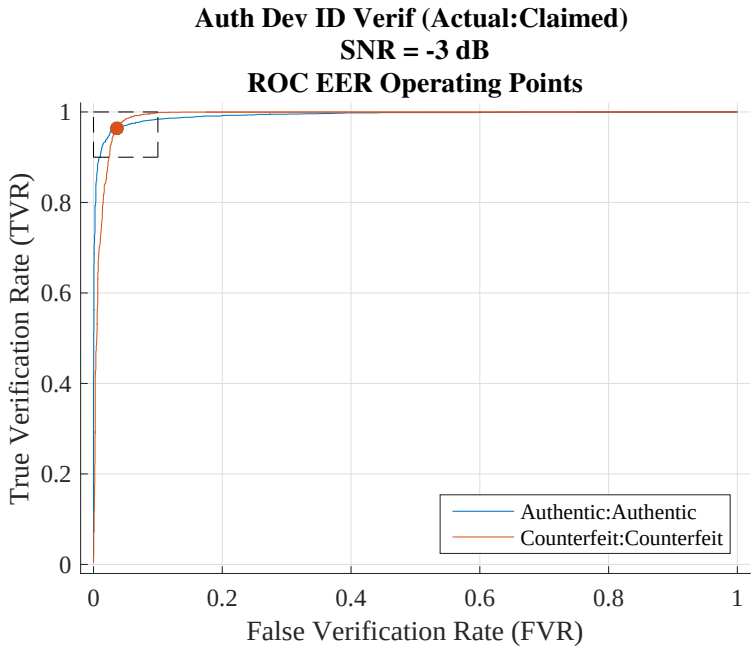


Figure 4.4. Verification results of held out testing set against the MDA/ML model at SNR = -3dB with each class's claimed identity being the class to which they belong.

All devices are identified as '*rogue*' and are claiming to be from the authentic class to represent counterfeit devices claiming to be the authentic part number. Figure 4.5 displays the verification results of the RF-DNA features extracted from 3,000 new observations, or one grid scan, with one simulated noise realization per observation scaled appropriately to a SNR = -3 dB for all of the authentic devices from Table 3.2 ("G1" - "G9"). The average Rogue Rejection Rate (RRR) for all nine devices is RRR = 4.9%. To describe this differently, on average 95.1% of the observations for the nine devices were classified as authentic. Five new devices were introduced to the model in addition to four new scans of the devices that were used to generate the model and correct classification only dropped approximately 96.47% - 95.1% = 1.37%. The blue dot on the graph represents the TVR value from the EER displayed in Figure 4.4.

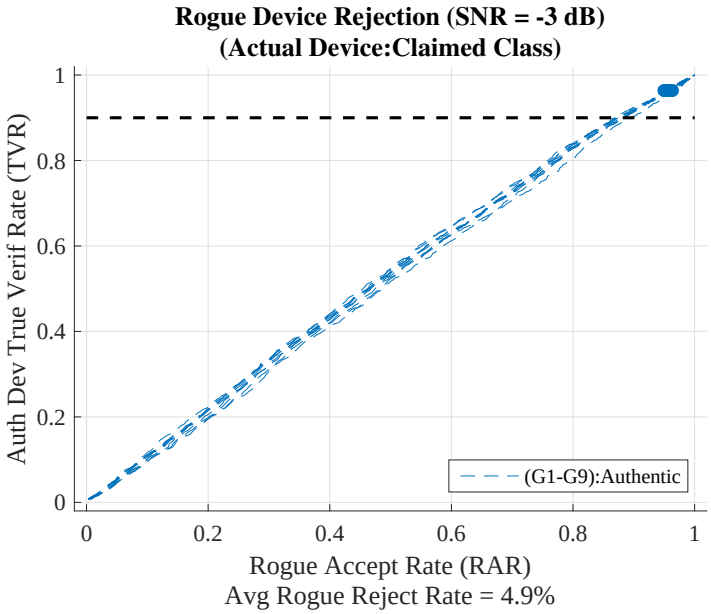


Figure 4.5. Verification results of testing 3,000 new observations per device using the MDA/ML model at SNR = -3dB when all of the authentic devices ("G1"-"G9") are unknown, rogue devices claiming to be authentic devices.

Similarly to the devices from Table 3.2, Figure 4.6 displays the verification results of the RF-DNA features extracted from 3,000 new observations, or one grid scan, with one simulated noise realization per observation scaled appropriately to a SNR = -3 dB for all of the counterfeit devices from Table 3.3 ("C1" - "C9"). The average RRR for all nine devices is RRR = 98.63%. All devices crossed the 90% dashed threshold line before Rogue Accept Rate (RAR) $\geq$ 10%.

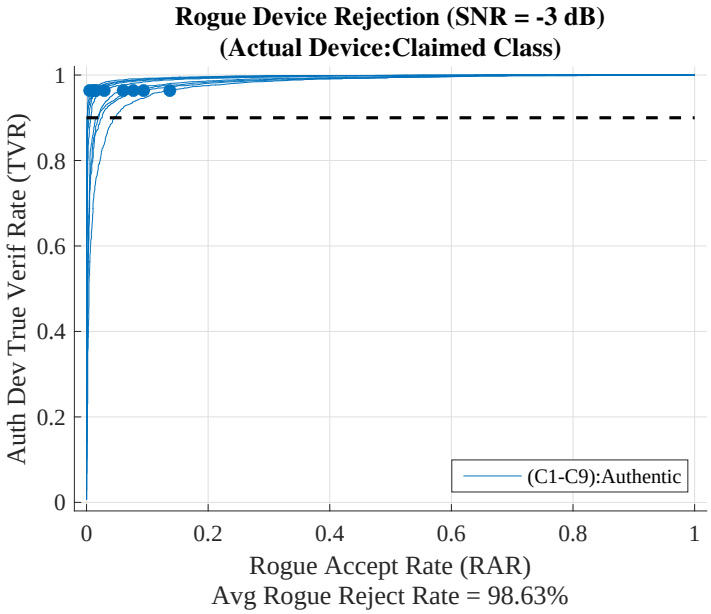


Figure 4.6. Verification results of testing 3,000 new observations per device using the MDA/ML model at SNR = -3dB when all of the counterfeit devices ("C1"-"C9") are unknown, rogue devices claiming to be authentic devices.

