The analysis of decapsulated chip surface with confocal microscopy

Rafaela Aliaj

Master's thesis

2021

Tomas Bata University in Zlín
Faculty of Applied Informatics

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
Ústav elektroniky a měření

Akademický rok: 2020/2021

ZADÁNÍ DIPLOMOVÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	**Rafaela Aliaj**
Osobní číslo:	**A19739**
Studijní program:	**N3902 Engineering Informatics**
Studijní obor:	**Security Technologies, Systems and Management**
Forma studia:	**Prezenční**
Téma práce:	**Analýza povrchu čipu konfokální mikroskopií**
Téma práce anglicky:	**The analysis of decapsulated chip surface with confocal microscopy**

Zásady pro vypracování

1.Fundamental study of counterfeit components problematics.
2.Fundamental study of semiconductor component design and technology.
3.Study of confocal microscopy principles and methodology.
4.Analyse decapsulated semiconductor chips surface with confocal microscope, study and recommend observable features suitable for authenticity evaluation.
5.Design a method for an efficient confocal microscopy outputs evaluation aimed at differences between genuine and counterfeit chips.
6.Create the studied chips confocal microscopy instructive set for differences demonstration

Forma zpracování diplomové práce: **tištěná/elektronická**
Jazyk zpracování: **Angličtina**

Seznam doporučené literatury:

[1] Tehranipoor, Mark (mohammad), Guin, U., & Forte, D. (2016). Counterfeit integrated circuits: Detection and avoidance. Cham, Switzerland: Springer International Publishing.
[2] Tehranipoor, Mohammad, Salmani, H., & Zhang, X. (2013). Integrated circuit authentication: Hardware Trojans and counterfeit detection (2014th ed.). Cham, Switzerland: Springer International Publishing.
[3] Nishi, Y., & Doering, R. (Eds.). (2017). Handbook of semiconductor manufacturing technology, second edition. doi:10.1201/9781420017663
[4] Hawkes, P. W., & Spence, J. C. H. (Eds.). (2008). Science of Microscopy (1st ed.). New York, NY: Springer.
[5] Paddock, S. W. (Ed.). (2013). Confocal microscopy: Methods and protocols (2nd ed.). doi:10.1007/978-1-60761-847-8
[6] Price, R. L., & Jerome, W. G. (jay) (Eds.). (2016). Basic confocal microscopy. New York, NY: Springer.

Vedoucí diplomové práce: **Ing. Petr Neumann, Ph.D.**
Ústav elektroniky a měření

Datum zadání diplomové práce: **23. července 2021**
Termín odevzdání diplomové práce: **20. srpna 2021**

doc. Mgr. Milan Adámek, Ph.D. v.r.
děkan

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta aplikované informatiky
DĚKAN
L.S.

Ing. Milan Navrátil, Ph.D. v.r.
ředitel ústavu

I hereby declare that:

- I understand that by submitting my Diploma thesis, I agree to the publication of my work according to Law No. 111/1998, Coll., On Universities and on changes and amendments to other acts (e.g. the Universities Act), as amended by subsequent legislation, without regard to the results of the defence of the thesis.
- I understand that my Diploma Thesis will be stored electronically in the university information system and be made available for on-site inspection, and that a copy of the Diploma/Thesis will be stored in the Reference Library of the Faculty of Applied Informatics, Tomas Bata University in Zlin, and that a copy shall be deposited with my Supervisor.
- I am aware of the fact that my Diploma Thesis is fully covered by Act No. 121/2000 Coll. On Copyright, and Rights Related to Copyright, as amended by some other laws (e.g. the Copyright Act), as amended by subsequent legislation; and especially, by §35, Para. 3.
- I understand that, according to §60, Para. 1 of the Copyright Act, TBU in Zlin has the right to conclude licensing agreements relating to the use of scholastic work within the full extent of §12, Para. 4, of the Copyright Act.
- I understand that, according to §60, Para. 2, and Para. 3, of the Copyright Act, I may use my work - Diploma Thesis, or grant a license for its use, only if permitted by the licensing agreement concluded between myself and Tomas Bata University in Zlin with a view to the fact that Tomas Bata University in Zlín must be compensated for any reasonable contribution to covering such expenses/costs as invested by them in the creation of the thesis (up until the full actual amount) shall also be a subject of this licensing agreement.
- I understand that, should the elaboration of the Diploma Thesis include the use of software provided by Tomas Bata University in Zlin or other such entities strictly for study and research purposes (i.e. only for non-commercial use), the results of my Diploma Thesis cannot be used for commercial purposes.
- I understand that, if the output of my Diploma Thesis is any software product(s), this/these shall equally be considered as part of the thesis, as well as any source codes, or files from which the project is composed. Not submitting any part of this/these component(s) may be a reason for the non-defence of my thesis.

I herewith declare that:

- I have worked on my thesis alone and duly cited any literature I have used. In the case of the publication of the results of my thesis, I shall be listed as co-author.
- That the submitted version of the thesis and its electronic version uploaded to IS/STAG are both identical.

In Zlin; dated: 19.08.2021

Rafaela Aliaj m.p
Student´s Signature

ABSTRAKT

Tato práce se zabývá možnostmi využití konfokální mikroskopie k rozpoznání rysů nepůvodních systémů na čipu (SoC) integrovaného obvodu a je jednou z prvních v oblasti aplikace konfokální mikroskopie. Práce sestává ze dvou částí, části teoretické a části experimentální. Teoretická část zahrnuje literární východiska pro danou problematiku, jak po stránce metod pro analýzu původnosti elektronických součástek, tak také po stránce principů a aplikace konfokální mikroskopie. Součástí je nezbytná terminologie, definice a postupy důležité pro orientaci ve výsledcích a závěrech v experimentální části. Experimentální část se opírá o nástroje a funkce konfokálního mikroskopu s laserovým skenováním (LSCM - Laser Scanning Confocal Microscope) firmy Zeiss, model LSM700. Tyto nástroje a funkce byly během experimentů kombinovány a nastavovány v zájmu dosažení co nejlepšího rozlišení při porovnávání původních a nepůvodních polovodičových součástek.

Klíčová slova: *systém na čipu (SoC), konfokální mikroskop s laserovým skenováním (LSCM), původní a nepůvodní elektronická součástka*

ABSTRACT

This thesis on using confocal microscopy to detect counterfeit electronic components is one of the first of its kind. It consists of two parts: theoretical background and practical experimentation. The theoretical part of the thesis includes a thorough, multi-vocal literature review that provides the reader with the baseline information on the thesis research area and familiarizes them with all the necessary terms, definitions and procedures needed to comprehend the practical experimentation results and conclusions. In the practical experimentation phase, the Laser Scanning Confocal Microscope (Zeiss LSM700) tools and functionalities are explored and actively combined in numerous different ways in order to design the right combination of parameters, tools and functionalities for an efficient confocal microscopy outputs evaluation aimed at differences between genuine and counterfeit chips.

Keywords: *counterfeit, ICs, confocal microscopy, LSCM, detection, methodology*

ACKNOWLEDGEMENTS

It is a genuine pleasure to express my sincere gratitude to my professor, supervisor and guide **Ing. Petr Neumann, Ph.D.** Senior Lecturer in the Electronics and Measurements Department, Scot at heart. He is the most lively, enthusiastic, and energetic professor I have ever had. I am truly thankful for his dedication, help and support throughout this research and, honestly, through the whole of my studies at Tomas Bata University. His timely advice, constructive feedback and academic approach have helped me to a great extent to finalize this diploma thesis.

I am forever grateful to **Ing. Milan Navrátil, Ph.D.** who, although being Head of Electronics and Measurements Department, found the time to teach me and guide me around the Confocal Microscope System. He has been willing to offer his help and support anytime needed and I believe that makes him a great educator model.

I am greatly thankful to all my UTB professors throughout these two years of Master studies. They have all been greatly supportive, highly competent and fair in their decisions. Special thanks go to **doc. Ing. Jiří Vojtěšek, Ph.D.**, Vice-Dean for Bachelor´s and Master´s Study, for being a source of information and support. I cannot help but mention one of the people I am sincerely and greatly thankful to, **doc. Ing. Marek Kubalčík, Ph.D.** He has solved all my queries, replied to all my questions and doubts and handled any possible issue in an exceptionally, timely manner. I am sincerely grateful to him for his extraordinary help.

Lastly, but most importantly, I am immensely thankful to my family and friends for their undying support. My family has given me unconditional love and care. I love them so much, and I would not have made it this far without them. Lots of love and appreciation for my close friend, roommate, classmate and colleague, Alerda Matrisi for always having my back.

I hereby declare that the print version of my Bachelor's/Master's thesis and the electronic version of my thesis deposited in the IS/STAG system are identical.

TABLE OF CONTENTS

I. INTRODUCTION

Although multiple definitions of counterfeiting exist, counterfeiting is often defined as the act of copying something original, aiming to steal, destroy, or replace the authentic product, and/or illegally use it to deceive individuals into trusting that the fake is of equal or greater value than the original. [7] The International Anticounterfeiting Coalition (IAC) defines counterfeiting as the manufacturing and/or distribution of goods under someone else's name, and without their authorization. Counterfeit products are generally made from low quality components and materials, in an attempt to sell a cheap imitation of similar goods produced by brands consumers know and trust. [8]

This global phenomenon has grown exponentially in the recent decades, causing significant levels of concern, attention and interest among policy makers, practitioners, and academic researchers. Counterfeiting has evolved into a well-organized, coordinated production of goods that are getting highly sophisticated, making these replicas harder and harder to differentiate from the "real-deal".

Counterfeiting affects a wide variety of industries worldwide, and constitutes of both, the forgeries of currency and documents, [9] as well as the imitations of items such as luxury goods, pharmaceuticals, automobile parts, unapproved aircraft parts, watches, software, toys, works of art, movies, and electronics (both parts and finished products). [10] Counterfeit electronic components have turned into a Multibillion-Dollar Black Market posing major financial, reliability and security concerns.

This thesis will focus on the analysis of decapsulated chip surface with confocal microscopy, in order to evaluate the differences between genuine and counterfeit chips and designing a methodology of efficient counterfeit components detection.

1.1 Background

Counterfeiting has a long and ignoble history, growing into the "crime of the 21st Century" as stated by James Moody, former chief of the FBI organized crime division. [11] According to the Organization for Economic Cooperation and Development (OECD) and the EU Intellectual Property Office (2019), the international trade of counterfeit products amounted to $509 Billion or 3.3% of world trade, in 2019. [12] Drawing a map of the amount and dynamics of counterfeits in the global economy is a complicated task for

methodological purposes, but the available data and evidence points out an ever-growing trend in the worldwide trade of counterfeit goods.

Figure 1.1 depicts the industries most affected by counterfeit products, by showing the percentage of the total value of seized counterfeit and pirated goods worldwide in 2019. [12]

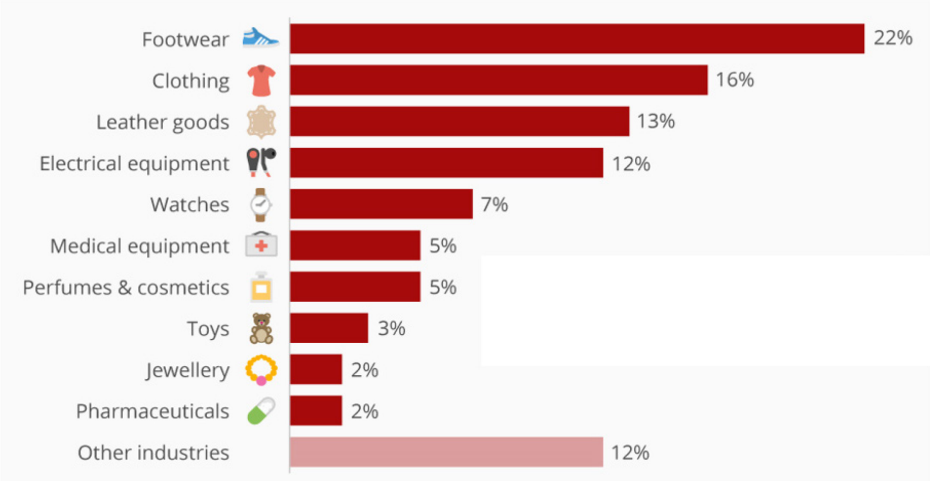

Figure 1. 1 Industries most affected by counterfeit products

Source: OECD [12]

Figure 1.2 shows sales losses from counterfeit goods worldwide in 2020, by retail sector. The amounts are in *billion euro* [13]

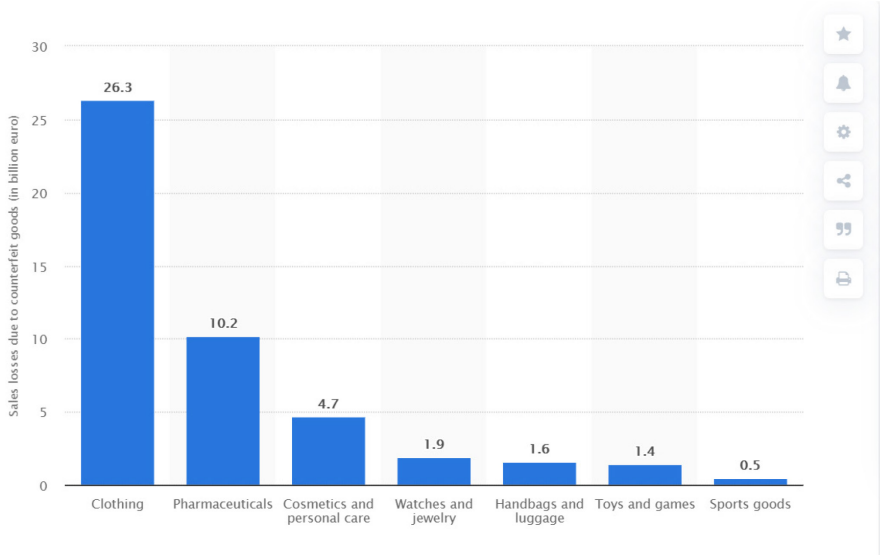

Figure 1. 2 Sales losses from counterfeit goods in 2020

Source: Statista [13]

The International Trademark Association (INTA), in collaboration with the International Chamber of Commerce – Business Action to Stop Counterfeiting and Piracy, share a report titled "The Economic Impacts of Counterfeiting and Piracy", in February 2017. This report quantified the social and economic damage of counterfeiting, by using the data of 2013 and projecting it to 2022. [14] In *Table 1* there is a detailed report estimating the total value of counterfeit and pirated goods, breaking it into domestic and international trade, and digital piracy for 2022.

