Boston University Theses & Dissertations

Boston University Theses & Dissertations

2016

# Modeling and model-aware signal processing methods for enhancement of optical systems

https://hdl.handle.net/2144/19504 Downloaded from DSpace Repository, DSpace Institution's institutional repository

### BOSTON UNIVERSITY COLLEGE OF ENGINEERING

Dissertation

# MODELING AND MODEL-AWARE SIGNAL PROCESSING METHODS FOR ENHANCEMENT OF OPTICAL SYSTEMS

by

#### AYDAN AKSOYLAR

B.S., Sabanci University, 2010M.S., Boston University, 2015

Submitted in partial fulfillment of the

requirements for the degree of

Doctor of Philosophy

2016

© 2016 by AYDAN AKSOYLAR All rights reserved

### Approved by

First Reader	
	M. Selim Ünlü, Ph.D. Professor of Electrical and Computer Engineering Professor of Biomedical Engineering Professor of Materials Science and Engineering
Second Reader	
	Bennett B. Goldberg, Ph.D.
	Professor of Physics
	Professor of Biomedical Engineering
	Professor of Electrical and Computer Engineering
Third Reader	
	Ajay Joshi, Ph.D. Associate Professor of Electrical and Computer Engineering
Fourth Reader	
	Matthew Brand, Ph.D.
	MERL Fellow, Mitsubishi Electric Research Laboratories
Fifth Reader	
	W Clem Karl Ph D
	Professor and Chair of Electrical and Computer Engineering
	Professor of Biomedical Engineering
	Professor of Systems Engineering

#### Acknowledgments

I am deeply grateful to my advisors, Prof. M. Selim Unlü and Prof. Bennett B. Goldberg for their support and guidance during my PhD studies. Thanks to their support, I have been privileged to work on many interdisciplinary projects that helped me gain extensive knowledge and experience. I would like to thank Prof. Ünlü for his continuous encouragement and for trusting me with all the projects I was assigned, since the first day I joined his group. I would like to thank Prof. Goldberg for his help in giving directions to my research and his invaluable feedback.

I would like to extend my thanks to my committee members, Prof. Ajay Joshi, Dr. Matthew Brand and Prof. Clem Karl. I would like to thank Prof. Joshi for being available when I needed further critique on my research; his collaboration helped my dissertation become stronger. I feel lucky to have Dr. Brand as my host during my internship at MERL. I appreciate all his time and efforts in guiding and contributing to my internship work (in Chapter 4). I learned a lot from his approach to research. I would like to thank Prof. Karl for his insightful feedback on my dissertation.

I have had the privilege to work with many talented scientists during my PhD studies. In particular, I would like to thank Dr. Berkin Cilingiroglu and Dr. Abdulkadir Yurt for their help in my research. I learned a lot from them when I started working on my dissertation project. I would like to thank Dr. Ronen Adato for his collaboration on the work in Chapter 3. In addition, I would like to thank Boyou Zhou, Oguzhan Avci, Kyle Vigil, Negin Zaraee, Dr. Mahmoud Zangeneh, Dr. Yang Lu and Dr. Helen Fawcett for their collaboration.

I would like to thank my fellow graduate students Ahmet, Berkin, Emir, Limor, Marc, Oguzhan, Theodora and everyone in the OCN lab for their friendship. I wish to thank the ECE staff, especially Cali Stephens for helping things run smoothly.

Last but not least, I would like to thank my loving family. They have been a

constant source of support and love. My parents have always believed in me to reach my goals. Most of all, I would like to thank my beloved husband, Cem for always being there to support me whenever I needed. He was the biggest support and inspiration during most difficult times.