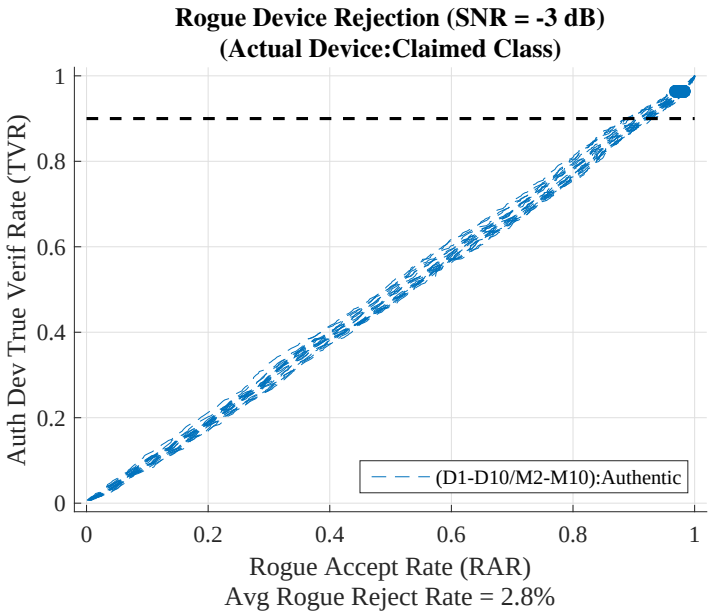


Figure 4.7. Verification results of testing 1,500 new observations per device using the MDA/ML model at SNR = -3dB when all of the 19 devices ("D1"-"D10" and "M2"-"M10") are unknown, rogue devices claiming to be authentic devices.

The blue dots represents the TVR value from the EER displayed in Figure 4.4 and if the threshold values were set for the EER operating point, device "C3" would have a RAR = 13.63% and would not meet the the TVR $\geq$ 90% and RAR $\leq$ 10% limits.

The values contained within Table 3.4 indicate that the unknown devices are expected to be authentic when compared to "Class 1". Figure 4.7 displays the verification results of the RF-DNA features extracted from 1,500 new observations, or one grid scan, with one simulated noise realization per observation scaled appropriately to a SNR = -3 dB for all of the unknown devices purchased from two separate distributors from Table 3.4 ("D1" - "D10" and "M2" - "M10"). The average RRR was 2.8% between all 19 devices.

Based upon the results of Table 3.4 and the findings in Figure 4.7, it is the determination of this research that the classification model developed in Figure 4.3 can accurately determine between the functional and non-functional devices selected in this research.

4.3 Feature Subset Selection

New MDA/ML models were constructed with a reduced subset of RF-DNA features according to Section 3.7. Of these models, the averages between the authentic class, "Class 1", and the counterfeit class, "Class 2", were recorded for each SNR value for each different subset of features. A 95% Confidence Interval (CI) was calculated for each average value for subset of features to assess statistical equivalence; however, the CIs are omitted from figures to improve visual clarity. Figure 4.8 displays the average percent correct classification between authentic class, "Class 1", and counterfeit class, "Class 2", at various SNR values using a reduced number of features as dictated by the legend.

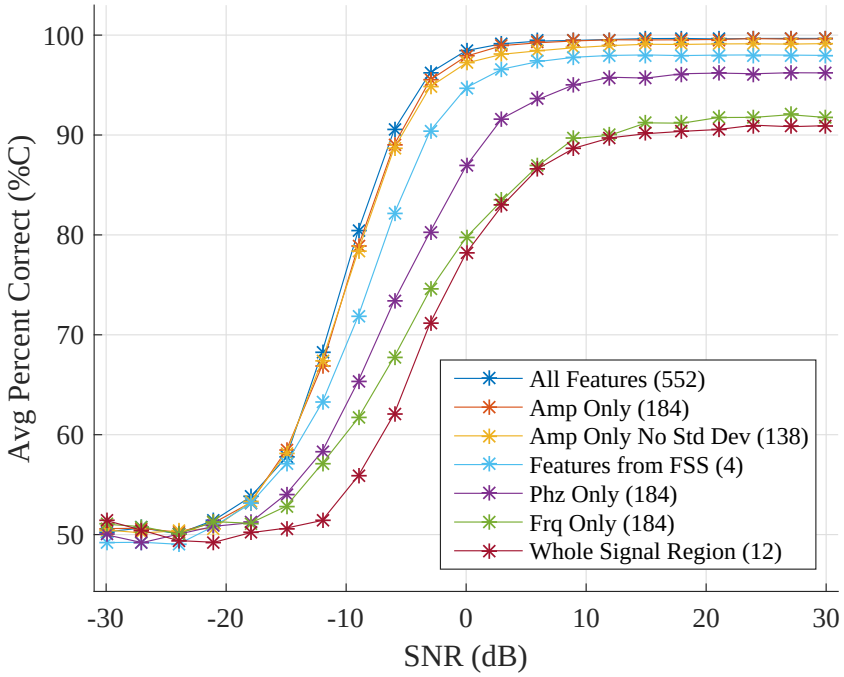


Figure 4.8. Average percent correct classification between authentic class, "Class 1", and counterfeit class, "Class 2", at various SNR values using a reduced number of features as dictated by the legend. [57]

The subsets consisting of the original feature set (N_{Feats} = 552 RF-DNA features), the instantaneous amplitude only feature set ($N_{InstFeatsAmp}$ = 184 RF-DNA features), and the modified instantaneous feature set which did not contain standard deviation ($N_{NoStdDevFeats}$ = 138 RF-DNA features) were all statistically different based on a 95% confidence interval for 6,000 observations for each SNR value from SNR = [-3,30] dB.

When SNR $\geq$ 6dB, the feature set containing the top four relevant features extracted from Forward Stepwise Selection (FSS) (N_{FSS} = 4 RF-DNA features) was statistically different based on a 95% confidence interval of 6,000 observations to the three statistically different sets N_{Feats}, $N_{InstFeatAmp}$, and $N_{NoStdDevFeats}$ and produced a maximum $\%C$ = 98.02%. The top four features from FSS were the standard deviation (σ) from the normalized instantaneous amplitudes subdivided

regions 14, 3, 44, and 24 in that order. These subregions correlate to execution commands provided to the DUT such as loading the least/most significant bits and loading the output registers. The standard deviation from subdivided regions 14 and 44 also appeared in the top four features from FSS when conducted at SNR = -9 dB and SNR = 30 dB [57]. This research recommends reducing to $N_{InstFeatAmp} =$ 184 RF-DNA features if time is not a critical factor for classification. Calculating only the normalized instantaneous amplitude subset reduces the computational time by one third of the original, while maintaining near equivalent classification performance. If time is a critical component to classification, this research would recommend using the $N_{FSS} = 4$ RF-DNA features subset for device classification. The FSS based subset reduces computational time nearly 99% and calculates only lower order statistics while suffering less than a 2% loss in classification performance.

4.4 Reduced Sampling Rate

Various sampling rates and their effect on classification was observed in this research. Figure 4.9 displays the held out testing set classification results for eight different sample rates which were accomplished via post-collection decimation. The figure is similar to Figure 4.8 where each line represents the average classification between the two separate classes. As the sampling rate is reduced beyond 143 MSps, the samples within each subdivided region approach singularity and statistical measures would not be appropriate as a means of determining features for each class. Since the cutoff frequency of the Low Pass Filter (LPF) used in collections was $f_{CO} \approx 96.8$ MHz, this research recommends using a reduced sample rate of $f_{ReducedS} =$ 200 MSps as it is double the bandwidth of the anti-aliasing LPF preserving Nyquist-criteria and maximum $\%C$ is only reduced by 0.14%.