Estimate	2013	2022 (forecast)
Total international trade in counterfeit and pirated goods	$461 Billion	$991 Billion
Total domestic production and consumption of counterfeit pirated goods	$249 - $456Billion	$524 - $959 Billion
Digital piracy in movies, music and software	$213Billion	$384 - $856 Billion
- Digital piracy in film	$160 Billion	$289-644 Billion
- Digital piracy in music	$29 Billion	$53-117 Billion
- Digital piracy in software	$24 Billion	$42-95 Billion
Total value of counterfeit and pirated goods	**$923 Billion – 1.13 Trillion**	**$1.90 -$2.81 Trillion**

Table 1 Estimates of Counterfeit and Pirated Goods

Source: Frontier

Estimate	2013	2022 (forecast)
Wider economic and social costs		
- Displacement of legitimate economic activity	$470-$597 Billion	$980-$1244 Billion
- Estimated reduction in FDI	$111 Billion	$231 Billion
- Estimated fiscal losses	$96-$130 Billion	$199-$270 Billion
- Estimated costs of crime	$60 Billion	$125 Billion
Total Wider economic and social costs	**$737-$898 Billion**	**$1.54 - $1.87 Trillion**
Estimated employment losses	**2-2.6 million**	**4.2-5.4 million**
Foregone economic growth in OECD 2017	**$30 Billion to $54 Billion**	

Table 2 Estimates of Economic and Social Costs of Counterfeit and Pirated Goods

Source: Frontier

In *Table 2* above, there is a wider representation of economic and social costs of counterfeit and pirated goods, including displacement of legitimate activity, reduction in Foreign Direct Investment (FDI) and estimated employment losses.

As shown in the tables above, the estimated cost of counterfeit and pirated goods was about $1.13 trillion. By 2022, the counterfeit goods and digital piracy is estimated to cost the global economy $1.90 to $2.81 trillion. Additionally, it is predicted to have 5.4 million jobs lost as a result of counterfeiting and piracy, by 2022. [14]

It is important to note that the data used for these statistics does not include the counterfeit goods that were produced and consumed domestically, or the pirated digital products shared over the internet, but is solely based on custom seizures.

1.2 Problem Discussion

The data presented above indicates that the counterfeit worldwide problem is reaching the tipping point of becoming a very serious threat to national and international economies. Counterfeit electronics (products and components) have become a major challenge as the electronic component industry is growing more complex due to globalization. A detailed research on the electronic component counterfeit problem is given in the Analysis section.

Most research on the area of counterfeit electronics focuses on the analysis of the counterfeit threat, [15] and the impact of this rising phenomenon on numerous areas and industries. [16] [17] There is also academic research in the area of detection and avoidance of counterfeit electronics products and components. [1] [2] [17] [18] [19]

Currently, there is insubstantial academic research on the topic of using microscopy for counterfeit detection, it mainly being the optical microscopy. [20] However, there has not yet been a single full-fledged study on using confocal microscopy to detect counterfeit chips. This thesis will provide such a study, assessing the existing data and designing a methodology to evaluate the differences of original and counterfeit parts. Therefore, succeeding to fill the gap in the literature.

1.3 Purpose

The purpose of this thesis is to design a method for an efficient confocal microscopy outputs evaluation aimed at differences between genuine and counterfeit chips.

1.4 Methodology

The methodology of this thesis is divided into two distinct parts.

I. The first part deals with reviewing and analyzing previous work and studies related to counterfeit components problematics, risks of using counterfeit electronic components, semiconductor component design and technology and confocal microscopy principles and methodology. Therefore, the used methodology is a multi-vocal Literature Review.

The Literature Review is structured based on the protocol suggested by Kitchenham [20] which mentions a detailed list of inclusion and exclusion criteria so as to achieve a non-biased and coherent selection of adequate literature.

The papers were selected by first examining the titles of the whole result group and excluding all the generally non-relevant papers. Secondly, the abstract of the remaining papers was scanned and once again, the ones not meeting the inclusion criteria were excluded. Finally, the remaining papers were fully read in order to determine which papers were to be included in the literature review.

Aiming to affirm the quality of the literature, only academic databases were researched to begin with, and only conference papers and journal articles. Additionally, considering the importance of the quality of the papers while conducting a multi-vocal literature review, only top tier, well-recognized literature like international organizational reports and books and well-known magazines and journals in the electronics and counterfeiting industries were considered to be included and cited in the review.

II. The second part of this thesis is practically oriented, with focus on applying the confocal microscopy practices and principles into analyzing the decapsulated semiconductor chips surface in order to create a methodology for efficient counterfeit chips detection.

There are two major approaches for the inspection of electronic devices and components, the electric parametric examinations, and the inspection of the physical properties, interior and exterior, for counterfeiting traces. The electric parametric inspective methods are fast and exclusively designed for specific devices and components, therefore, not suitable for a bigger pool of general results. On the other hand, although physical inspection methods can be time-consuming, they generate better comprehensive solutions.

As the counterfeiting is getting highly sophisticated, the process of physical inspection and detection of such counterfeit electronic components is getting more challenging by the day. One considerable example of such challenges is the fact that counterfeit components no longer have any major exterior defects that could indicate counterfeiting traces by a physical exterior inspection. Additionally, there is a considerable use of counterfeited "recycled" integrated circuits (ICs). [22] Such parts, being originally genuine, appear as the original parts and are being sold as new ICs. Hence, an internal investigation of the structure of the IC is deemed crucial.

Here, however, we are met with another challenge, as most methods of internal inspection are too invasive, such as the usage of chemical substances or physical force. Therefore, the method chosen to be adopted during the practical part of this thesis is the confocal microscopy, also known as Laser Scanning Confocal Microscopy (LSCM). The confocal microscope type used during this thesis is Zeiss LSM700.

1.5 Thesis Structure

This thesis is structured in two main parts: theory and analysis. Additionally, the outline of the chapters is as follows:

Introduction chapter presents an inclusive introduction to the research area of this thesis, followed by a background quantitative and qualitative assessment to provide the reader with information and introduce them to the state of the art of the thesis problem. A problem discussion is also included which ends up in the purpose of this thesis. There is a comprehensive description of the methodology and the structure of the following chapters is outlined.

Chapter II gives a detailed overview of the counterfeit electronic components' problematics. It starts by providing the reader with information regarding the electronic components' manufacturing design and technology, follows with the counterfeit components' origin, and is finalized by the classification of counterfeit types. This chapter aims to provide a comprehensive description of all different types of counterfeit ICs.

Chapter III focuses on identifying and describing the types of risks emerging from using counterfeit electronic components. It also includes short descriptions of the major industries affected.

Chapter IV presents a thorough introduction to confocal microscopy, its principles and methodology. It also includes a study of the advantages and disadvantages of confocal microscopy and, as a result, why it was chosen as the preferred tool in conducting the practical part of this research.

Chapter V gives an overview of the existing methods for detection of counterfeit components and their classification and serves as a bridge to the rest of the thesis.

The following chapters are part of the ***Analysis*** section.

Chapter VI analyses the settings and parameters of the confocal microscope and how they can be optimally used to detect counterfeit components.

Chapter VII describes the process of designing a method for an efficient confocal microscopy outputs evaluation, focusing on the features that are the most optimal to be examined. It also gives a final, concise overview of this methodology.

Conclusion chapter sums up and concludes the thesis.

I. THEORY

II. COUNTERFEIT ELECTRONIC COMPONENTS

Illicit trade in counterfeit electronic components is a major challenge in an innovation-driven global economy. Electronic Integrated Circuits (ICs) altogether with other electronic components form the foundation of all modern systems. Rapidly escalating globalization has caused a dramatic rise in vulnerabilities within the supply chain of electronic components, ICs in particular. Counterfeit ICs have become one of the most serious and major issues faced by the society, industry and governments. Turning into a multibillion-dollar industry and increasing at an unprecedented rate, counterfeit ICs has had a huge impact on the profits of intellectual property (IP) holders alongside their reputation and corporate identity.

A counterfeit electronic component is one whose identity (e.g., date code, lot code, manufacturer) has been purposely misrepresented. Semiconductor Industry Association (SIA) [23] defines counterfeit electronic parts as:

- Unauthorized or substitute copies of a product,
- A product the performance and materials of which have been modified without notice,
- A substandard component misrepresented by the supplier.

There were $169 billion worth of counterfeited electronics and components sold annually in the global market, based on INTERPOL figures. In 2016, the United States Government seized $123,892 million in counterfeit electronics. [24] Data shows that reports of counterfeit components have quadrupled since 2009 – the reporting entities being the Electronic Resellers Association International (ERAI) Inc. [26] and the Government-Industry Data Exchange Program (GIDEP). [27] According to this report, [25] the vast majority of these counterfeit incidents were reported by the electronic firms from the aerospace industry in the US and US-based military bodies.

In the past decade, numerous reports have pinpointed serious counterfeiting issues in the electronic components supply chain in the US. A particular example of this problem is demonstrated by the 2014 Picone case. [28] Peter Picone pled guilty to importing thousands of counterfeit integrated circuits (ICs) from Hong Kong and China with the purpose of reselling them to US customers. What differentiates this case from the others, is the fact that Picone did not solely sell to private consumers, but also targeted the contractor

suppliers of the US navy for use of these counterfeit ICs in nuclear submarines. He assured the contractors that the ICs were manufactured in Europe, as they specifically requested ICs that were new and not produced in China. However, later tests conducted by the US Navy concluded that the ICs purchased from Picone had been resurfaced, the date-code changed, and the counterfeit marks affixed, all this with the intention of selling them as new ICs that are manufactured in Europe.

2.1 Electronic Component Manufacturing Design and Technology

A semiconductor chip can be defined as an electric circuit containing components such as transistors, etc., and wiring on a semiconductor wafer. [3] An electronic device containing many of these components is known as an "Integrated Circuit" (IC). The IC manufacturing process consists of the layout of the part being patterned into a reticle and then projected onto a wafer. During this process there are many inspections included to verify if the patterns are projected as designed. The manufacturing will get interrupted if any defects are found in order to remove them and improve the conditions to correct the imperfections. [3] [41] Nowadays, the biggest silicon wafer has a 300 mm diameter and includes more than 100 semiconductor dies in a single wafer. [41]

There are around 400-600 steps in the general manufacturing process of semiconductor wafer [41], which testifies to the complex techniques and technology used in the electronic components' fabrication. There are two critically important processes that follow the whole manufacturing, the metrology and inspection procedures. Metrology does the overall measurements and calculations regarding the line width, hole diameters, thickness of the thin films located on the surface of the wafer, and the accuracy of the overlay. On the other hand, inspection aims on detecting defects and identifying their locations using position coordinates. The main causes of these defects are generally dust or unwanted particles interfering with the process. [3] [41]

To measure the patterns, lines and dimensions on a semiconductor wafer, a Critical Dimension Scanning Electron Microscope (CD-SEM) is used. Additionally, to review the measurements and defects a Defect Review Scanning Electron Microscope (DR-SEM) is incorporated. [3] Finally, there is an Etch System that is used to create the desired designs and patterns by either using reaction gases, liquid chemicals or ion chemical reaction. [41]

2.2 Counterfeit Components (ICs) Origins

Counterfeit electronic ICs and other electronic components are illegitimate parts that are circulated beyond the authorized supply chain of component manufacturers, authorized distributors, and legitimate aftermarket manufacturers. Counterfeiters have access to scrapped, reclaimed, and excess parts, which are easily available from unofficial sources. Counterfeit components are mostly relabeled components (e.g., marked with a way recent date code, or as a higher grade), refurbished components (e.g., a used component altered to appear new), or a repackaged component (e.g., die recovery and repackaging).

These counterfeit components, as shown in *Figure 2.1*, can originate in any of the sections of the component supply chain. [22]

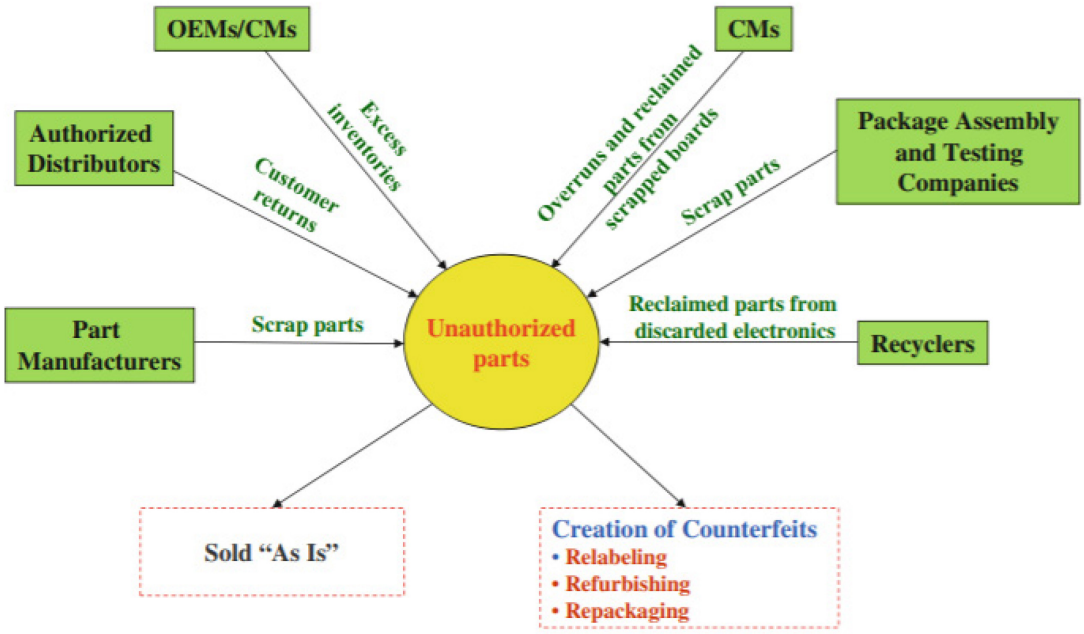

Figure 2. 1 Origin of unauthorized electronic parts from across the supply chain

Note: In Figure 2.1, CM stands for contract manufacturer and OEM stands for original equipment manufacturer.