### MODELING AND MODEL-AWARE SIGNAL PROCESSING METHODS FOR ENHANCEMENT OF OPTICAL SYSTEMS

#### AYDAN AKSOYLAR

Boston University, College of Engineering, 2016

Major Professors: M. Selim Ünlü, Ph.D. Professor of Electrical and Computer Engineering Professor of Biomedical Engineering Professor of Materials Science and Engineering Bennett B. Goldberg, Ph.D. Professor of Physics

Professor of Physics Professor of Biomedical Engineering Professor of Electrical and Computer Engineering

#### ABSTRACT

Theoretical and numerical modeling of optical systems are increasingly being utilized in a wide range of areas in physics and engineering for characterizing and improving existing systems or developing new methods. This dissertation focuses on determining and improving the performance of imaging and non-imaging optical systems through modeling and developing model-aware enhancement methods. We evaluate the performance, demonstrate enhancements in terms of resolution and light collection efficiency, and improve the capabilities of the systems through changes to the system design and through post-processing techniques. We consider application areas in integrated circuit (IC) imaging for fault analysis and malicious circuitry detection, and free-form lens design for creating prescribed illumination patterns. The first part of this dissertation focuses on sub-surface imaging of ICs for fault analysis using a solid immersion lens (SIL) microscope. We first derive the Green's function of the microscope and use it to determine its resolution limits for bulk silicon and silicon-on-insulator (SOI) chips. We then propose an optimization framework for designing super-resolving apodization masks that utilizes the developed model and demonstrate the trade-offs in designing such masks. Finally, we derive the full electromagnetic model of the SIL microscope that models the image of an arbitrary sub-surface structure.

With the rapidly shrinking dimensions of ICs, we are increasingly limited in resolving the features and identifying potential modifications despite the resolution improvements provided by the state-of-the-art microscopy techniques and enhancement methods described here. In the second part of this dissertation, we shift our focus away from improving the resolution and consider an optical framework that does not require high resolution imaging for detecting malicious circuitry. We develop a classification-based high-throughput gate identification method that utilizes the physical model of the optical system. We then propose a lower-throughput system to increase the detection accuracy, based on higher resolution imaging to supplement the former method.

Finally, we consider the problem of free-form lens design for forming prescribed illumination patterns as a non-imaging application. Common methods that design free-form lenses for forming patterns consider the input light source to be a point source, however using extended light sources with such lenses lead to significant blurring in the resulting pattern. We propose a deconvolution-based framework that utilizes the lens geometry to model the blurring effects and eliminates this degradation, resulting in sharper patterns.

### Contents

1	Intr	oduction	1
	1.1	Integrated circuit imaging	1
	1.2	Illumination with free-form lenses	3
	1.3	Organization and contributions	4
<b>2</b>	Bac	kground and Related Work	6
	2.1	Spatial resolution	6
	2.2	Solid immersion lenses for subsurface imaging of integrated circuits .	8
		2.2.1 Central and aplanatic solid immersion lenses	8
		2.2.2 Optical model for solid immersion microscopy of integrated circuits	10
	2.3	Hardware Trojan detection	11
	2.4	Free-form lenses for illumination	13
3 Performance of subsurface aplanatic solid immersion microscopy		formance of subsurface aplanatic solid immersion microscopy for	
	inte	grated circuit imaging	16
	3.1	Green's function derivation for the aSIL microscope $\hdots$	16
	3.2	Performance in bulk silicon chips	22
	3.3	Performance in silicon on insulator chips	31
	3.4	Super-resolution through pupil mask engineering	38
		3.4.1 Mask parametrization and objective function	42
		3.4.2 Gaussian Process optimization	44
		3.4.3 Simulation results	45
	3.5	Full electromagnetic model of an aSIL microscope	49

		3.5.1	Focused light	51
		3.5.2	Interaction of the light with the sample	52
		3.5.3	Far-field propagation	53
		3.5.4	Image formation on the detector	54
		3.5.5	Simulation results	57
	3.6	Concl	usions	60
4	Gat tegi	e class rated c	sification methods for detecting malicious tampering of in circuits	- 62
	4.1	Rapid	identification of gates using multi-spectral reflectance measure-	
		ments	at low resolution	63
		4.1.1	Model of the system	65
		4.1.2	Gate identification	66
	4.2	Identi	fication of gates with improved accuracy using high resolution	
		imagin	ng	77
		4.2.1	Dictionary learning	80
		4.2.2	Gate classification using dictionary coefficients	85
	4.3	Concl	usions	88
<b>5</b>	Free	e-form	lens illumination with extended light sources	91
	5.1	Shift-	variant deconvolution framework	92
		5.1.1	Partitioning the lens	93
		5.1.2	Blur kernel estimation	95
		5.1.3	Deconvolution	95
	5.2	Result	s and discussion	99
		5.2.1	Physical set-up and parameters	99
		5.2.2	Experimental and simulation results	101
		5.2.3	Discussion	110