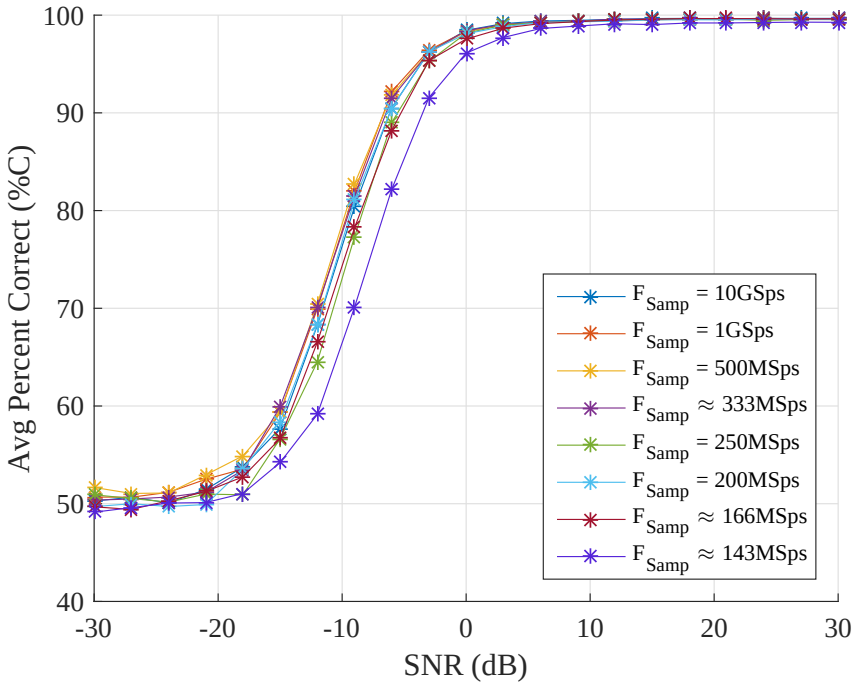


Figure 4.9. Average percent correct classification between authentic class, "Class 1", and counterfeit class, "Class 2", at various SNR values using reduced sampling rates as dictated by the legend.

4.5 Die Layout Classification and Verification

A new MDA/ML classification model was developed using a held out test set similar to the test set described in Section 3.5. Figure 4.10 displays the testing results of the authentic class and the newer die class correct classification results. The layout dependent model achieved an $\%C \geq 90\%$ occurring at SNR ≥ 0 dB and an maximum $\%C = 99.7\%$ occurring at SNR $= 27$ dB.

Verification was conducted on the die layout classification MDA/ML layout using all available devices similar to the verification results presented in Section 4.2. All devices are identified as '*rogue*' and are claiming to be either from the authentic class, older die layout, MAX526CCWG or current class, newer die layout, MAX526CCWG+. Figure 4.11 displays the verification results of the RF-DNA fea-

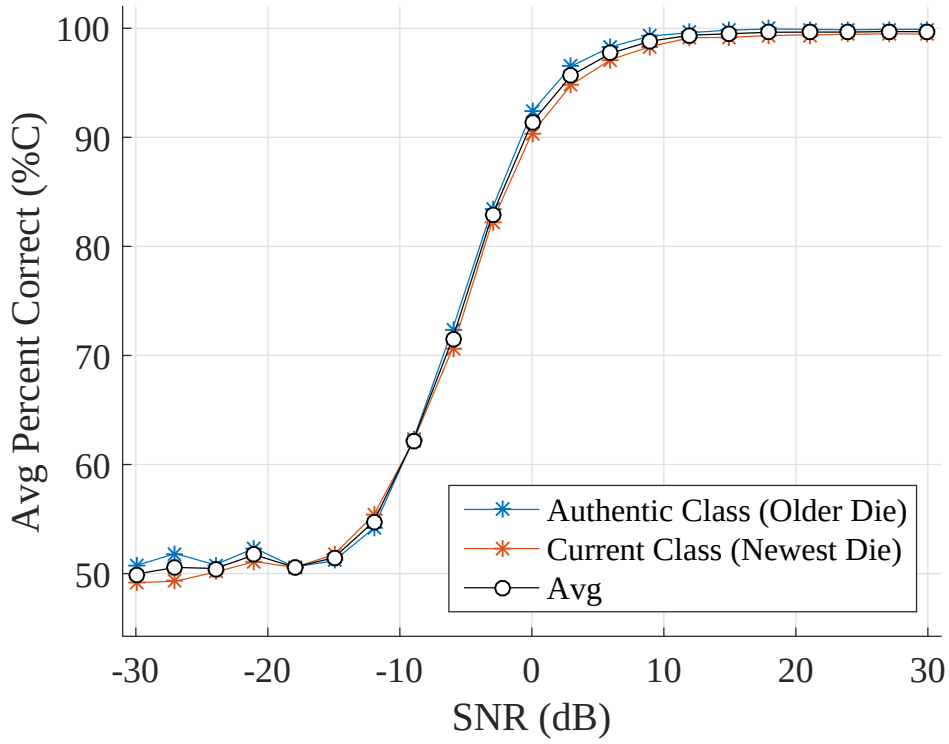


Figure 4.10. MDA/ML classification results using all $N_{Feats} = 552$ RF-DNA features of a held out testing set at each of the SNR_R values for both the authentic class, "Older Die", and the current class, "Newest Die", as well as the average of the two classes.

tures extracted from 3,000 new observations, or one grid scan, with one simulated noise realization per observation scaled appropriately to a SNR = 21dB for all of the authentic devices from Table 3.2 claiming to be a newer die layout or part number MAX526CCWG+. The average RRR for all nine devices is RRR = 99.43%. All devices met TVR $\geq$ 90% and FVR $\leq$ 10%. Figure 4.12 displays the verification results of the RF-DNA features extracted from 3,000 new observations, or one grid scan, with one simulated noise realization per observation scaled appropriately to a SNR = 21dB for all of the open market devices from Table 3.4 claiming to be an older die layout or part number MAX526CCWG.