Excess inventories contain electronic parts that are no longer claimed by product or contract manufacturers for normal production needs. [29] There's a variety of reasons causing excess inventories, among them being the differences between forecast and actual productions scheduling, lag in the discontinuation of slow-going product lines and economic recession. [29] [30] There are quite a few disposal options for excess inventories starting from alternate usage within the company; continuing with the returning these

components to original manufacturers and distributors; disposal of them into the gray (unauthorized) markets; and scrapping the parts. Among the listed disposal options, the selling of them in the gray (illegitimate) markets creates a favorable setting for counterfeiting. Additionally, improper scrapping practices that some companies use to scrap the excess parts in the lack of other disposal options, can also effectuate counterfeiters salvaging those parts. [1] [29] [30] Testing companies and part manufacturers often scrap parts that fail functional tests, quality checks and other screening tests.

More often it happens that these companies do not destroy the components in-house but instead use third parties to perform the procedure, by doing so, leaving room for some of these components to be salvaged by counterfeiters. Some examples of the attributes of scrapped parts consist of manufacturing defects such as lifted wire bongs, die absence, missing bond wires and damaged terminations (e.g., broken leads).

Types of components	Sources	Attributes
Excess inventories	• Original equipment manufacturers (OEM) • Contract manufacturers	• Handling-, packaging- and storage- related damage; • Defects due to aging • No traceability • Unknown pedigree
Scrapped components	• Inspection fallouts from component manufacturers • Testing companies • Contract manufacturers	• Internal quality problems • Die failure & contamination • Part- termination damage
Reclaimed components	• Recyclers	• Damaged terminations and body; • Inherent defects induced during reclamation; • Unknown pedigree

Table 3 Types of components used to create counterfeits

Table 3 shows the sources and attributes of various types of parts that can be used to create counterfeits. [1]

In addition to excess inventories and scrapped parts, there's also the reclaimed parts which have been salvaged from printed circuit boards of damaged electronic assemblies that are scrapped by contract manufacturers.

Most of the time, the traceability (also known as “pedigree”) of these damaged assemblies, is unknown, therefore the components that are reclaimed from such products may have serious undetected defects or degradation. Furthermore, the reclaimed parts may have problems caused during the reclamation process, such as damaged terminations, molding compound damage, and delamination. [31]

2.3 Types of Counterfeit ICs

As the counterfeit component industry is vastly expanding, it is important to know what ICs are most likely to be counterfeited and which are the industries affected the most. *Table 4* shows the top 5 most counterfeited components, based on the data from Information Handling Services (IHS). [1]

Ranks	Component 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%

Table 4 Top-5 most counterfeited semiconductors

Source: IHS parts management

In 2012, these components represented $169 billion in potential annual risk for the global electronics supply chain. As the amount increased exponentially the past decade, the report has little to no change.

The components being: analog ICs, microprocessor ICs, memory ICs, programmable logic ICs, and transistors. Together, these five types of components make up around 68% of all the counterfeit incidents that were reported.

2.4 Classification of Counterfeit Types

The counterfeit components are classified into seven distinct categories. [1] [32] [33] This classification is displayed in *Figure 2.2* [1] [32] [33] and descriptions of each type are given in the subsections below.

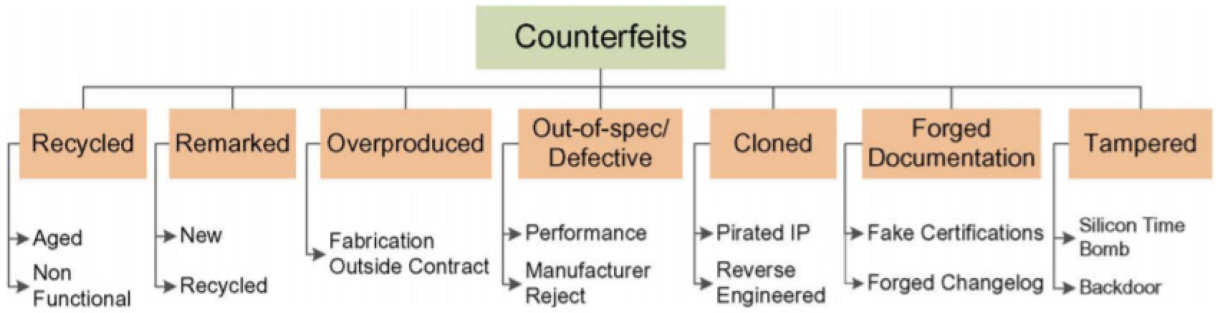

Figure 2. 2 Classification of counterfeit types

The types that draw the major attention in the media are the recycled and remarked components, as they altogether contribute to 80% of counterfeit incidents in test labs, and the industry as a whole. [34]

2.4.1 Recycled

Recycled components can be defined as electronic components which have been reclaimed or recovered from a system and are then modified to be misrepresented as new. Subsequently, these recycled components have lower performance and much shorter service lives due to aging and past usage. The mentioned reclaiming process includes numerous damaging procedures, such as: aggressive physical removal, removal under very high temperatures, ESD exposure, repackaging, etc., and can make the parts completely useless and unfunctional. On the other hand, the defects could be latent and introduced later in the component's life, after passing initial testing. Such parts will, without a doubt, be untrustworthy and potentially cause the failure of the systems that incorporate them.

A typical recycling process goes as the following: [1]

1. Electronic components (analog ICs, digital ICs, capacitors, etc.) are collected and harvested from discarded printed circuit boards (PCBs).

2. The collected PCBs are heated to a high degree, and as the solder joints start to melt the above-mentioned components are detached from the boards.

3. The recycler micro-blasts the component's surface in order to remove its original marking. The most popular blasting agents are: sodium bicarbonate powder, aluminum oxide powder and glass bead.
4. The recycler proceeds to apply a new coating material to the component by using resurfacing and black topping.
5. Information like PIN number, date, lot number, manufacturing company name/logo, etc., are then printed on the new black topped surface.
6. Finally, the component is cleaned and reworked in order to appear as new.

2.4.2 Remarked

Remarked electronic components are those whose important identification information and markings have been removed, tampered and altered. Such markings are the component identifying number (PIN), lot and date identification codes, manufacturers' name and country, electronic discharge sensitivity (ESD), certifications marks, etc., and they serve to uniquely identify these components and their functionality. They introduce the user not only to the origins of the component, but also to the procedures of how they should be handled. A thorough description of these markings can be found in the Department of Defense, Performance specification's report. [35]

A factor that favors remarking of ICs and other electronic components is how fairly easy it is for counterfeiters to change and remodel these markings, and therefore, making them identical to original markings on plain sight. Firstly, the original markings have to be removed chemically or physically before the component is resurfaced and prepared for the remarking. Afterwards the fake markings are printed onto the component making it look like it is genuine. [1]

2.4.3 Overproduced

The complexity and costs of producing high-density ICs has largely increased, influencing a shift to a contract foundry business model (horizontal model).

Such a model is presented in *Figure 2.3* [1] This figure displays the security concerns that rise as a result of this horizontal model. The design houses outsource their works for manufacturing and packaging to companies all around the globe, in order to reduce the production costs. Despite the agreements of producing the exact required amount of

components, the outsourced companies could in fact exceed that amount. Since these third-party companies that deal with the production and assembly are usually overseas, the design houses cannot watch over these processes and monitor the procedures. And here lies the risk, that the components are produced in excess of the agreed amount in order to be sold without the knowledge of the outsourcer design house. [1] [2]

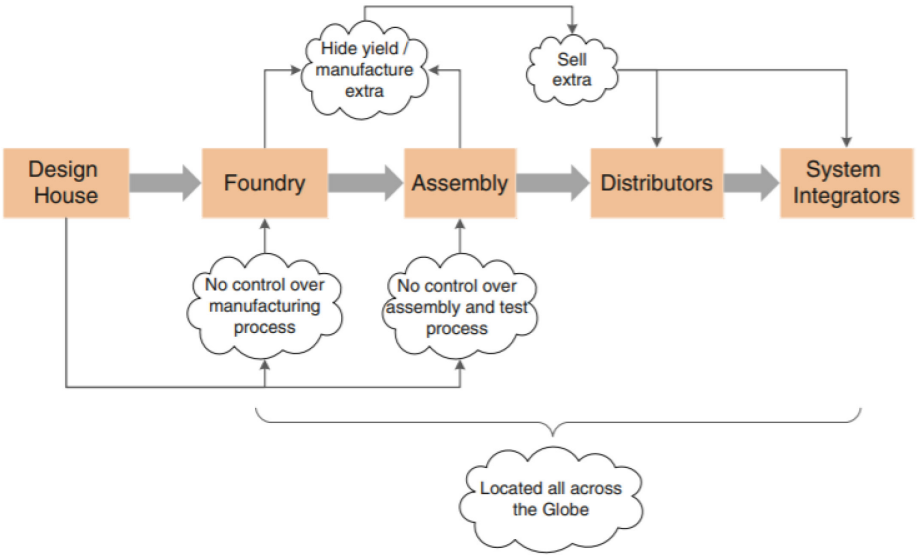

Figure 2. 3 Security issues in the supply chain

The process of exceeding the contracted amount of components and selling outside of the contract with the design house is called "Overproduction." One major concern with overproduction is the profit loss for the design houses, which are not getting any revenue for the sold, overproduced components, although they are the ones investing in large amounts in Research and Development (R&D) of their products.

Additionally, it is as important and concerning the fact that these "overproduced" components are not going through the proper testing of functionality and efficiency, posing serious reliability concerns. Finally, as these components have the same markings and codes of the original company, any failures in their functionality, seriously damages the reputation of the real design houses. [1] [2]

2.4.4 Cloned

As mentioned above, design houses spend enormous amounts of money, time and effort in the R&D department. In order to avoid these costs, or further minimize them, counterfeiters will use a technique called cloning to copy the component's design. There are two major techniques that enable such counterfeiting, the first being reverse

engineering and the second is illegitimate gathering of intellectual property (IP), such as HDL design blocks, netlists, layouts and so on. [1] Reverse engineering (RE) can be defined as the process of analyzing an original component in order to draw information regarding its purpose, nature and functionality. [37] [38]

Based on the proceedings of the 11th International Workshop on cryptographic hardware and embedded systems reverse can be achieved both destructively, which is layer-by-layer, and non-destructively, which is done by reconstructing the whole structure of the part using image processing analysis. [37] [40]

In addition to reverse engineering, cloning can also be made possible by illegally obtaining the necessary data and information regarding the components design from an entity that has access to it. Watermarks like design constraints, signatures, etc., are used as a protective measure of this knowledge and proof of authorship. [1]

2.4.5 Out-of-spec/ Defective

A component is considered defective if it fails one of the post-production quality tests. These post-manufacturing tests are performed in different stages in order to be all-inclusive. *Figure 2.4* shows a typical series of testing. [36]

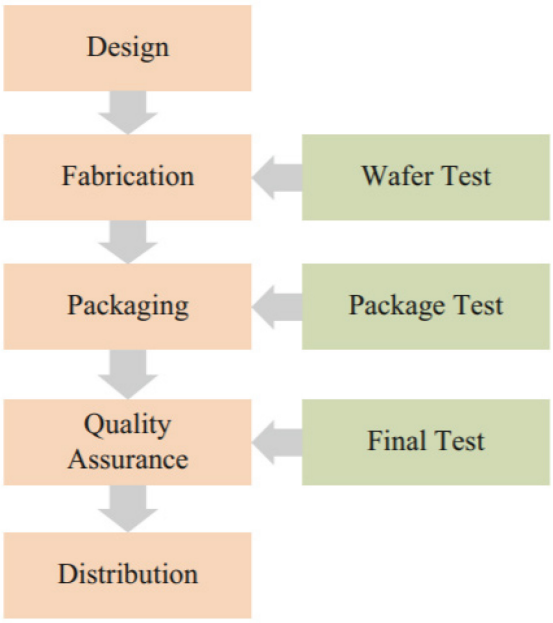

Figure 2. 4 Production series of test

The first test during production is the wafer test, which determines if the ICs produced on the wafer, are defective or not. Based on the number of the defective parts in a wafer sometimes the whole wafer is rejected by the foundry. Depending on the size of the wafer, it could hundreds of ICs which may be worth a lot of money. It is possible for a counterfeiter to sell these defective components to third-party assemblies and therefore, produce out-of-specification ICs. [1]

As the next phase is packaging, the chips undergo the package test. The healthy chips are sorted and packaged, whereas the damaged chips are discarded. Also, at this point, a counterfeiter could use these discarded chips and throw them into the supply chain. Finally, there is a last quality-assurance test before sending the packaged parts into the market.

Usually, this test consists of a burn-in, in high voltage/ temperature, in order to test latent defects and avoid early operational failures of the chips.

All the components that fail any of the above-mentioned tests, should be properly disposed of. But in many cases, they are either stolen or consciously sold in the market by a trusted entity.

In ways of detecting these out-of-spec chips the difficulty increases with how many of the stages' tests the chips passed already during production. Thus, chips that only failed the final test are extremely difficult to distinguish from the other original, legitimate parts.

2.4.6 Tampered

Tampering can be achieved by using hardware Trojans, and by circuit editing the components after manufacturing. The mentioned hardware Trojans can interrupt a component's functionality and its usual operations at the moment they have been inserted into a part. [1]

Moreover, they could open a backdoor, giving access to a malicious third party to the critical systems and top-secret information. For example, a hardware Trojan could easily disable the crypto-module of a part and therefore expose critical data as unencrypted plain text. [2] Regarding the circuit editing of the components, counterfeiters use technologies of nanoscale manipulation like the focused ion beam (FIB) and it has been reported that they have managed to rework the circuit netlist in widths of 20 nm and pitch of 40 nm. [1] [2] [40]

2.4.7 Forged documentation

Beside the components themselves being unauthentic, there is also the matter of the documentation accompanying them, which generally contains information related to the parts' specifications, functionality, testing, statement of work (SoW) and certificates of conformance (CoC). If this documentation is forged, the components can be illegally sold as authentic, while being defective or completely non-functional. Another issue is the difficulty of verifying the authenticity of the documentation as data may not be available by the OCM. [1] Forged documentation can be paralleled with remarking regarding its basis on deceiving and misrepresenting.