	5.3	Conclusions	111
6	Con	clusion	112
	6.1	Summary and Conclusions	112
	6.2	Future directions	114
References		117	
Curriculum Vitae 1		125	

## List of Figures

$1 \cdot 1$	Progression of MOSFET gate length and component density. Adapted	
	from (Schwierz, 2010)	2
$2 \cdot 1$	(a) Rayleigh, (b) modified Rayleigh, (c) Sparrow and (d) Houston	
	resolution criteria. Obtained from (Köklü, 2010)	7
$2 \cdot 2$	(a) Conventional, (b) cSIL, (c) aSIL subsurface imaging. R denotes the	
	radius of the sphere.	9
$2 \cdot 3$	Schematic illustrating an aSIL microscope	10
$2 \cdot 4$	Schematic illustrating the metal layers (M1–M3) of an IC. Obtained	
	from (Wittmann, 2007)	12
$2 \cdot 5$	Schematic illustrating a free-form lens that forms the image of a target	
	pattern on a projection surface	14
3.1	Schematic of the aSIL system for the Green's function derivation. $\ .$ .	17
$3 \cdot 2$	Detection of evanescent waves. Red and green areas correspond to	
	forbidden light and allowed light regions respectively	23
$3 \cdot 3$	The logarithm of the electric field intensity distribution for horizontal	
	(left column) and vertical dipoles (middle column) for (a) $d = 0$ , (b)	
	d = $\lambda_{ins}/2$ , (c) d = $\lambda_{ins}$ . The size of each image is 8 mm by 8 mm. A	
	cross-section of the intensity profile as a function of $\theta_{\rm obj}$ at $\phi=0$ for	
	(d) horizontal, (e) vertical dipole	25
$3 \cdot 4$	Wave-front aberrations due to forbidden light (in radians) in (a) $E_{\theta}^{\text{GRS1}}$ ,	
	(b) $E_{\phi}^{\text{GRS1}}$ for horizontal dipole and (c) $E_{\theta}^{\text{GRS1}}$ for vertical dipole	26

3.5Normalized wide-field detector images of a horizontal dipole when d = 0 (top row) and  $d = \lambda_{ins}$  (bottom row). Intensity images when the (a,d) full angles, (b,e) only subcritical angles, (c,f) supercritical angles are collected. The size of each image is  $3\lambda_{\rm ins} \times Magnification$ by  $3\lambda_{\rm ins} \times {\rm Magnification}$ . The intensity values are normalized to the 283.6Normalized wide-field detector images of a vertical dipole when d = 0(top row) and  $d = \lambda_{\text{ins}}$  (bottom row). Intensity images when the (a,d) full angles, (b,e) only subcritical angles, (c,f) supercritical angles are collected. The size of each image is  $3\lambda_{ins} \times Magnification$  by  $3\lambda_{ins} \times$ Magnification. The intensity values are normalized to the maximum 293.7Collection efficiency and spot-size (in x and y axes) as a function of the dipole distance from the dielectric interface for horizontal (left) and vertical (right) dipole. Note that the intensity distribution for the vertical dipole is circularly symmetric, resulting in the same spot-size 30 Simulated images of a test structure when (a) d = 0, (b)  $d = \lambda_{\text{ins}}/2$ , 3.8(c)  $d = \lambda_{\text{ins}}$ . The size of each image is  $8.3\lambda_{\text{ins}} \times \text{Magnification}$  by  $17.7\lambda_{\rm ins} \times {\rm Magnification}$ . The intensity of each panel are normalized to 30