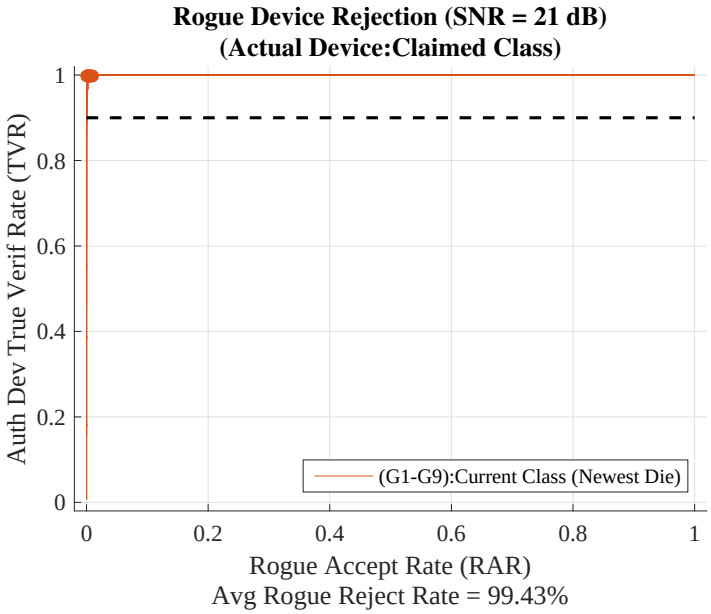


Figure 4.11. Verification results of testing 3,000 new observations per device against the die layout classification MDA/ML model at SNR = 21dB when all of the 9 authentic devices ("G1"-"G9") are unknown, rogue devices claiming to be newer layout devices or MAX526CCWG+.

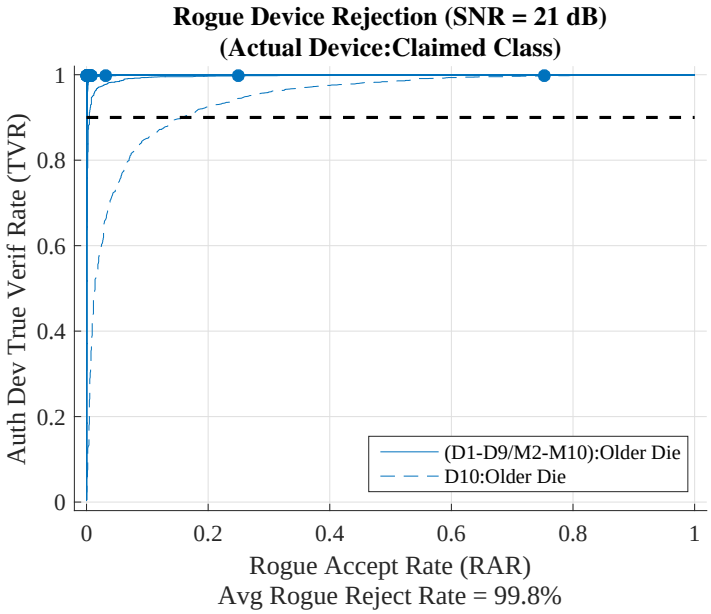


Figure 4.12. Verification results of testing 1,500 new observations per device against the die layout classification MDA/ML model at SNR = 21dB when all of the 19 open market devices ("D1"-"D10" and "M2"-"M10") are unknown, rogue devices claiming to be older layout devices or MAX526CCWG.

The average RRR for all nine devices is RRR = 99.8%. All devices met the TVR $\geq$ 90% and FVR $\leq$ 10% criteria except device "D10". At the given SNR, device "D10" would be flagged a possible older die layout. Additional testing such as X-Ray verification could be accomplished to verify the layout of device "D10".

This research has shown that the same devices that were classified as authentic when compared to counterfeit devices can also be discriminated based upon die layout changes. The RF-DNA features are an effective means of discriminating between the MAX526CCWG and MAX526CCWG+ devices.

V. Conclusion

5.1 Research Summary

Counterfeit electronic components have become a plague on the defense industry market. The problem has become more costly and more of a threat to national security. The Federal Bureau of Investigation (FBI) seized counterfeit Cisco routers worth at least $76 million and replacing counterfeit memory in a Missile Defense Agency high-altitude missile mission computer cost $2.7 million [14]. As a response to this growing costly threat, the United States (US) government has seen an increase in acquisition regulations, such as Defense Federal Acquisition Regulation Supplement (DFARS), on the entire life-cycle of a defense weapon system over the past few years [15]. Multiple industry companies such as Power Fingerprinting Inc. [69], Battelle [68], and Nokomis Inc. [5, 70, 71] have emerged as a commercial means of using Radio-Frequency (RF)-based techniques to determine authenticity of Integrated Circuit (IC) devices. This research effort addressed the usability of a *non-contact*, *non-destructive* method for determining electronic component authenticity by means of RF Distinct Native Attribute (RF-DNA) fingerprinting.

The research goal was focused on applying the RF-DNA feature were extract technique in combination with machine learning classification algorithms to discriminate authentic and counterfeit mixed-signal ICs. The RF-DNA features extracted from Unintentional RF Emission (URE) emitted from the Device Under Test (DUT), MAX526CCWG, and used with four different classification models: Multiple Discriminant Analysis/Maximum Likelihood (MDA/ML), Generalized Relevance Learning Vector Quantized-Improved (GRLVQI), Quadratic Discriminate Analysis (QDA), and Random Forest (RndF). The objective was to determine the authenticity of a small subset of certified authentic and counterfeit parts. A

computationally effective method of conducting RF-DNA feature selection in addition to reducing the sampling rate of collections was also evaluated by this research. Finally to expand upon the individual device classification originally conducted by a similar research effort [56], a different model was retrained using the same RF-DNA features to determine if the features could be used to differentiate die changes within the IC while functionality remains equivalent.

5.1.1 Classification Performance.

The machine learning classification model that was selected under this research was chosen based on two primary criteria, including 1) the lowest Signal-to-Noise Ratio (SNR) value for which average percent correct classification $\%C \geq 90\%$ and 2) maximum $\%C$. Of the four models trained and tested under this research, MDA/ML produced the best model based upon the first criteria. MDA/ML achieved $\%C \geq 90\%$ at the lowest SNR $= -6$ dB. GRLVQI, QDA, and RndF achieved $\%C \geq 90\%$ when SNR$= -3$ dB. GRLVQI produced the highest maximum $\%C = 100\%$, but a close second was MDA/ML with a maximum $\%C = 99.67\%$. All models were developed and tested using all of the $N_{Feats} = 552$ RF-DNA features extracted from the URE collected for four different devices and combined into two separate classes: the authentic class (Class 1) and the counterfeit class (Class 2).

All four models exhibited similar performance measures. QDA had a model induced bias when compared to MDA/ML as the peak of maximum $\%C$ occurred when SNR$= 9$ dB. QDA also had the lowest maximum $\%C = 99\%$ of the four models. Of the remaining three models, RndF performed the closest and most consistently to MDA/ML. The process of performing the K=5 fold Cross-Validation (CV) was standardized as a method to compare classification models; however, the CV can be accomplished by performing an Out-of-Bag (OOB) test within the RndF

model on the ensemble of trees to observe how the classifier would behave with unseen observations. This would have reduced computational time and does not stray from the intent of observing how observations not used to train fair against the developed model as a means of determining future testing results.