III. RISKS OF USING COUNTERFEIT COMPONENTS

The electronic component counterfeiting is a worldwide pandemic affecting all industries and segments of the market. A US Department of Commerce report [42] issued in January 2010, by the Office of Technology Evaluation (OTE) gives deep insight into the state of counterfeit electronics as stated below:

- "all elements of the supply chain have been directly impacted by counterfeit electronics.
- there is a lack of dialogue between all organizations in the U.S. supply chain,
- companies and organizations assume that others in the supply chain are testing parts,
- lack of traceability in the supply chain is commonplace,
- there is an insufficient chain of accountability within organizations,
- recordkeeping on counterfeit incidents by organizations is very limited,
- most organizations do not know who to contact in the U.S. Government regarding counterfeit parts,
- stricter testing protocols and quality control practices for inventories are required;
- most DOD (Department of Defense) organizations do not have policies in place to prevent counterfeit parts from infiltrating their supply chain." [42]

Considering that the counterfeiting of electronic components had directly impacted all elements of the supply chain since 2010, the growth of threats in today's industry can be well-presumed.

3.1 Types of Risks Emerging from Counterfeit Components

Counterfeit electronic components have major effects in the industry, consumers and society as a whole. The risks vary from the social impacts, to financial losses, and finally, even posing life-endangering threats.

3.1.1 Financial Risks

Counterfeit electronic components cost the semiconductor manufacturing companies more than $7.5 billion annually in lost avenue in the US, according to the statistics taken from Semiconductor Industry Association (SIA). [23]

Moreover, a separate investigation made by the Information Handling Services (HIS), [43] states that these counterfeit electronic components represent $169 billion in potential annual risk for the global electronics business. The financial costs do not only apply to the Original Component Manufacturers (OCM) but affect the society as a whole. For example, as the counterfeiters do not pay any taxes, they affect the entire economy of a city/country. Furthermore, counterfeiting of electronic components will eventually cost the consumer, as the counterfeiters are unfairly profiting from another company's name and reputation to deceive the customers. At the end of the day, the consumers are getting an inferior good for an excessive price. On an important note, the counterfeit numbers mentioned this far are not the total number of counterfeit parts, but the number of these counterfeits that were found and reported.

3.1.2 Social Risks

In addition to the financial risks of counterfeit electronic components, there are also numerous social threats. To begin with, counterfeiting causes serious damage to the image and reputation of the legitimate companies. Since there are a lot of customers who may not realize the component is fake, when they fail to work accordingly, and do not meet their expectations, then the consumer ends up blaming the original company. Either by word of mouth, or leaving negative reviews online, these customers can have a huge impact on the company's online presence and reputation.

Another social cost comes from the fact that counterfeiters generally have poor working conditions, they do not pay their employees fair wages and often use forced or child labor. Additionally, while being an illegal activity, counterfeiting supports organized crime. According to International Anticounterfeiting Coalition (IAC) [8] the profits from counterfeiting sales have been linked to funding organized crime, drug trafficking and even terrorist activity.

3.1.3 Health & Safety Risks

While the financial and social risks are quite important, nothing compares with the "Health & Safety" issues caused by the presence of counterfeit, defective electronic components, as they put the public at tremendous risk of harm, and even death. [44]

Defective counterfeit electronic components may end up being part of case-sensitive medical equipment, avionics, automotive, and many other critical systems, where its malfunctioning could pose severe or even lethal outcomes. On *Subsection 4.2* below, there is a description of these risks in the industries affected the most by counterfeit electronic components.

3.2 Industries Affected by Counterfeit Components

As the majority of industries have been infiltrated by counterfeit electronic components, here is a list with the industries which are significantly and fundamentally affected.

3.2.1 Medical Equipment

Medical equipment refers to implantable devices, small stationary equipment and large infrastructure equipment. All the mentioned equipment requires high-reliability and functionality, as they use life-critical applications. For example, medical imaging systems, electronic implants, resuscitation systems, Magnetic Resonance Imaging (MRI) are just a few of these systems.

While legacy devices are used, the issue rises for the hospitals, health clinics and all medical institutions, to have a reliable and dependable supply of replacement parts. Defective parts could have serious effects on the patients, starting from misdiagnosis, to even loss of life.

3.2.2 Automotive Electronics

Automotive electronic applications and devices need improved process controls and have specific requirements made to withstand temperature extremes. Process controls communicate with the rest of the integrated system including drive relays, sensors, motors, injectors, solenoids and lamps. The most complex device for harsh-environment automotive electronics is currently the engine controller. Furthermore, the high current and power circuitry need large traces. On an important note, automotive electronics have two more crucial requirements, being long life and high reliability in order for the product

warranty to extend to as long as 10 years. [42] The counterfeit components will most definitely cause severe damage to these systems.

3.2.3 Aerospace & Military

The aerospace and military (defense) industry have products that require impeccable performance on demand, in numerous harsh environments, and moreover, must maintain this performance over long, continuous service lives. As a result of these long service lives, systems must rely on legacy devices to sustain and develop existing systems. Aerospace and military systems need comprehensive testing to meet performance requirements and their designs are ruggedized (modified) to meet the vibration, temperature, humidity, fog, salt, and other reliability and environmental requirements related to Department of Defense (DoD) platforms. Therefore, these industries need to have an authentic, legitimate supply chain that ensures the functionality and reliability of the devices and components to meet the security requirements. [42] [44]

3.2.4 High-End Systems

High-end systems include three major categories: data centers, communications and high-performance computing. Communications has become an integral part of enterprise computing, and the technology advancements have enabled a denser integration of computing technologies and communications in commercial systems. This has caused for the computing and networking hardware to gain more common electronic components. And so, creating a window for the counterfeit electronic components to infiltrate even the high-performance computers, server farms, data centers, switches, routers and other service electronic equipment. [44]

3.2.5 Consumer Goods

Although the consumer goods have been increasing in complexity; the main drivers are the increase in functionality and reduction in cost while simultaneously searching for ways of continuously declining the system footprint. This is the sector of industry that has the shortest product life, and is cost-sensitive, therefore the most serious vulnerabilities are product "skimming", cloning, remarking, tempering and recycling. [42] [44]

IV. INTRODUCTION TO CONFOCAL MICROSCOPY

Confocal microscopy, also known as laser scanning confocal microscopy (LSCM) or confocal laser scanning microscopy (CLSM), can be defined as an optical imaging technique that increases contrast and optical resolution by using a spatial pinhole to avoid out-of-focus light in image formation. [5] [48] The basic concept of confocal microscopy lies in a technique called optical sectioning, which is the reconstruction of three-dimensional structures by capturing numerous two-dimensional images at various depths in a sample. [6] Optical sectioning is a well-known technique, extensively used in the industrial and scientific communities. Some typical applications are material science, semiconductor inspection and life sciences. [4] [5] [6] [49]

4.1 Basic Concept and Principles

Confocal imaging aims to overcome some limitations of traditional wide-field fluorescence microscopes [47] and the principle of it was patented 1957 by Marvin Minsky. [46]

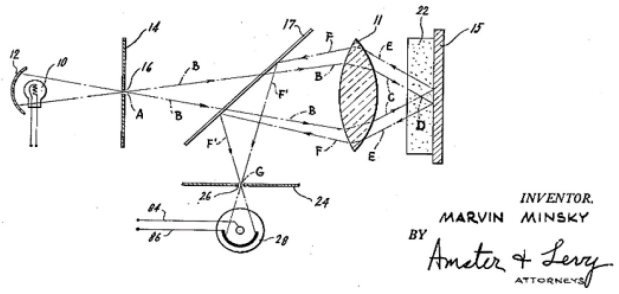

Figure 4. 1 Minsky's patent: Confocal Point Sensor Principle [46]

While in a conventional fluorescence microscope the entire sample is flooded uniformly with a light source, a confocal microscope uses a pinhole and point illumination to eliminate out-of-focus light (as shown in *Figure 4.2*) – the name confocal derives from this configuration. [45] However, long exposure is often required as the most part of the light is blocked at the pinhole, and the resolution is increased at the cost of signal intensity. So, in order to readjust the decrease in signal after the pinhole, the intensity of the light is examined by a sensitive detector, such as a photomultiplier tube (PMT), converting the light signal into an electrical one. [48] 2D and 3D imaging needs scanning over a regular pattern (i.e., a rectangular or square pattern of parallel scanning lines) in the sample, as only one point at a time is illuminated through the pinhole. So, the beam is scanned in the horizontal plane using vacillating mirrors. The speed of this scanning method varies and is

directly correlated with the signal-to-noise ratio, meaning the slower the scanning, the better the contrast. [48]

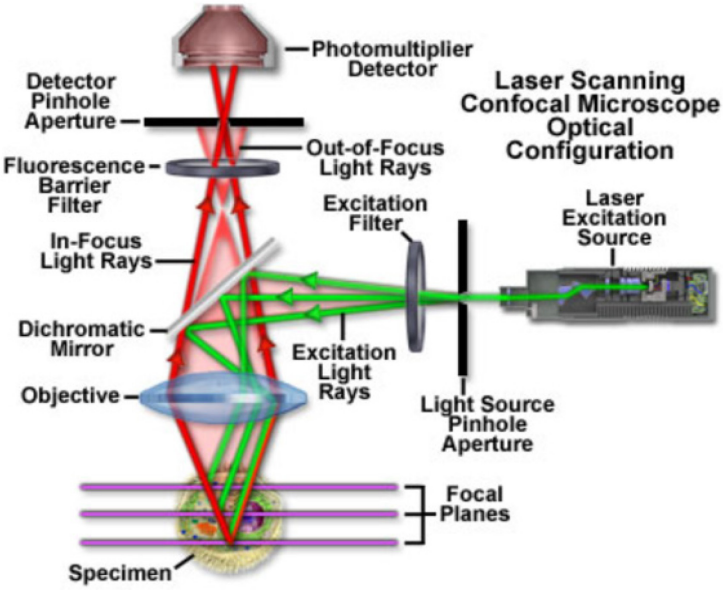

Figure 4. 2 The confocal principle in laser scanning microscopy [49]

At the heart of the confocal microscope system is the scan head, which is responsible for converting the excitation scans into a raster image, as well as gathering the photon signals from the sample (specimen) that are needed to assemble the ultimate image. A typical scan-head includes inputs from the fluorescence filter sets, external laser sources, and dichromatic mirrors, pinhole cuts for developing the confocal image, a galvanometer-based scanning mirror raster system, varying tube detectors adjusted for different fluorescence wavelengths. [49]

4.2 Types of Confocal Microscopes

There are four types of confocal microscopes [5] [6] [48] [49] currently available:

1. The Laser Scanning Confocal Microscope (LSCM), which uses multiple mirrors (usually around 2 or 3) to scan the laser linearly across the sample and "de-scan" the image across the fixed pinhole and detector. [5] [6]

2. Spinning-Disk Confocal Microscope (also known as Nipkow disk), which uses a number of moving pinholes set on a disc to scan spots of light in the sample. As a number of pinholes scans an area in parallel, each of them is allowed to be over a specific area for longer, therefore decreasing the excitation energy required to illuminate a specimen compared to LSCM. Reduced excitation energy also lowers

the phototoxicity and photobleaching of a sample typically making it the preferred system for the imaging of live cells and organisms. [5] [6] [48]

3. Dual Spinning-Disk or Microlens Enhanced Confocal Microscope (MECM) is quite similar to the spinning-dick confocal microscope, the only difference being a second spinning-disk consisting of micro-lenses located before the first spinning-disk which contains the pinholes. Every microlens is associated with a pinhole. The role of these micro-lenses is to capture a larger amount of light and manage it focus it all on each pinhole, and by doing so, significantly intensifying the amount of light going into each pinhole. [5]

4. Programmable Array Microscope (PAM) uses spatial light modulator (SLM) which is electronically controlled and creates a set of moving pinholes. In practice, PAM allows numerous pinholes to scan the same area parallelly, given that the pinholes are sufficiently apart from each other. [6] [49]

4.3 Advantages and Disadvantages of Confocal Microscopy

The primary advantage of confocal microscopy is the non-invasive sectioning technique that facilitates the examination of the sample (specimen) under various conditions with intensified clarity. Laser scanning confocal microscopes are able to produce thin (0.5-1.5 μm) optical sections through samples that have a width ranging up to 50 μm (micrometres) or more. Image information is not affected by any signal arising from different remote areas of the sample, but is focused in a well-defined plane. Compared to widefield techniques, the reduction of the background fluorescence and the enhanced signal-to-noise, have dramatically improved contrast and definition. Moreover, the optical sectioning manages to eliminate fluorescent staining and artefacts that typically occur during physical sectioning with the traditional forms of microscopy. [49]

Another advantage is given by the technological software advancements which can generate vertical sections in x-z and y-z planes, in addition to the horizontal x-y plane. Practically, the vertical sections are acquired by merging numerous x-y scans taken along the z- axis by using the software, and then creating and projecting the image as it would look like if the hardware of the confocal microscope had been capable of executing a vertical section. [49] Therefore, is able to give a 3D representation of the desired image during the specimen inspection. The 3D software packages can create either a single 3D

representation of the sample or even a video incorporating different angles of the sample's volume. Furthermore, a lot of software packages offer some extra benefits such as conducting different measurements (length, depth, volume) and other specific characteristics of the images (i.e., opacity) that can be modified to expose the desired internal structures at varying levels within the sample. Additional advantages of confocal microscopy consist of the ability to electronically modify magnification of the laser-scanned area without having to alter objectives. This feature is called the zoom factor and is typically used in adjusting the sample's spatial resolution by altering the sampling period, resulting in a higher number of samples, higher image spatial resolution and magnified display on the monitor. The zoom factor also matches the optical resolution with the digital image resolution when low magnification and aperture objectives are employed to collect the data. [49] Finally, the processed digital data and images of the sample can be easily printed and published.