3.9	(a) Layout and (b) simulated image of a test structure with wires	
	at different depths. L1 and L2 are located at $d = \lambda_{\rm ins}/2$ , where L2	
	and L3 are located at $d = \lambda_{\text{ins}}$ . The scalebar in(a) corresponds to a	
	length of $\lambda_{\text{ins}}$ . The size of each image is $10.11\lambda_{\text{ins}} \times \text{Magnification}$ by	
	$7.28\lambda_{\rm ins}\times {\rm Magnification.}$ (c) Cross-section of the image taken along the	
	dotted line in (b)	31
$3 \cdot 10$	Schematic of the problem for objects located in the substrate and ultra-	
	thin silicon layer for bulk silicon and SOI technology respectively. $T_{\rm BOx}$	
	and $T_{\rm Si}$ refer to the thickness of the BOx region and ultra-thin silicon	
	region, respectively	32
3.11	The logarithm of the electric field intensity and phase profile for a	
	horizontal dipole. Intensity profile for (a) bulk silicon, (b) SOI with	
	$T_{\rm BOx} = 10$ nm, and (c) SOI with $T_{\rm BOx} = 145$ nm. The size of each	
	image is 8 mm by 8 mm. A cross section of (d) intensity profile, (e)	
	phase profile (in radians) as a function of polar angle $(\theta_{obj})$ at azimuthal	
	angle $\phi = \pi/2$	34
3.12	Normalized wide-field detector images for a horizontal dipole for (a)	
	bulk silicon, (b) SOI with $T_{\rm BOx} = 10$ nm, (c) SOI with $T_{\rm BOx} = 145$	
	nm and (d) their line-cuts. The edge length of each image is $\lambda_{\rm ins} \times$	
	Magnification.	35
3.13	Simulated images of a test structure for (a) bulk silicon, (b) SOI with	
	$T_{\rm BOx} = 10$ nm (c) $T_{\rm BOx} = 145$ nm. The size of each image is $6.99 \lambda_{\rm ins} \times$	
	Magnification by $3.55\lambda_{ins} \times$ Magnification.	36
3.14	(a) Collection efficiency and (b) spot size as a function of NA. $\ . \ . \ .$	37
3.15	Schematic of the problem for bulk silicon and SOI chips for objects	
	located in the insulating medium.	38

3.16	Collection efficiency and spot-size as a function of dipole distance from	
	the interface comparing bulk silicon chips and SOI chips with a standard	
	BOx thickness.	39
3.17	Simulated images of an example metal layer. (a) Layout and design	
	parameters. Optical images of the object with the metal line width	
	$\delta=145$ nm, when the depth (b) $d=0,$ (c) $d=175$ nm for bulk silicon,	
	(d) $d=0,$ (e) $d=175$ nm for SOI with standard BOx thickness	39
3.18	Illustration of the pupil mask, its location and parameters	43
3.19	Illustration of Bayesian optimization steps on a 1-D example. Adapted	
	from (Brochu et al., 2010)	46
3.20	(a) PSF of the PEM instrument for the clear aperture case. (b) Cross-	
	sections of the PSF taken along the x and y axes. $\ldots$ . $\ldots$ .	47
3.21	Strehl-ratio vs. spot-size	48
3.22	Examples of masks and their resulting PSFs. Top row and bottom	
	row plot mask designs with higher and lower Strehl-ratios, respectively.	
	(a,d) Cross-sections of the masks as a function of $\theta_{\rm obj},$ (b,e) resulting	
	PSFs, (c,f) cross-sections taken from the PSFs along the $x$ and $y$ axes.	49
3.23	(a) Focused field and (b) its cross-section at the aplanatic point of the	
	aSIL	52
$3 \cdot 24$	Schematic of the aSIL illustrating the parameters for the derivation of	
	the reflected field	54
3.25	Point spread function of the microscope for an Al sphere located at the	
	Si-air interface.	58
3.26	(a) SEM, (b) experimental and (c) simulated image of an Al bar. $\ .$ .	59
3.27	Cross-sections taken from the experimental and simulated image of the	
	Al bar in Figure 3.26	60