For die layout classification, the MDA/ML testing results displayed that an $\%C \geq 90\%$ occurred when SNR $\geq$ 0 dB and the maximum $\%C = 99.7\%$ occurred when SNR= 27 dB. Die layout discrimination testing results have similar performance to the testing results of the counterfeit and authentic class model. The MDA/ML testing results mimic those previously conducted on the DUT via a slightly different collection method when discriminating between individual devices [56]. Verification results are a better measurement of the model's future usability. If the model still performs well given new unknown devices that were not involved in the model development process, then the model has practical usability for counterfeit detection.

5.1.2 Verification Performance.

Verification using the authentic versus counterfeit classification model demonstrated excellent discriminatory capability at SNR = -3 dB. The verification testing demonstrated that, on average, 95.1% of the observations taken from the authentic devices were correctly classified and 98.63% of the observations taken from the counterfeit devices were correctly rejected. Additionally on average, 97.2% of the observations taken from the 19 MAX526CCWG+ devices were classified as authentic devices. While those devices are not in fact MAX526CCWG devices, functionally the devices perform the same task and could be used as the MAX526CCWG is intended to be used with the added benefit of containing no lead. RF-DNA combined with MDA/ML was successful in discriminating between MAX526CCWG de-

vices. Functionality testing and certification which consisted of physical inspections were conducted to verify the authenticity of the set of authentic MAX526CCWG devices and subsequently the counterfeit MAX526CCWG devices.

Verification performance conducted upon the die layout detection model at SNR = 21 dB demonstrated an average of 99.43% rejection for older die layout devices claiming to be updated die layouts. Conversely an average of 99.8% was observed for updated die layouts claiming to be an old layout. All devices met threshold value except device "D10". It is unknown why device "D10" did not meet the threshold rejection rate. One possible reason is the devices chosen to represent the newer die layout class did not encompass enough of a variance spread to represent the full production lots of newer devices. Another possible reason is that device "D10" is a different manufactured device that appears to more closely resemble the older die layout.

Based upon the verification performance, it has been determined that RF-DNA fingerprinting using MDA/ML machine learning is an effective, practical means of determining IC authenticity if a set of counterfeit ICs is available for model training. It is unknown how RF-DNA combined with MDA/ML would function as a single class model which is trained only on the authentic class.

5.1.3 Dimensional Reduction Performance.

The Dimensional Reduction Analysis (DRA) results demonstrated that only four RF-DNA features, as determined by Forward Stepwise Selection (FSS), are required to achieve an average $\%C \geq 90\%$ at SNR = -3 dB. If time are not factors, using the amplitude only subset of 184 RF-DNA features as this set produced the closest model to the original 552 feature model while reducing computational intensity by at least 66%. If time is a factor or a possible 1% decline in maximum

performance is tolerable, using the four RF-DNA features of standard deviation (σ) from the normalized instantaneous amplitudes subdivided regions 14, 3, 44, and 24 will provide a 99% reduction in computational complexity and has the potential to be designed on a near real-time application.

The second form of reduction addressed under this research was sampling rate reduction. The clock frequency at which the DUT was loading outputs was $f_{DUTclk} \approx$ 0.7353MHz and the spectral cutoff frequency for the anti-aliasing filter was $f_{CO} =$ 90MHz. Due to this fact it was suspected that a sampling rate of $f_S = 10$ GSps might be oversampling. The intent of this research to perform $f_S = 10$ GSps was to possibly sample small changes that might occur during transitions between execution commands. Based upon the post-collection reduction in number of samples per subregion, it is recommended that the sampling rate be reduced to $f_{ReducedS} = 200$ MSps as this maintains Nyquist-criteria for the anti-aliasing Low Pass Filter (LPF) and produced a lose of 0.14% in maximum $\%C$ when compared to the $\%C$ of the orginially $f_S = 10$ GSps sampled observations.

5.2 Future Research Recommendations

Every research effort is scoped down based on certain deadlines that must be met or shortages of materials; however, there have been many lessons learned throughout this research effort. The following are recommendations for possible research objectives:

1. Explore the one "class" option: The current method of supervisory counterfeit detection machine learning requires a second class of counterfeit devices to differentiate between an unknown feature set. However, there might not always be a counterfeit or a known counterfeit device available to train the detection model. Instead, explore the option of building a model of a known

authentic device and observing if an unknown device matches the model or not.

2. Acquire various types of counterfeits: The counterfeits used in this testing did not function with the specifications that were dictated in the datasheet. To fully test the effectiveness of the model detection process, a function counterfeit possibly repackaged or cloned would be optimum.

3. Replace the Dual In-line Package (DIP) Zero-Insertion Force (ZIF) socket: This research used an adapter board to solder the DUT to a DIP package to use available ZIF replacement method. There exists Small Outline Integrated Circuit (SOIC) ZIFs which may eliminate the possible inconsistencies of adapter boards and allow device re-usability after collections are complete.

4. Reduce collected grid size: Previous research demonstrated individual device discrimination [56] by only collecting at a single collection point. The grid scan used in this research required approximately 30 minutes of collection time per device. If a smaller grid scan can be used, it may be able to achieve similar results in a reduced time frame.

5. X-Ray all available device without the adapter: There was no issue noted when devices were X-Rayed; however, the DIP adapter provided a different resolution. X-Ray without the adapter could improve visual clarity. Additionally, performing an X-Ray on all devices helps in determining authenticity.

Bibliography

[1] IHS Technology. (2012, February) Reports of counterfeit parts quadruple since 2009, challenging us defense industry and national security. [Online]. Available: https://technology.ihs.com/389481/reports-of-counterfeit-parts-quadruple-since-2009-challenging-us-defense-industry-and-national-security

[2] ——. (2012, April) Top 5 most counterfeited parts represent a $169 billion potential challenge for global semiconductor market. [Online]. Available: http://press.ihs.com/press-release/design-supply-chain/top-5-most-counterfeited-parts-represent-169-billion-potential-cha

[3] US Senate, Armed Services Committee, *et al.*, "National Defense Authorization Act for Fiscal Year 2012," in *112th Congress. Washington*, 2011.

[4] G. Wilshusen, "Cybersecurity: A Better Defined and Implemented National Strategy Is Needed to Address Persistent Challenges," U.S. Government Accountability Office, Tech. Rep. GAO-13-462T, March 2013.

[5] B. Stone, "Comparison of radio frequency distinct native attribute and matched filtering techniques for device discrimination and operation identification," Master's thesis, Air Force Institute of Technology, March 2016.