Regarding the disadvantages of confocal microscopy, they are primarily related to the restricted number of excitation wavelengths accessible with average lasers, which are quite costly to produce in the ultraviolet spectrum. However, regular widefield microscopes use xenon-based or mercury arc-discharge lamps to arrange a full range of wavelengths in the visible, ultraviolet and near-infrared spectrums.

Another disadvantage is the harmful and unhealthy nature that the high-intensity laser irradiation has to living cells and tissues. Lastly, purchasing and operating multiple-user confocal microscope systems can be highly expensive, costing much more than the widefield microscopes, therefore cannot be afforded in smaller laboratories. A solution to this problem would be implementing cost-sharing confocal microscope systems that are used in two or more departments of a facility. Moreover, recently personal confocal systems have also been introduced with lower prices for the down-end confocal microscopes which has raised the number of individual users. [49]

The numerous technical and practical advantages mentioned above make confocal microscopy a desired method in semiconductor inspection. Therefore, it was chosen by the author, as well as suggested by the thesis supervisor, as the preferred set of tools and procedures in conducting the practical part of this thesis. Fortunately, the disadvantages do not apply to the environment of this thesis, as Tomas Bata University is well-equipped with a confocal microscope system and the damage caused to living cells is not applicable to semiconductor chip surface.

V. DETECTION OF COUNTERFEIT COMPONENTS

This chapter gives an overview of the counterfeit detection methods available and their main classification and serves as a bridge to the rest of the analysis chapters that follow.

5.1 Counterfeit Detection Methods

Over the past decade, several counterfeit components detection methods have been created and implemented. These methods can generally be classified into three main categories: physical inspections, electrical inspections and aging-based fingerprints, where the first two are the most significant ones. *Figure 5.1* shows a generalized classification of counterfeit components detection methods base on a study from the Institute of Electrical and Electronics Engineers (IEEE). [16]

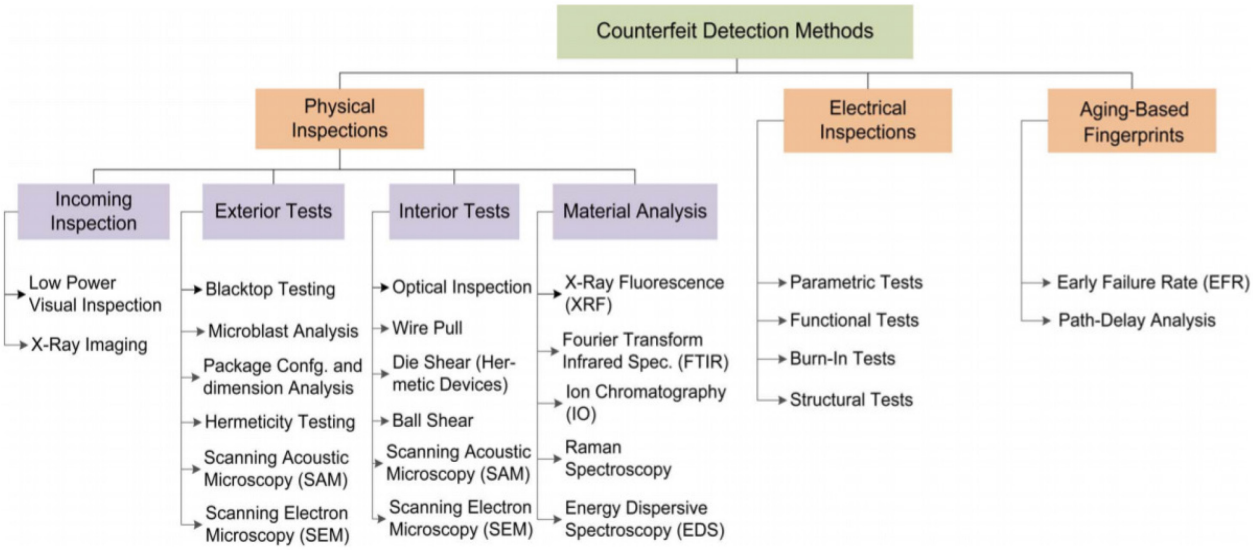

Figure 5. 1 Classification of Counterfeit Detection Methods

Source: IEEE [16]

5.1.1 Physical Inspections

The physical inspection methods are divided into four categories, as shown in the figure above. Those counterfeit detection methods include:

- Incoming Inspection (Low Power Visual Inspection and X-Ray Imaging) where every component is inspected thoroughly. Exterior Tests (Blacktop Testing, Microblast Analysis, Package Configuration and Dimension Analysis, SAM and SEM) where it is the packages that are inspected and analyzed to find anomalies or defects indicating counterfeiting.

- Interior Tests (Optical Inspections, Wire Pull, Die Shear, Ball Shear, SAM and SEM) where the components are decapsulated and then internally inspected.
- Material Analysis (X-Ray Fluorescence, FTIR, Ion Chromatography, Raman Spectroscopy and EDS) where the analysis aims to find the defects or anomalies related to the material of the package, die, and leads. [15] [16] [20] [50]

Studying decapsulated chip surface with confocal microscopy follows under the Interior Tests of the Physical Inspection Category.

5.1.2 Electrical Inspections

Electrical inspections are used to check the electrical parameters of the electronic components in order to differentiate between genuine and counterfeit ones. This category is also divided into four subcategories as follows:

- Parametric Tests which efficiently identify IC's direct current (DC) and alternating current (AC) parameters.
- Functional Tests which detect any defect or anomaly that can affect the functionality of the component, like bond wires (broken/ missing), open interconnect, cracks, etc.
- Burn-in Tests which aim to find rapid failures in stressed conditions, such as high temperatures, in order to insure reliability.
- Structural Tests which aim to find the anomalies and defects regarding the internal structure of the component, logic gates and interconnect. [15] [16] [20] [50]

5.1.3 Aging-Based Statistical Fingerprints

With time, the overall performance of the electronic components continuously degrades due to various aging mechanisms. The performance and functionality of new devices would significantly reduce if we were to use a recycled IC instead of a brand-new one. Some of the most common aging phenomena consist of electromigration, hot carrier injection (HCI), negative bias temperature instability (NBTI) and time-dependent dielectric breakdown (TDDB). [15] [16] [20] [50] The methods used to detect counterfeit ICs related to these aging phenomena are Early Failure Rate (EFR) Data Analysis and Circuit Path-Delay Analysis.

II. ANALYSIS

VI. CONFOCAL MICROSCOPE PARAMETERS

A crucial point of the process of using confocal microscopy as a tool to detect counterfeit decapsulated chips is setting the right operating parameters. The Laser Scanning Confocal Microscope Zeiss LSM700 has an abundance of tools and functionalities which can actively be combined in numerous different ways depending on the purpose, operation and usage. For the purpose of this thesis, the goal is setting the right combination of parameters, tabs and tools in order to succeed in creating a methodology for an efficient confocal microscopy outputs evaluation aimed at differences between genuine and counterfeit chips.

This chapter will provide the reader with a concise but complex approach to setting the confocal microscope operating parameters. The very first steps consist of *Starting the system* by switching on the LSM 700 system (can be done via the switch-operated multipoint connectors), switching on scanning stage and *Starting the Zen software* (Zen Black for the laser-based instruments and Zen Blue for widefield microscopes and cameras).

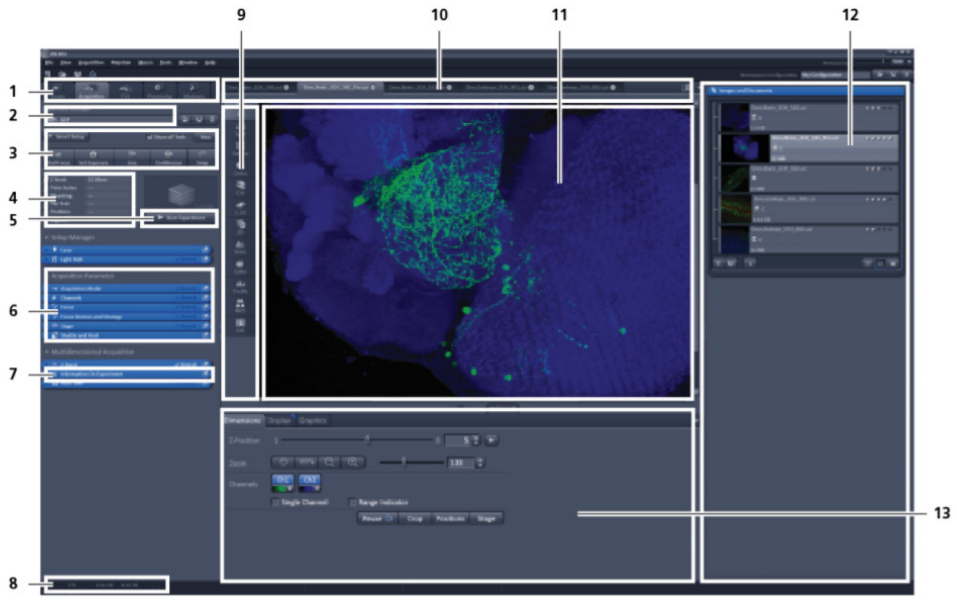

Figure 6. 1 ZEN Application Window Overview

Figure 6.1 shows the ZEN application window immediately after startup. This is what each tab in the image above stands for:

1 - Main tool tabs
2 - Configuration
3 - Action buttons
4 - Multidimensional tool section panel
5 -Starting multidimensional experiments
6 - Tool group
7 - Tool
8 - Status bar
9 - View tabs
10 - Image tabs
11 - Displayed image
12 - File handling area
13 - View Controls

Since the laser-based instruments are in the focus and scope of this thesis, the focal point is going to be the Zen Black software. Upon running the software, the user will have to choose *Start System* tool which will initialize the entire confocal microscope system and activate the whole software package pertaining new image acquisition and analysis. This immediately offers all of ZEN's features in the newly opened window. The most significant tab is *Acquisition* as it contains the most important tools for the experiments. Find Focus, Set Exposure, Live and Continues mode, Snap are in the Experiment bar. They serve to offer digital visuals of the sample while starting the laser scanning experiment. The laser tool has the power to switch lasers on/off and also shows all available lasers that can be operated. This tab is shown in *Figure 6.2* below.

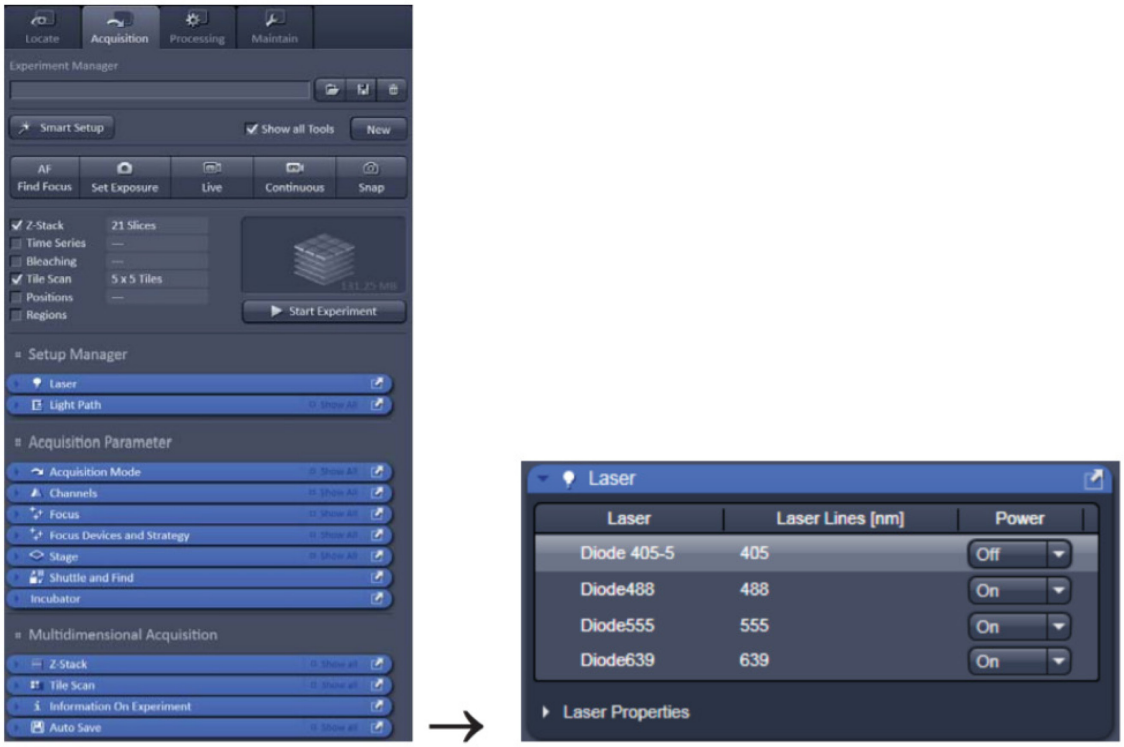

Figure 6. 2 Acquisition Tab and Laser Tool Overview

After Laser selection, you can proceed to the laser scanning phase where the Z-stack tool is employed. This tool allows the user to select the upper and lower limit coordinated (Set First and Set Last), time and/or number of "slices" that determine the creation of a 3D digital representation of the sample. A high number is undoubtedly more detailed, but not necessarily more efficient as it is highly time-consuming.

As mentioned in the theoretical part of the thesis, one of the most important aspects differentiating confocal microscopy from other types of microscopes is the use of a so-called pinhole to eliminate out-of-focus light and artifacts resulting from it. To properly set this this crucial function the user has to access the Channels tool in the Acquisition tab. To reach the best compromise between depth discrimination and detection efficiency it is recommended to set the Pinhole to 0.3 AU (Airy unit).

VII. COUNTERFEIT COMPONENTS DETECTION USING CONFOCAL MICROSCOPY

Laser Scanning Confocal Microscopy (LSCM) as a tool of counterfeit components detection falls under the category of physical inspections mentioned in *Chapter 5*. As the counterfeiting is getting highly sophisticated, the process of physical inspection and detection of such counterfeit electronic components is getting more challenging by the day. One considerable example of such challenges is the fact that counterfeit components no longer have any major exterior defects that could indicate counterfeiting traces by a physical exterior inspection. Additionally, there is a considerable use of counterfeited "recycled" integrated circuits (ICs). [22] Such parts, being originally genuine, appear as the original parts and are being sold as new ICs. Hence, an internal investigation of the structure of the IC is deemed crucial. LSCM can create a 3D reconstruction of the sample's surface by collecting a "stack" or series of focal planes or otherwise known as "slices" in the LSCM application. Therefore, this technique offers a direct comparison of the differences in surface roughness, surface texture, depth of laser markings, and also different curvature and warping in a microscopic range.