- 4.1 Layouts for the M1 layer (black lines) and contacts (gray squares) for(a) AND, (b) OR (c) NAND, (d) NOR, (e) XOR and (f) XNOR gates. 64
- 4.2 Spectral reflectance measurements for the six gates for (a) horizontal (x) polarized (b) vertical (y) polarized illumination at NA = 0.8... 67
- 4·3 Effect of the number of features and the noise level on the classification performance. Classification accuracy (a) as a function of number of features at noise level σ = 0.05 (b) as a function of noise level using 5 features. Selected features are illustrated with dashed black lines for (c) x-polarization (d) y-polarization (legends same as in Fig. 4·2). . . 69
- 4·4 Example tiling of the gates. (a) Layout of the 4x4 tiling, (b) Simulated
  0.8 NA image of the layout, (c) simulated reflectance measurement for
  each of the gate in the tile for y-polarized illumination at λ = 1.22µm.
  Scale bars in (a) and (b) correspond to 1 µm.
- 4.5 Likelihood of the measurement for each class shown for x and y-polarized illumination. Intensity level illustrates the probability distribution. The discontinuities in some of the spectra are artifacts of the periodic boundary conditions caused by diffraction orders.
  72

$4 \cdot 8$	Confusion matrix illustrating the number of gates that are correctly	
	and incorrectly classified	77
$4 \cdot 9$	Example tiling of the gates. (a) layout of the 4x4 tiling, (b) Simulated	
	2 NA image of the layout for x-polarized illumination at $\lambda = 1.22 \mu m$ .	
	Scale bars in (a) and (b) correspond to 1 $\mu$ m.	79
4.10	Box plots for learned dictionary coefficients corresponding to each dictio-	
	nary element for different gate classes in the training set with 54 AND,	
	50 OR, $50$ NAND, $50$ NOR, $14$ XOR and $14$ XNOR gates. The circle	
	with dot represents the median coefficient value, the limits of the blue	
	box represent 25% and 75% percentile values, empty circles represent	
	outliers and the thin whiskers represent minimum and maximum values	
	excluding the outliers.	83
4.11	(a) Dictionary element with index 2, (b,c,d) randomly selected measure-	
	ment images for AND gates, sharing the same colorbar. Each image	
	corresponds to an area of 1400 nm $\times$ 760 nm	84
$4 \cdot 12$	(a) Dictionary element with index 8, (b,c,d) randomly selected measure-	
	ment images for NOR gates, sharing the same colorbar. Each image	
	corresponds to an area of 1400 nm $\times$ 760 nm	84
4.13	(a,b) Dictionary element with indices 20 and 15, (c,d,e) randomly	
	selected measurement images for XOR gates, sharing the same colorbar.	
	Each image corresponds to an area of 1400 nm $\times$ 760 nm. $\ldots$ .	85
4.14	Cross validation accuracies for different number of dictionary elements $p$ .	86
4.15	Box plots for dictionary coefficients corresponding to each dictionary	
	element estimated using OMP, for different gate classes in the test set	
	with 29 AND, 27 OR, 27 NAND, 25 NOR, 8 XOR and 8 XNOR gates.	88

$4 \cdot 16$	Confusion matrix illustrating the number of gates that are correctly	
	and incorrectly classified	89
$5 \cdot 1$	The direction of a ray from the point source in (a) compared o the	
	direction of the rays with an LED in (b). Adapted from (Luo et al.,	
	2010)	92
$5 \cdot 2$	Blur kernel estimation for a single point on the lens	96
5.3	Letter E pattern. (a) Original target pattern, (b) height map of the lens,	
	(c) simulated LED image of the target on the projection surface, (d)	
	deconvolved target pattern, (e) height map of the new lens, (f) simulated	
	LED image of the new target. The contrast of the deconvolved target	
	is enhanced to increase visibility.	102
$5 \cdot 4$	Partitioning into sub-regions for the letter E pattern. Partitioning on	
	the lens overlaid with the log-magnitude and orientation of (a) the	
	major curvature, (b) the minor curvature. (c) Partitions as projected	
	to the projection surface. Colors in (a,b) denote the log-magnitude	
	of the curvatures and arrows indicate the orientation of the curvature	
	axes. The blue grid denotes the boundaries of each partition	103
5.5	Comparison of experimental and simulated data for the letter E pat-	
	tern. (a) Original target pattern simulated with a point source, (b)	
	deconvolved target pattern simulated with an LED, (c) photograph of	
	the pattern created by the fabricated lens illuminated with an LED	104
$5 \cdot 6$	Letter a pattern. (a) Target pattern, (b) height map of the lens, (c)	
	LED image of the target, (d) deconvolved target, (e) convolved image	
	of the new target and the blur operator and (f) LED image of the new	
	target. The contrast of the deconvolved target is enhanced to increase	
	visibility	105