[6] J. Eng. (2015, October) OPM hack: Government finally starts notifying 21.5 million victims. [Online]. Available: http://www.nbcnews.com/tech/security/opm-hack-government-finally-starts-notifying-21-5-million-victims-n437126

[7] B. Koerner. (2016, October) Inside the cyberattack that shocked the us government. [Online]. Available: https://www.wired.com/2016/10/inside-cyberattack-shocked-us-government/

[8] G. Hale. (2011, August) Stuxnet effect: Iran still reeling. [Online]. Available: http://www.isssource.com/stuxnet-affect-iran-still-reeling/

[9] P. Szoldra. (2015, December) The 9 worst cyberattacks of 2015. [Online]. Available: http://www.businessinsider.com/cyberattacks-2015-12/#hackers-breached-the-systems-of-the-health-insurer-anthem-inc-exposing-nearly-80-million-personal-records-1

[10] F. Rashid. (2014, January) How cybercriminals attacked target: Analysis. [Online]. Available: http://www.securityweek.com/how-cybercriminals-attacked-target-analysis

[11] S. Tobias. (2014, December) 2014: The year in cyberattacks. [Online]. Available: http://www.newsweek.com/2014-year-cyber-attacks-295876

[12] K. Zetter, "How the NSA's firmware hacking works and why it's so unsettling," February 2015. [Online]. Available: https://www.wired.com/2015/02/nsa-firmware-hacking/

[13] J. Stradley and D. Karraker, "The electronic part supply chain and risks of counterfeit parts in defense applications," *IEEE Trans. Compon. Packag. Technol.*, vol. 29, no. 3, pp. 703–705, Sept 2006.

[14] D. Goldman. (2012, November) Fake tech gear has infiltrated the u.s. government. [Online]. Available: http://money.cnn.com/2012/11/08/technology/security/counterfeit-tech/

[15] Defense, FAR, "Defense Federal Acquisition Regulation Supplement: Detection and avoidance of counterfeit electronic parts-further implementation (DFARS Case 2014-D005)," September 2015. [Online]. Available: https://www.federalregister.gov/documents/2015/09/21/2015-23516/defense-federal-acquisition-regulation-supplement-detection-and-avoidance-of-counterfeit-electronic

[16] K. Bernstein. (2017) Trusted integrated circuits (TRUST). [Online]. Available: http://www.darpa.mil/program/trusted-integrated-circuits

[17] ——. (2017) Supply chain hardware integrity for electronics defense (SHIELD). [Online]. Available: http://www.darpa.mil/program/supply-chain-hardware-integrity-for-electronics-defense

[18] D. Boak. (1973, July) A history of U.S. communications security: The david g. boak lectures. [Online]. Available: https://www.nsa.gov/news-features/declassified-documents/cryptologic-histories/assets/files/history_comsec.pdf

[19] W. E. Cobb, "Exploitation of unintentional information leakage from integrated circuits," Ph.D. dissertation, Air Force Institute of Technology, December 2011.

[20] W. E. Cobb *et al.*, "Intrinsic physical-layer authentication of integrated circuits," *IEEE Trans. Inf. Forens. Security*, vol. 7, no. 1, pp. 14–24, February 2012.

[21] ——, "Physical layer identification of embedded devices using RF-DNA Fingerprinting," in *Military Communications Conference (MILCOM)*, October 2010, pp. 2168–2173.

[22] R. Deppensmith and S. Stone, "Integrated circuit (IC) aging effects on radio-frequency distinct native attributes (RF-DNA)," in *IEEE National Aerospace and Electronics Conference, (NAECON)*, June 2014, pp. 331–333.

[23] C. Dubendorfer *et al.*, "An RF-DNA verification process for ZigBee networks," in *Military Communications Conference (MILCOM)*, October 2012, pp. 1–6.

[24] R. Klein *et al.*, "Sensitivity analysis of burst detection and RF fingerprinting classification performance," in *IEEE International Conference on Communications (ICC)*, Jun 2009, pp. 1 –5.

[25] ——, "Application of wavelet-based RF fingerprinting to enhance wireless network security," *Journal of Communications and Networks*, vol. 11, no. 6, pp. 544–555, December 2009.

[26] R. Klein, "Application of dual-tree complex wavelet transforms to burst detection and RF fingerprint classification," Ph.D. dissertation, Air Force Institute of Technology, September 2009.

[27] D. Reising and M. Temple, "WiMAX mobile subscriber verification using gabor-based RF-DNA fingerprints," in *IEEE International Conference on Communications (ICC)*, June 2012, pp. 1005–1010.

[28] D. Reising *et al.*, "Authorized and rogue device discrimination using dimensionally reduced RF-DNA fingerprints," *IEEE Trans. Inf. Forens. Security*, vol. 10, no. 6, pp. 1180–1192, June 2015.

[29] ——, "Gabor-based RF-DNA fingerprinting for classifying 802.16e WiMAX mobile subscribers," in *International Conference on Computing, Networking and Communications (ICNC)*, February 2012, pp. 7 –13.

[30] D. Reising, "Exploitation of RF-DNA for device classification and verification using GRLVQI processing," Ph.D. dissertation, Air Force Institute of Technology, December 2012.

[31] B. Wright, "PLC hardware discrimination using RF-DNA fingerprinting," Master's thesis, Air Force Institute of Technology, June 2014.

[32] W. Suski *et al.*, "Radio frequency fingerprinting commercial communication devices to enhance electronic security," *Int. J. Electron. Secur. Digit. Forensic*, vol. 1, pp. 301–322, October 2008.

[33] ——, "Using spectral fingerprints to improve wireless network security," in *IEEE Global Telecommunications Conference (GLOBECOM)*, December 2008, pp. 1–5.

[34] M. Williams *et al.*, "Augmenting bit-level network security using physical layer RF-DNA fingerprinting," in *IEEE Global Telecommunications Conference (GLOBECOM)*. IEEE, December 2010, pp. 1–6.

[35] ——, "RF-DNA fingerprinting for airport WiMAX communications security," in *4th International Conference on Network and System Security (NSS)*, September 2010, pp. 32–39.

[36] B. Ross *et al.*, "Physical-layer discrimination of power line communications," in *International Conference on Computing, Networking and Communications (ICNC)*, January 2017.

[37] ——, "Simulcasted power line communication network (SPN) discrimination using wired signal distinct native attribute (WS-DNA) features," in *International Conference on Cyber Warfare and Security (ICCWS)*, March 2017.

[38] R. Deppensmith and S. Stone, "Optimized fingerprint generation using unintentional emission radio-frequency distinct native attributes (RF-DNA)," in *IEEE National Aerospace and Electronics Conference, (NAECON)*, June 2014, pp. 327–330.

[39] H. Patel, "Advances in SCA and RF-DNA fingerprinting through enhanced linear regression attacks and application of random forest classifiers," Master's thesis, Air Force Institute of Technology, September 2014.

[40] S. Mangard *et al.*, *Power analysis attacks: Revealing the secrets of smart cards*. Springer Science & Business Media, 2008, vol. 31.

[41] P. Kocher, "Timing attacks on implementations of diffie-hellman, RSA, DSS, and other systems," in *Annual International Cryptology Conference*. Springer, August 1996, pp. 104–113.