LSCM technique and methodology can be applied to certain counterfeit types, such as recycled, remarked, cloned, defective and tampered chips, as they usually contain counterfeiting traces in the surface of the chip itself. When considering overproduced and forged documentation types of counterfeiting there could be other detection techniques that are more suitable and time-efficient in determining whether the chip is genuine or not.

This approach presumes the accessibility of the data on the genuine IC of the same type, to provide a baseline with which to compare the results obtained from LSCM of the presumed counterfeit.

7.1 Preliminary Studies Using a Coin

This Subsection lays out the baseline study performed as an exploratory part of the practical experimentation. It consists of studying different ways to use the LSCM tools and functions in the most optimized form and most efficient approach. The goal of this preliminary research initially was to “pave the way” for the study of decapsulated chip surface which is considerably smaller and particularized.

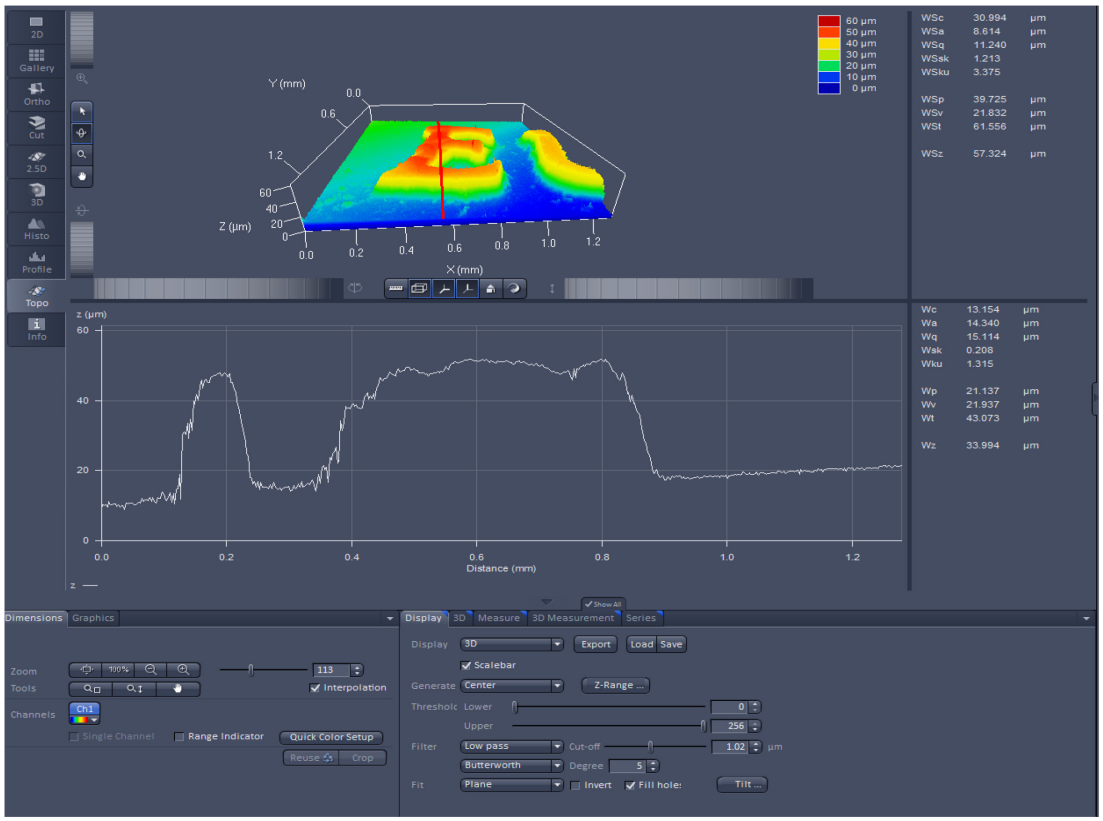

Figure 7. 1 Image Processing Overview

As an exploratory research to establish the feasibility of LSCM in counterfeit components detection, preliminary results were obtained on the sample of a small 10 cent coin.

Figure 7.1 shows an overview of two important taskbars, the vertical taskbar on the left and the horizontal one below. Out of all the Tabs in the vertical taskbar, the most important ones, as far as this research goes, are 3D, Profile and Topography. 3D tab offers a reconstruction of the sample based on the laser-scanning technique.

The Profile tab, in *Figure 7.2*, shows the rate of the intensity in relation to the absolute frequency used over a certain part of the sample or the whole sample itself. It displays three markers or reference points, based on which it analyzes the data considering distance and intensity.

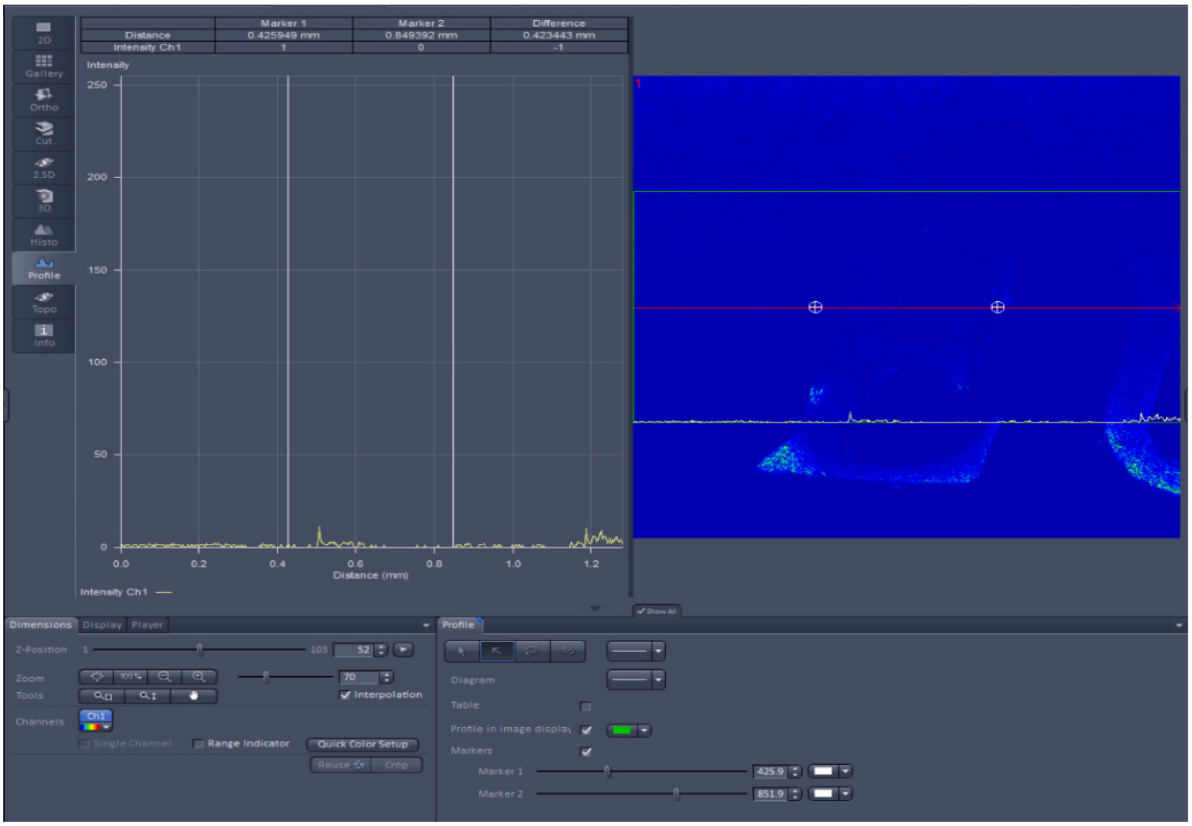

Figure 7. 2 Profile Tab Overview

Meanwhile in the horizontal taskbar we have the Dimensions tab and based on the vertical taskbar tab that is chosen, there is also another functionality that could be Display – 3D – Measure – 3D Measurement – Series, or another set of Profile tab, Histogram and Gallery.

As shown in *Figure 7.3*, here are some tools like zoom, channels and quick color setup where the user can change the way depth and height is displayed and what do different colors stand for. The interpolation and range indicator should be checked for better results.

In the Display tab, as shown in *Figure 7.4*, the user can choose the display form (which in our case should be 3D), should tick Scalebar, for timely measurement detailed information, and among other things can play with the different options of displaying the sample's optical replica by customizing the threshold, filter, fit and range.

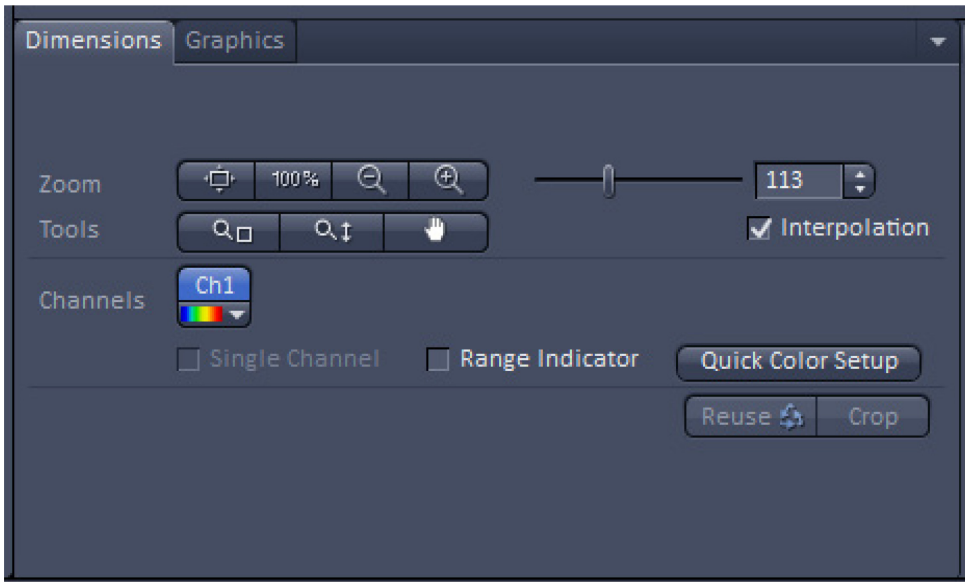

Figure 7. 3 Dimensions Tab Overview

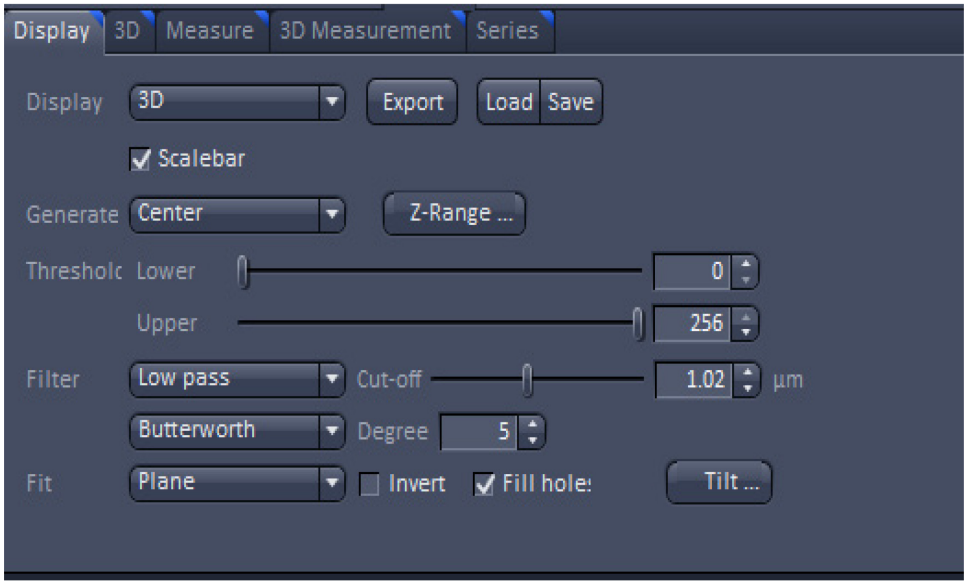

Figure 7. 4 Display Tab Overview

The 3D tab is quite rich in functionalities, offering different settings for Profiles (A), Grid (B), Filled (C) and Surface (D), each having their own sub-settings and details interacting with the user interface and customizable to their needs and intentions. Below are the visual representations of each of the tabs from A to D.