- 5.7 Partitioning into sub-regions for the letter a pattern. Partitioning on the lens overlaid with the log-magnitude and orientation of (a) the major curvature, (b) the minor curvature. (c) Partitions as projected to the projection surface. Colors in (a,b) denote the log-magnitude of the curvatures and arrows indicate the orientation of the curvature axes. The blue grid denote the boundaries of each partition. . . . . 106
- 5.8 Deconvolution results. (a) Deconvolved target, (b) LED image of the original target for comparison, (c) LED image of the deconvolved target.
  The contrast of the deconvolved target is enhanced to increase visibility.107
- 5.10 Letter E, illustrating the overlapping of the tiles when the blur kernels are not calibrated. (a) Target image, (b) height map of the lens, (c)
  LED image of the target, (d) deconvolved target, (e) height map of the new lens, (f) LED image of the new target. The contrast of the deconvolved target is enhanced to increase visibility. . . . . . . . . 109
- 6.1 Spectral response of (a) bare gates, (b) gates labeled with nano-antennas for x-polarized illumination. Near-field intensity distributions of (c) bare AND gate, (d) AND gate with a nanoantenna label (bottom) at  $\lambda = 1.25 \mu m$ . (e) Error rates as a function of noise level with and without the antenna labels. Adapted from (Adato et al., 2015) . . . . 115

### List of Abbreviations

ASR	 Angular Spectrum Representation
BOx	 Buried Oxide
BS	 Beam Splitter
FDTD	 Finite Difference Time Domain
FEM	 Finite Element Method
FWHM	 Full-width-at-half-maximum
GP	 Gaussian Process
GRS	 Gaussian Reference Sphere
IC	 Integrated Circuit
ITRS	 International Technology Roadmap for Semiconductors
LED	 Light-emitting Diode
LVI	 Laser Voltage Imaging
MAP	 Maximum a Posteriori
MOM	 Method of Moments
NA	 Numerical Aperture
NIR	 Near Infra-red
OMP	 Orthogonal Matching Pursuit
PEM	 Photon Emission Microscope
PSD	 Positive Semidefinite
PSF	 Point Spread Function
PSO	 Particle-swarm Optimization
RL	 Richardson-Lucy
SEM	 Scanning Electron Microscope
SIL	 Solid Immersion Lens
SLIC	 Simple Linear Iterative Clustering
SNR	 Signal-to-noise Ratio
SOI	 Silicon on Insulator
SVM	 Support Vector Machine

# Chapter 1 Introduction

The goal of this dissertation is to model optical systems to evaluate their performance in terms of resolution and light collection efficiency and develop model-aware methods to enhance their capabilities. We specifically consider two different application areas in imaging and non-imaging optical systems, where the former is on microscopic imaging of ICs and the latter focuses on illumination systems using free-form lenses. In this chapter, we introduce these application areas and provide an overview of the organization and contributions of this dissertation.

#### 1.1 Integrated circuit imaging

Following Moore's law (Moore, 1998), the semiconductor industry continues to manufacture electronic devices with shrinking dimensions. The decreasing sizes of transistors allows for smaller, cheaper and faster devices with higher functionality and power efficiency. Each year with the decrease of the gate length of transistors, the component density increases as illustrated in Fig. 1.1. By 2030, the International Technology Roadmap for Semiconductors (ITRS) targets a gate length of 7.4 nm (Schwierz, 2010).