[42] D. Agrawal *et al.*, *The EM Side—Channel(s)*, B. S. Kaliski, ç. K. Koç, and C. Paar, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2003. [Online]. Available: http://dx.doi.org/10.1007/3-540-36400-5_4

[43] P. Kocher *et al.*, "Differential power analysis," in *Annual International Cryptology Conference*. Springer, December 1999, pp. 388–397.

[44] S. Skorobogatov, "Using optical emission analysis for estimating contribution to power analysis," in *IEEE Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC)*, September 2009, pp. 111–119.

[45] P. Harmer and M. Temple, "An improved LFS engine for physical layer security augmentation in cognitive networks," in *International Conference on Computing, Networking and Communications (ICNC)*, January 2013, pp. 719–723.

[46] P. Harmer *et al.*, "Using differential evolution to optimize 'learning from signals' and enhance network security," in *Proceedings of the 13th Annual Conference on Genetic and Evolutionary Computation*, ser. GECCO. New York, NY, USA: ACM, 2011, pp. 1811–1818.

[47] ——, "Using de-optimized LFS processing to enhance 4g communication security," in *Proceedings of 20th International Conference on Computer Communications and Networks (ICCCN)*, August 2011, pp. 1 –8.

[48] D. Montminy, "Enhancing electromagnetic side-channel analysis in an operational environment," Ph.D. dissertation, Air Force Institute of Technology, September 2013.

[49] H. Ott, *Electromagnetic Compatibility*. John Wiley and Sons, Inc., 2009, ch. 2, pp. 44–105. [Online]. Available: http://dx.doi.org/10.1002/9780470508510

[50] Federal Communications Commission. (2016, December) Code of federal regulations title 47. [Online]. Available: https://www.fcc.gov/general/rules-regulations-title-47

[51] S. Stone, "Radio frequency based programmable logic controller anomaly detection," Ph.D. dissertation, Air Force Institute of Technology, September 2013.

[52] S. Stone and M. Temple, "RF-based anomaly detection for PLCs," in *Sixth Annual IFIP Working Group 11.10 International Conference on Critical Infrastructure Protection*, 2012.

[53] ——, "Radio-frequency-based anomaly detection for programmable logic controllers in the critical infrastructure," *International J. of Critical Infrastructure Protection*, vol. 5, no. 2, pp. 66 – 73, 2012. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1874548212000200

[54] B. D. Stone and S. J. Stone, "Radio frequency based reverse engineering of microcontroller program execution," in *IEEE National Aerospace and Electronics Conference (NAECON)*, June 2015, pp. 159–164.

[55] B. Stone and S. Stone, "Comparison of radio frequency based techniques for device discrimination and operation identification," in *11th International Conference on Cyber Warfare and Security: (ICCWS)*. Academic Conferences and publishing limited, March 2016, p. 475.

[56] S. O'Neill and S. Stone, "Determining authenticity of mixed-signal devices using unintentional Radio Frequency (RF) emissions," in *IEEE National Aerospace and Electronics Conference (NAECON) and Ohio Innovation Summit (OIS)*, 2016, pp. 478–481.

[57] S. O'Neill *et al.*, "Comparison of various discrimination techniques on counterfeit mixed-signal integrated circuits," in *International Conference on Cyber Warfare and Security (ICCWS)*, March 2017.

[58] S. Stone *et al.*, "Detecting anomalous programmable logic controller behavior using RF-based Hilbert transform features and a correlation-based verification process," *International J. of Critical Infrastructure Protection*, vol. 9, pp. 41–51, 2015.

[59] G. Wood. (2016, January) Costly counterfeit electronic components in the supply chain can also be a safety concern. [Online]. Available: http://blog.ihs.com/costly-counterfeit-electronic-components-in-the-supply-chain-can-also-be-a-safety-concern

[60] U. Guin *et al.*, "Anti-counterfeit techniques: from design to resign," in *14th International Workshop on Microprocessor Test and Verification*. IEEE, December 2013, pp. 89–94.

[61] ——, "Counterfeit IC detection and challenges ahead," *ACM SIGDA*, vol. 43, no. 3, pp. 1–5, 2013.

[62] ——, "A comprehensive framework for counterfeit defect coverage analysis and detection assessment," *J. of Elect. Testing*, vol. 30, no. 1, pp. 25–40, 2014.

[63] U. Guin, D. DiMase, and M. Tehranipoor, "Counterfeit integrated circuits: detection, avoidance, and the challenges ahead," *J. of Elect. Testing*, vol. 30, no. 1, pp. 9–23, 2014.

[64] Altera. (2016, December) Military temperature range qualified devices. [Online]. Available: https://www.altera.com/solutions/industry/military/applications/mil-temp.html

[65] M. Tehranipoor and F. Koushanfar, "A survey of hardware Trojan taxonomy and detection," *IEEE Design and Test of Computers*, vol. 27, no. 1, pp. 10–25, February 2010.

[66] J. Federico. (2012, November) Awareness of marking permanency and black top testing in todays electronic component industry. [Online]. Available: https://www.erai.com/CustomUploads/ca/wp/2012_7_Awareness_of_Marking_Permanency.pdf

[67] European Union. (2011, July) Recast of the RoHS directive. [Online]. Available: http://ec.europa.eu/environment/waste/rohs_eee/index_en.htm

[68] T. Bergman and K. Liszewski, "Battelle barricade: A nondestructive electronic component authentication and counterfeit detection technology," in *IEEE Symposium on Technologies for Homeland Security (HST)*, May 2016, pp. 1–6.

[69] PFP Cybersecurity. (2015) Supply chain protection a white paper on counterfeit detection. [Online]. Available: http://www.pfpcybersecurity.com/assets/PFP_Supply-Chain_White_Paper_v7.pdf

[70] W. Keller *et al.*, "System and method for physically detecting counterfeit electronics," U.S. Patent US20 120 226 463 A1, September, 2012. [Online]. Available: http://www.google.com/patents/US20120226463

[71] W. Keller and B. Pathak, "Integrated circuit with electromagnetic energy anomaly detection and processing," U.S. Patent US9 059 189 B2, June, 2015. [Online]. Available: https://www.google.com/patents/US9059189

[72] I. Verbauwhede, *Secure integrated circuits and systems*. Springer, 2010.

[73] S. Theodoridis and K. Koutroumbas, "Pattern recognition and neural networks," in *Machine Learning and Its Applications*. Springer, 2001, pp. 169–195.

[74] R. Duda *et al.*, *Pattern classification*. John Wiley & Sons, 2012.

[75] D. MacKay, *Information theory, inference and learning algorithms*. Cambridge university press, 2003.

[76] G. James *et al.*, *An Introduction to Statistical Learning with Applications in R*. Springer-Verlag New York, 2013.