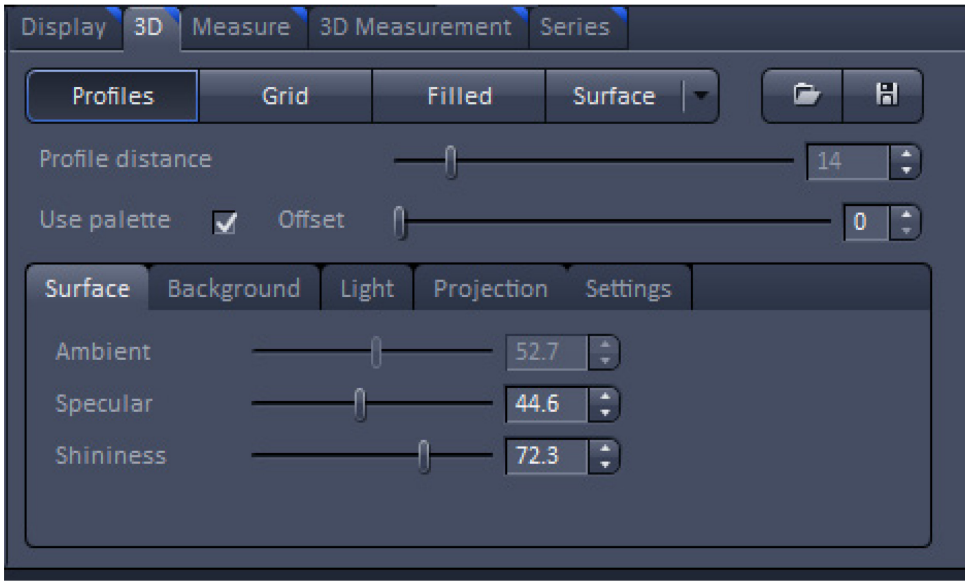

Figure 7.5. A

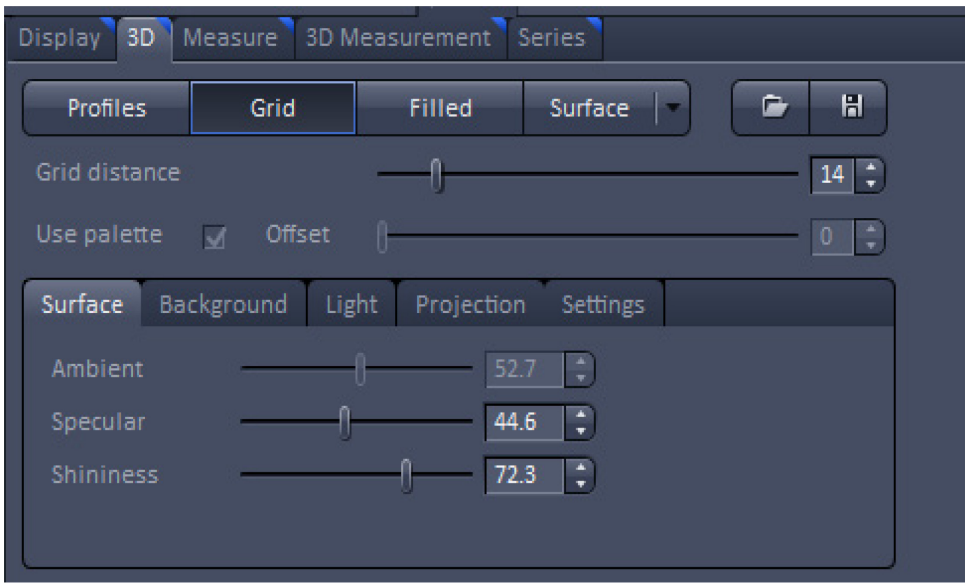

Figure 7.5. B

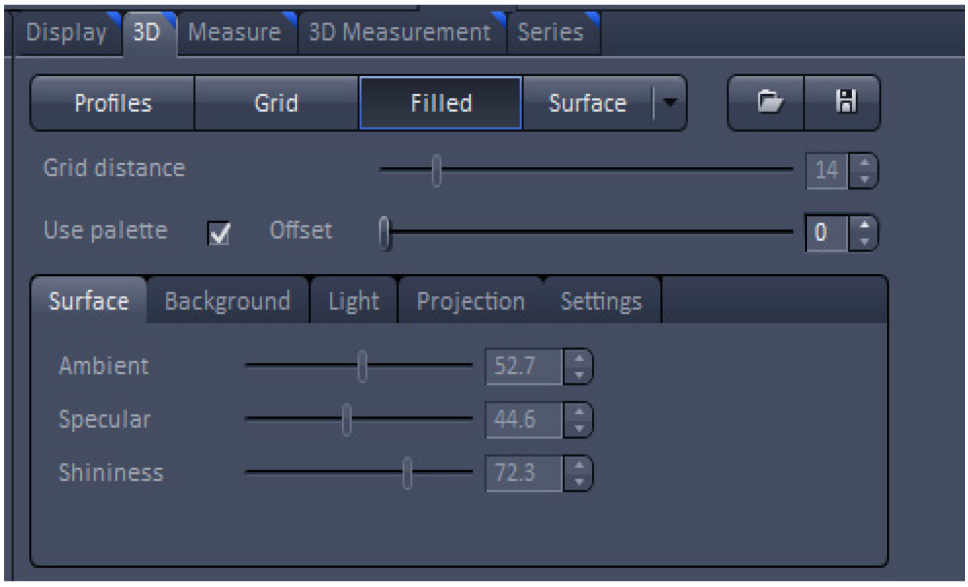

Figure 7.5. C

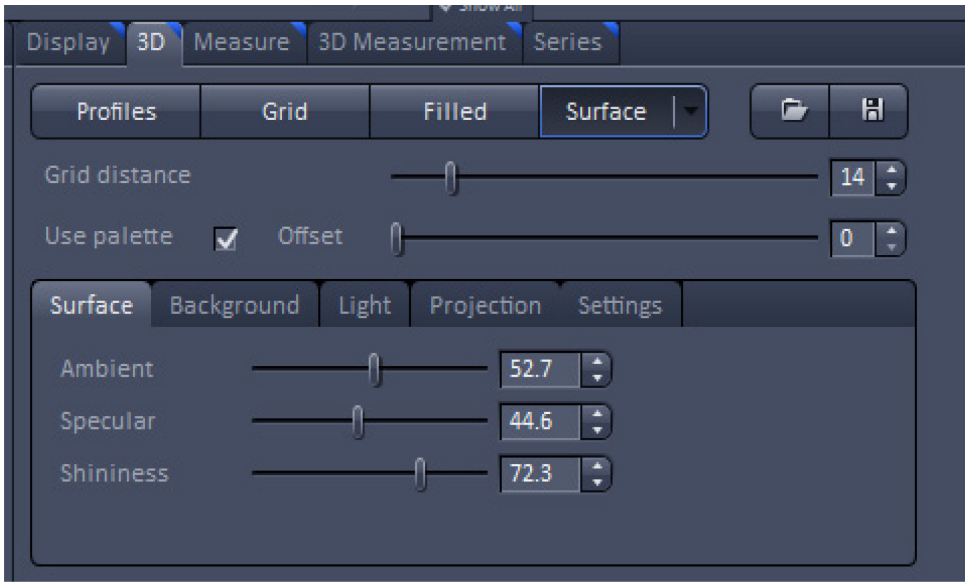

Figure 7.5. D

Figure 7. 5 The 3D Tab Overview

Another important indicator is Roughness in the Measure tab, shown in *Figure 7.6*, which contains surface roughness information needed regarding the sample. More 3D information like the Volume and Z-level can also be provided.

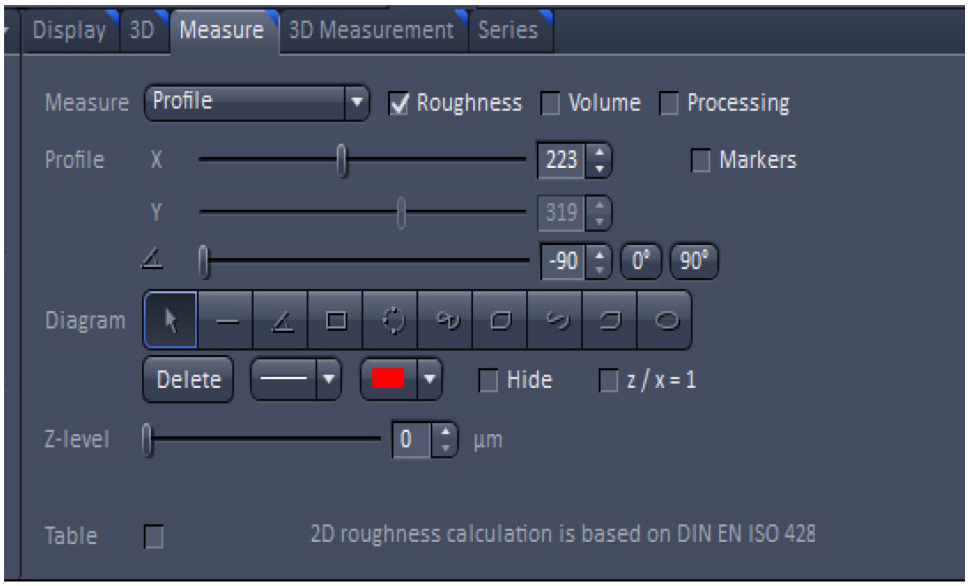

Figure 7. 6 Measure Tab Overview

7.2 Preliminary Studies Results

As mentioned previously, the purpose of this preliminary study using LSCM to examine the surface of a coin was to "pave the way" for the study of decapsulated chip surface by studying different ways to use the LSCM tools and functions in the most optimized form and providing the most efficient approach. The different tabs, tools and functions of Zen Black software of the LSCM available to the researcher were explored. A set of the most crucial parameters was identified and their optimal settings for obtaining the most conclusive result set were established.

As a result of adhering to this set of parameters and settings, we managed to gain important information regarding our sample's surface attributes. The 3D visual reconstruction of the sample's surface recreated by the LSCM offered a wide range of information regarding the surface roughness, surface texture, depth of markings, and also different curvature and warping in a microscopic range. This assortment of information could easily be compared to a parallel assortment of a "genuine" sample information obtained in exactly the same manner, following the same steps. By comparison of these two result sets, the user can reach a reasonably certain conclusion on authenticity of the sample.

As each and every examined sample has its own unique set of characteristics, the optimal settings for various parameters are, of course, going to slightly differ. However, as a general guide or methodology, the parameter sets obtained and described in this thesis are sufficient. Over the course of this study, a step-by-step approach to the proper setup for the LSCM through the Zen Black software was outlined and its results can be seen throughout the previous subsection. To make this more approachable, an easy-to-follow overview is provided in the next subchapter. After gathering all these highly promising results from this preliminary stage of the research, the decision to move forward was reached as the LSCM can be of great benefit in detecting counterfeit ICs, as recycled, remarked, cloned, defective and tampered chips generally contain counterfeiting traces in their surface, and these can be detected by the LSCM while adhering to the proposed methodology.

7.3 Counterfeit Components Detection Methodology Overview

As mentioned in the previous subchapter, to make the created methodology more approachable, concise and user-friendly, an easy-to-follow overview is provided below.

After starting the LSM 700 system, switching on the scanning stage and starting the Zen Black software, the user should choose ***Start System*** mode to acquire new images or ***Image Processing*** mode to edit already existing images. In the main window after the startup, the ***Left Tool Area*** is where the user will find the most relevant and crucial functionalities needed for an efficient implementation of this methodology to detect counterfeit components. These main functionalities to recognize and examine are sample observation, image acquisition, image processing and system maintenance. To begin with, the ***Oculars Online*** button should be turned on in the ***Locate*** tab or else the user will not be able to have real time visuals of the specimen and observe the changes take effect immediately.

The most essential feature to be mentioned is ***Image Acquisition*** and all its tools in the ***Acquisition*** tab. Starting from top to bottom, in the ***Smart Setup*** tab, the ***Linear unmixing*** has proven to be the most optimal setup during the practical part of this thesis, offering both speed and best signal. In the experiment bar, the user should click the ***Set Exposure*** button or the ***Snap*** button to start a new image document. Afterwards, it is really important to turn on the relevant laser that is going to be used during the procedure, in the ***Laser Control*** tool. Regarding the ***Acquisition Mode*** bar, the scan mode should be a ***Frame*** and the number of pixels should be set to ***Highest***. When it comes to the ***Scan Speed*** slider the user will have to make the choice between setting it to 8 for the fastest results or setting the scanning speed to 6 or 7 for higher quality images. In the ***Bit Depth*** pull-down 12 Bit should be chosen as it gives 4096 gray levels. In the ***Channels*** tool, the ***Pinhole*** should be set to 0.3 AU (Airy Unit) to achieve the optimal compromise between detection efficiency and depth discrimination, and the ***Gain*** can be adjusted for this chosen pinhole size and given laser power. For image optimization it is important to activate the ***Range Indicator*** check box, in the ***View – Dimensions*** tab.

After going through all the aforementioned settings, it is the time for the scanning itself through the ***Z-stack*** tool. At this point, the user needs to click the ***Continuous*** button and use the focus drive of the confocal microscope on the upper part of the specimen area and click on ***Set First***.

Afterwards, the focus drive can be used to focus the lower specimen area and the user can click on the ***Set Last*** button to set this as the lower position. Then, the Smallest button should be clicked, and the experiment can start by clicking the ***Start Experiment*** button on the top of the toolbar. It is really important to manually ***Store*** and ***Export*** the image data as it is not done automatically. Save and Save As buttons are located in the ***File*** menu on top.

After repeating the same procedure with a genuine IC of the same type, a comparison between the two result sets can be performed and a conclusion on the authenticity of the IC can be reached.

VIII. CONCLUSION

The main purpose of this thesis was to design a methodology for an efficient confocal microscopy outputs evaluation aimed at differences between genuine and counterfeit chips. To begin with, a thorough, multi-vocal literature review was conducted to provide the reader with the baseline information on the thesis research area and familiarize them with all the necessary terms, definitions and procedures needed to comprehend the practical experimentation results and conclusions.

Among other things, an introduction to the current state of counterfeit components was presented, alongside with the necessary background information and problem discussion. It was deemed important to give an overview of the counterfeit components origins and types, and naturally, an outline of the numerous types of risks that using counterfeit parts brings to different industries. Moreover, an inclusive presentation of the basic principles and types of confocal microscopy was implemented, describing the main advantages and disadvantages of this method and, therefore, stating the reason why it was chosen as the preferred tool in conducting the practical part of this thesis.

Over the course of this research on practical application of confocal microscopy as a convenient tool for detection of counterfeit Integrated Circuits (ICs), the desired step by step methodology was designed and tested on a substitute sample.

Due to unforeseen circumstances, resulting in the destruction of the control elements of the LSCM available to the researcher during a storm, a follow-up study with the use of real ICs was impossible. Therefore, the conclusions of this thesis are based on extrapolation from results obtained in the preliminary, exploratory research phase.

This research concluded that Laser Scanning Confocal Microscopy can be of great benefit in detecting counterfeit ICs, as recycled, remarked, cloned, defective and tampered chips generally contain counterfeiting traces in their surface which are easily identifiable by the Laser Scanning Confocal Microscope while adhering to the proposed methodology.

8.1 Future Recommendations

As mentioned above due to unforeseen circumstances during a storm and resulting destruction of the control elements of the Zeiss LSM700 (the confocal microscope available to the researcher), a follow-up study with the use of real ICs was impossible. The conclusions of this thesis are based on extrapolation from results obtained in the preliminary, exploratory research phase with the use of a coin as a sample, therefore, a sequent study implementing the designed methodology in detecting counterfeit ICs is suggested.

To further expedite the process of counterfeit ICs detection on an industrial scale, the LSCM method can prove as a viable tool for continuous evaluation of test pieces. Possibly all decapsulated/delided chips of various semiconductor components can be compared to a database which includes an open collection of confocal signatures (features) according to the component type, component technology, its origin (supplier), etc.

A creation of such a database could prove an enormously valuable asset in the fight against electronic components counterfeiting because it would mean the authentic ICs' parameters and features would always be within reach for the comparison with all suspicious parts. Of course, a database of this kind would need a state-of-the-art security due to its sensitive nature and the fact that a data leak could prove disastrous in the hands of the counterfeiters.

Furthermore, as the technology continues to progress, the tools and methodologies used in counterfeit chips detection will also improve and upgrade. Some future possibilities could be further research and development in the technology of aging detection sensors, such as ring oscillators and machine learning aging sensors. [51] [52] [53]

Another promising area of research is the Physical Unclonable Function (PUF) method which generates a device-specific output by using production variability. This output, in a way, can be seen as the fingerprint of a device. [51] [54] [55] As a future recommendation, several security and cryptography applications of PUF can be improved and further developed. For example, the secret-key generation requires an error-free operation which is difficult to guarantee, but there is space for upgrade and advancement. [54] [55]

BIBLIOGRAPHY

[1] Tehranipoor, Mark (mohammad), Guin, U., & Forte, D. (2016). Counterfeit integrated circuits: Detection and avoidance. Cham, Switzerland: Springer International Publishing.

[2] Tehranipoor, Mohammad, Salmani, H., & Zhang, X. (2013). Integrated circuit authentication: Hardware Trojans and counterfeit detection (2014th ed.). Cham, Switzerland: Springer International Publishing.

[3] Nishi, Y., & Doering, R. (Eds.). (2017). Handbook of semiconductor manufacturing technology, second edition. doi:10.1201/9781420017663

[4] Hawkes, P. W., & Spence, J. C. H. (Eds.). (2008). Science of Microscopy (1st ed.). New York, NY: Springer.

[5] Paddock, S. W. (Ed.). (2013). Confocal microscopy: Methods and protocols (2nd ed.). doi:10.1007/978-1-60761-847-8

[6] Price, R. L., & Jerome, W. G. (jay) (Eds.). (2016). Basic confocal microscopy. New York, NY: Springer.

[7] "Definition Of COUNTERFEIT". Merriam-Webster.Com, 2021

https://www.merriamwebster.com/dictionary/counterfeit.

[8] "What Is Counterfeiting | International Anticounterfeiting Coalition". International Anticounterfeiting Coalition, 2021, https://www.iacc.org/resources/about/what-is-counterfeiting.

[9] "Counterfeiting. "Encyclopedia of American Law, edition 2nd. 2008. The Gale Group 16 Mar. 2021 https://legal-dictionary.thefreedictionary.com/counterfeiting

[10] Böhm, Christoph, and Maximilian Hofer. Physical Unclonable Functions in Theory and Practice. 1st ed., Springer-Verlag New York, 2013, pp. 270 / 278, Accessed 16 Mar 2021.

[11] Wilcox, K., Kim, H., Sen, S. (2009), “Why do Consumers buy Counterfeit Luxury Brands?”, Journal of Marketing Research, Vol. 46, Issue 2, pp. 247-259.

[12] "Trends in Trade in Counterfeit and Pirated Goods". Oecd.Org, 2019, https://www.oecd-ilibrary.org/trade/trends-in-trade-in-counterfeit-and-pirated-goods_g2g9f533-en Accessed 20 Mar 2021.

[13] "Sales Value Losses from Fake Goods, By Industry Worldwide 2020 | Statista". Statista, 2021, https://www.statista.com/statistics/1117921/sales-losses-due-to-fake-good-by-industry-worldwide/.

[14] Razavi, Maysa and Lori S Schulman. "Counterfeiting and Data Privacy: Achieving the Right Balance in Consumer Protection | World Trademark Review". Worldtrademarkreview.Com, 2020, https://www.worldtrademarkreview.com/anti-counterfeiting/counterfeiting-and-data-privacy-achieving-right-balance-consumer-protection Accessed 20 Mar 2021.

[15] G. Mura, R. Murru, G. Martines, Analysis of counterfeit electronics, Microelectronics Reliability, Volume 114, 2020, ISSN 0026-2714, https://doi.org/10.1016/j.microrel.2020.113793

[16] K. Huang, J. M. Carulli and Y. Makris, "Counterfeit electronics: A rising threat in the semiconductor manufacturing industry," 2013 IEEE International Test Conference (ITC), Anaheim, CA, USA, 2013, pp. 1-4, Doi: 10.1109/TEST.2013.6651880

[17] Gilmore, E.T., Frazier, P.D., Collins, I.J. et al. Infrared analysis for counterfeit electronic parts detection and supply chain validation. Environ Syst Decis 33, 477–485 (2013). https://doi.org/10.1007/s10669-013-9482-1

[18] Henry Livingston. Avoiding Counterfeit Electronic Components[J]. IEEE Transactions on Components and Packing Technologies, 2007(1): Pages 187-189.

[19] Liu Ping. Identification and Analysis on Counterfeit Electronic Components[J]. Electronic Components and Materials, 2012(2).

[20] Mura, G. et al. "Analysis of Counterfeit Electronics". Microelectronics Reliability, vol 114, 2020, p. 113793. Elsevier BV, Doi: 10.1016/j.microrel.2020.113793.

[21] B. Kitchenham, “Procedures for performing systematic reviews,” Software Engineering Group, Keele University & Empirical Software Engineering, National ICT Australia Ltd., Tech. Rep., 2004

[22] M. Pecht, The counterfeit electronics problem, Open J. Soc. Sci. 01 (2013) 12–16, https://doi.org/10.4236/jss.2013.17003

[23] Semiconductor Industry Association (SIA) Anti-Counterfeiting Task Force (2016)

[24] McKeefry, Hailey Lynne. "Counterfeits Costing Semiconductor Industry Billions - EE Times Asia". EE Times Asia, 2021, https://www.eetasia.com/counterfeits-costing-semiconductor-industry-billions/.

[25] J. Cassell, Reports of counterfeit parts quadruple since 2009, challenging US Defense Industry and National Security Pressroom (April 2012), http://press.ihs.com/press-release/designsupply-chain/reports-counterfeit-parts-quadruple-2009-challenging-us-defense-in

[26] ERAI, Report to ERAI, http://www.erai.com/information_sharing_high_risk_parts

[27] GIDEP, Government-Industry Data Exchange Program (GIDEP), http://www.gidep.org/

[28] U.S. Department of Justice, Massachusetts man pleads guilty to importing and selling counterfeit integrated circuits from China and Hong Kong (June 2014), http://www.justice.gov/opa/pr/2014/June/14-crm-595.html

[29] K. Chatterjee, D. Das, Semiconductor manufacturers' efforts to improve trust in the electronic part supply chain. Compon. Packag. Tech. IEEE Trans. 30(3), 547–549 (2007)

[30] K. Chatterjee, D. Das, M. Pecht, P. Suorsa, C. Ricci, Solving the counterfeit electronics problem. Proceedings of Panpacific Microelectronics Symposium (SMTA), Jan. 30–Feb. 1, pp. 294–300, 2007

[31] K. Snider, A time for change: the not so hidden truth behind the Chinese open market. ERAI special report, 2007

[32] U. Guin and M. Tehranipoor, ''On selection of counterfeit IC detection methods,'' in Proc. IEEE North Atlantic Test Workshop, May 2013.

[33] U. Guin, M. Tehranipoor, D. DiMase, and M. Megrdician, ''Counterfeit IC detection and challenges ahead,'' in ACM SIGDA E-Newslett., vol. 43, no. 3, Mar. 2013.

[34] SAE International, ''Counterfeit electronic parts; Avoidance, detection, mitigation, and disposition,'' 2009. [Online]. Available: http://standards.sae.org/as5553/

[35] Department of Defense, Performance specification: hybrid microcircuits, general specification for (2016).

[36] L.-T. Wang, C.-W. Wu, X. Wen, VLSI Test Principles and Architectures: Design for Testability (Systems on Silicon) (Morgan Kaufmann, San Francisco, 2006).

[37] R. Torrance, D. James, The state-of-the-art in IC reverse engineering, CHES ’09. (Springer, 2009, Berlin), pp. 363–381. http://dx.doi.org/10.1007/978-3-642-04138-9_26

[38] I. McLoughlin, Secure embedded systems: the threat of reverse engineering, in Parallel and Distributed Systems, 2008. ICPADS ’08. 14th IEEE International Conference on (December 2008), pp. 729–736

[39] R.J. Abella, J.M. Daschbach, R.J. McNichols, Reverse engineering industrial applications. Comput. Ind. Eng. 26(2), 381–385 (1994), http://dx.doi.org/10.1016/0360-8352(94)90071-X

[40] CHASE, CHASE workshop on secure/trustworthy systems and supply chain assurance (April 2014), https://www.chase.uconn.edu/chase-workshop-2014.php

[41] Keiji Kojima, Keiji, and Takashi Iizumi. "1. Semiconductor Manufacturing Process: Hitachi High-Tech GLOBAL" (2021)

https://www.hitachihightech.com/global/products/device/semiconductor/manufacturing.html

[42] U.S. Department of Commerce, Bureau of Industry and Security, Office of Technology Evaluation, Defense Industrial Base Assessment: Counterfeit Electronics, January 2010. http://www.bis.doc.gov/defenseindustrialbaseprograms/osies/defmarketresearchrpts/final_counterfeit_electronics_report.pdf

[43] Gorman, C., 2012. IEEE Spectrum: Technology, Engineering, and Science News. Available at: https://spectrum.ieee.org/riskfactor/computing/hardware/the-financial-risks-of-counterfeit-semiconductors Accessed 1 Apr 2021.

[44] U.S. Chamber of Commerce’s Global Intellectual Property Center, *Counterfeits and Their Impact on Consumer Health and Safety.* April 27, 2016, U.S. Senate Committee on The Judiciary https://www.judiciary.senate.gov/meetings/counterfeits-and-their-impact-on-consumer-health-and-safety Accessed 1 Apr 2021.

[45] Pawley JB (editor) (2006). Handbook of Biological Confocal Microscopy (3rd ed.). Berlin: Springer.

[46] Marvin Minsky (1988). "Memoir on inventing the confocal scanning microscope". Scanning. 10 (4): 128–138. doi:10.1002/sca.4950100403.

[47] Memoir on Inventing the Confocal Scanning Microscope, Scanning 10 (1988), pp128–138.

[48] Fellers TJ, Davidson MW (2007). "Introduction to Confocal Microscopy". Olympus Fluoview Resource Center. National High Magnetic Field Laboratory. Accessed 2 Apr 2021.

[49] Fellers, Thomas J., and Michael W. Davidson. "Introduction to Confocal Microscopy". Olympus-Lifescience, 2021, https://www.olympus-lifescience.com/en/microscope-resource/primer/techniques/confocal/confocalintro/ . Accessed 3 Apr 2021.

[50] E. Oriero, S.R. Hasan, "Survey on recent counterfeit IC detection techniques and future research directions", Integration, the VLSI J 66 (2019) 135–152.

[51] Enahoro Oriero, Syed Rafay Hasan, "Survey on recent counterfeit IC detection techniques and future research directions", Integration, Volume 66, 2019, Pages 135-152, ISSN 0167-9260, https://doi.org/10.1016/j.vlsi.2019.02.006.

[52] Preston D. Frazier, E. Thomas Gilmore, Isaac J. Collins, Mohamed F. Chouikha, "Novel counterfeit detection of integrated circuits via infrared analysis: a case study based on the Intel Cyclone II" FPGAs Machine Learning and Cybernetics (ICMLC), 2016 International Conferenceon, IEEE (2016), pp. 404-409

[53] Navid Asadizanjani, Nathan Dunn, Sachin Gattigowda, Mark Tehranipoor, Domenic Forte "A database for counterfeit elec- tronics and automatic defect detection based on image processing and machine learning", Proceedings of the 42nd International Symposium for Testing and Failure Analysis. Texas, USA (2016), pp. 1-8

[54] Böhm Christoph, Maximilian Hofer "Physical Unclonable Functions in Theory and Practice", Springer Science & Business Media (2012)

[55] Y. Lao, B. Yuan, Ch. Kim, K. K. Parhi, "Reliable PUF-based local authentication with self-correction" IEEE Trans. Comput. Aided Des. Integr. Circuits Syst., 36 (2) (2017), pp. 201-213

LIST OF ABBREVIATIONS

BASCAP - Business Action to Stop Counterfeiting and Piracy

CD-SEM - Critical Dimension Scanning Electron Microscope

CLSM - Confocal Laser Scanning Microscopy

CM - Contract Manufacturer

DOD - Department of Defense

DR-SEM - Defect Review Scanning Electron Microscope

ERAI - Electronic Resellers Association International

ESD - Electrostatic Discharge Sensitivity

EUIPO – European Union Intellectual Property Office

FDI - Foreign Direct Investment

FIB - Focused Ion Beam

GIDEP - Government-Industry Data Exchange Program

IAC - International Anticounterfeiting Coalition

IC - Integrated Circuits

ICC - International Chamber of Commerce

IEEE - Institute of Electrical and Electronics Engineers

IHS – Information Handling Services

INTA - International Trademark Association

LPVI – Low Power Visual Inspection

LSCM - Laser Scanning Confocal Microscopy

MECM – Microlens Enhanced Confocal Microscope

OCM - Original Component Manufacturers

OECD - Organization for Economic Cooperation and Development

OEM - Original Equipment Manufacturer

OTE - Office of Technology Evaluation

PAM - Programmable Array Microscope

PCB - Printed Circuit Board

PIN – Part Identifying Number

PMT - Photomultiplier Tube

PUF - Physical Unclonable Function

RE - Reverse Engineering

SAM – Scanning Acoustic Microscopy

SEM - Scanning Electron Microscopy

SIA - Semiconductor Industry Association

SLM - Spatial Light Modulator

USDHS - United States Department of Homeland Security

WCO - World Customs Organization

LIST OF FIGURES

LIST OF TABLES