[77] M. Mendenhall and E. Merenyi, "Relevance-based feature extraction for hyperspectral images," *Neural Networks, IEEE Transactions on*, vol. 19, no. 4, pp. 658–672, April 2008.

[78] T. Bihl, "Feature selection and classifier development for radio frequency device discrimination," Ph.D. dissertation, Air Force Institute of Technology, December 2015.

[79] B. Hammer and T. Villmann, "Generalized relevance learning vector quantization," *Neural Networks*, vol. 15, no. 8, pp. 1059–1068, 2002.

[80] H. Patel *et al.*, "Application of ensemble decision tree classifiers to ZigBee device network authentication using RF-DNA fingerprinting," in *9th International Conference on Cyber Warfare and Security, March*, 2014, pp. 176–186.

[81] L. Raileanu and K. Stoffel, "Theoretical comparison between the gini index and information gain criteria," *Annals of Mathematics and Artificial Intelligence*, vol. 41, no. 1, pp. 77–93, 2004.

[82] L. Breiman *et al.*, *Classification and regression trees*. CRC press, 1984.

[83] A. Liaw and M. Wiener, "Classification and regression by randomForest," *R news*, vol. 2, no. 3, pp. 18–22, 2002.

[84] L. Breiman, "Random forests," *Machine Learning*, vol. 45, no. 1, pp. 5–32, 2001. [Online]. Available: http://dx.doi.org/10.1023/A:1010933404324

[85] Maxim Integrated Products, *Maxim Calibrated Quad 12-Bit Voltage-Output D/A Converters Datasheet*, 1997. [Online]. Available: http://datasheets.maximintegrated.com/en/ds/MAX526-MAX527.pdf

[86] Aries Electronics, Incorporated, *Series 450001 and 650000 SOIC and SOJ-to-DIP Adapter*, April 2016. [Online]. Available: http://www.arieselec.com/products/data/18011-soic-and-soj-to-dip-adapter.pdf

[87] ——, *Series 55 Universal Zero-Insertion-Force DIP Test Socket*, April 2016. [Online]. Available: http://www.arieselec.com/products/data/10001-universal-dip-zif-test-socket.pdf

[88] BK Precision, *Instruction Manual BK Precision Model 9130 Triple Output Programmable DC Power Supply*, 2014. [Online]. Available: https://bkpmedia.s3.amazonaws.com/downloads/manuals/en-us/9130_manual.pdf

[89] Terasic Inc., "Altera Cyclone V SoCKit - the Development Kit for New SoC Device." [Online]. Available: http://www.terasic.com.tw/cgi-bin/page/archive.pl?Language=English&CategoryNo=167&No=816

[90] ——, "General Purpose Input Output High-Speed Terasic Connector Card." [Online]. Available: http://www.terasic.com.tw/cgi-bin/page/archive.pl?Language=English&CategoryNo=67&No=322

[91] Riscure, *EM Probe Station Datasheet*, 2011. [Online]. Available: https://www.riscure.com/documents/datasheet_emprobestation.pdf

[92] Teledyne LeCroy, *WavePro 7 Zi-A Series 1.5GHz-6GHz*. [Online]. Available: http://cdn.teledynelecroy.com/files/pdf/wavepro_7_zi-a_datasheet.pdf

[93] Mini-Circuits, *BLP-90+ Coaxial Low Pass Filter Datasheet*. [Online]. Available: http://www.minicircuits.com/pdfs/BLP-90+.pdf

[94] J. Wylie, "Radio frequency-based microcontroller anomaly detection," Master's thesis, Air Force Institute of Technology, March 2016.

[95] M. Goldack and C. Paar, "Side-channel based reverse engineering for microcontrollers," Master's thesis, Ruhr-Universität Bochum, January 2008.

[96] Mathworks. Discrete-Time Analytic Signal Using Hilbert Transform. [Online]. Available: https://www.mathworks.com/help/signal/ref/hilbert.html

[97] J. Rodriguez *et al.*, "Sensitivity analysis of k-fold cross validation in prediction error estimation," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 32, no. 3, pp. 569–575, March 2010.

[98] T. Li *et al.*, "Using discriminant analysis for multi-class classification: an experimental investigation," *Knowledge and Information Systems*, vol. 10, no. 4, pp. 453–472, 2006. [Online]. Available: http://dx.doi.org/10.1007/s10115-006-0013-y

[99] L. Leemis and S. Park, *Discrete-event simulation: A first course*. Pearson Prentice Hall Upper Saddle River, 2006.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704–0188

1. REPORT DATE *(DD–MM–YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From — To)*
23–03–2017	Master's Thesis	May 2015 – Feb 2017

4. TITLE AND SUBTITLE

Radio Frequency-Based Device Discrimination of Mixed-Signal Integrated Circuits and Counterfeit Detection

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

O'Neill, Sean P., Capt, USAF

5d. PROJECT NUMBER

17G755

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Air Force Institute of Technology
Graduate School of Engineering and Management (AFIT/EN)
2950 Hobson Way
WPAFB OH 45433-7765

8. PERFORMING ORGANIZATION REPORT NUMBER

AFIT-ENG-MS-17-M-055

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

Air Force Research Laboratory, Integrated Electronic & Net-Centric Warfare Div
Attn: Yong C. Kim
2241 Avionics Circle
Wright-Patterson AFB, OH 45433-7322
(937) 528-8026 (DSN 798-8062) yong.kim@us.af.mil

10. SPONSOR/MONITOR'S ACRONYM(S)

AFRL/RYWA

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT

DISTRIBUTION STATEMENT A:
APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED.

13. SUPPLEMENTARY NOTES

14. ABSTRACT

The research presented here focused on applying radio frequency-distinct native attributes (RF-DNA) feature extraction combined with various types of machine learning such as: multiple discriminant analysis/maximum likelihood (MDA/ML), generalized relevance learning vector quantized-improved (GRLVQI), quadratic discriminant analysis (QDA), and random forest (RndF) to discriminate mixed-signal integrated circuit (IC) devices and perform counterfeit detection. Unintentional RF emissions (URE) were collected from the device under test (DUT), Maxim MAX526CCWG digital to analog converter (DAC), that were independently screened into two categories of authentic and counterfeit. A subset of these devices were used to generate a model and new collections from all devices were used to verify the model. Additionally, RF-DNA combined with (MDA/ML) was used to develop a model to discriminate between the MAX526CCWG devices and the update devices MAX526CCWG+, a lead free version of the MAX526CCWG. This research also explored feature and sampling rate reduction as a means to reduce complexity.

15. SUBJECT TERMS

Counterfeit Detection, Hardware Discrimination, Unintentional Emissions, RF-DNA, MDA/ML, GRLVQI, QDA, Random Forest, Mixed-Signal Devices

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Maj J. Addision Betances, AFIT/ENG
U	U	U	U	98	19b. TELEPHONE NUMBER *(include area code)* (937) 785-3636, x3305; jbetance@afit.edu