The decreased feature sizes increase the demand for high optical resolution systems for fault localization in integrated circuits (ICs). As the opaque metal layers in ICs prohibit front-side imaging, back-side imaging methods are frequently utilized to image buried device layers. Solid immersion lenses (SILs) (Serrels et al., 2008) are the current state-of-the-art technology for non-destructive back-side inspection of ICs,



Figure 1.1: Progression of MOSFET gate length and component density. Adapted from (Schwierz, 2010).

providing high spatial resolution through high numerical aperture (NA  $\geq$  3). In such high NA regimes, investigation of imaging performance of SILs based on detailed electromagnetic modeling is crucial in determining the limitations of the SILs for failure analysis applications of ICs. In this dissertation, we develop an accurate model for SIL microscopy, investigate its performance for different scenarios and use the developed model to increase the resolution through engineering super-resolving masks.

While there is a significant effort to increase the resolution of the SIL microscopy systems through hardware and software improvements such as using radially polarized illumination (Yurt et al., 2014a; Rutkauskas et al., 2015), image reconstruction based post-processing methods (Cilingiroglu et al., 2015) and super-resolving masks, these methods are still are limited in their capability to resolve smallest structures in ICs. With the progressing technology nodes resulting in smaller structures, these methods will not be able meet the resolution requirements of modern circuits. Keeping this in mind, we develop a new method for identifying different digital gate types which operates on lower NA regimes, does not require resolving individual structures in a chip and relies on the model of the system to determine the optimum parameters which will result in high accuracy. Being able to identify different gate types will particularly be useful for the problem of detecting malicious hardware inserted in ICs, called hardware Trojans.

With the increasing complexity of ICs and demand for low-cost chips, IC design and fabrication process is becoming increasingly fragmented and globalized, making the ICs vulnerable to malicious modifications (Mitra et al., 2015). This trend increases security concerns regarding possible threats to military systems, financial infrastructures and transportation security. For instance, Trojans can be designed to leak confidential information or disable or destroy a system at a specified time (Tehranipoor and Koushanfar, 2010). The detection of hardware Trojans are therefore important for many practical and security applications.

#### **1.2** Illumination with free-form lenses

With the rapid advances in high power light-emitting diode (LED) light sources, their use in illumination applications have greatly increased. Such applications, including street, surgical, signage lights and headlights, involve mapping the light from an input LED source to a desired target illumination pattern on a projection surface. For applications such as signage lights which require specific illumination patterns using compact set-ups, free-form optics offers great precision in producing the target pattern with high energy efficiency (Jacobsen and Cassarly, 2016).

Free-form lens design algorithms that map a given source to a desired target pattern typically consider the input light source to be a point source and neglect the size of the LED. These algorithms establish a one to one correspondence between each ray from the point source and their mapped locations on the projection surface. However, in compact and energy efficient systems where the size of the lens is comparable to the effective size of the LED, neglecting the size of the LED causes significant blurring in the target image. This is due to the inability of these algorithms to account for the direction of rays from extended light sources such as LEDs. In this dissertation, we propose a model-based enhancement method to eliminate the blurring caused by extended light sources. Our method models the blur kernel of the lens system due to the extended light source and modifies the target pattern using deconvolution methods to obtain a new target pattern. We demonstrate that the new lens designed for this new target forms a sharper illumination pattern on the projection surface when illuminated with an LED.

#### **1.3** Organization and contributions

We begin Chapter 2 by introducing various systems and problems that we consider in the dissertation. We first describe the resolution of an optical system and review different criteria on the resolution. We then review two types of SILs, namely central SIL (cSIL) and aplanatic SIL (aSIL) and discuss their use on backside imaging of ICs and their high NA capabilities. We also review the related work on modeling of SILs in the context of IC imaging. We next introduce the problem of detecting hardware Trojans, and detail the commonly used methods for detection. We then introduce free-form lenses and describe an algorithm to form a desired image on a projection screen.

Chapter 3 focuses on subsurface imaging of ICs with a SIL microscope. We first derive the Green's function of an aSIL microscope and use it to investigate the imaging performance of aSILs for different metal layers in an IC for a bulk silicon chip technology. We then extend our model to silicon on insulator (SOI) technology and present our results comparing the SOI technology with bulk silicon technology. Next, using the derived Green's function, we propose a Gaussian Process optimization method for engineering pupil masks to increase the resolution of a photon emission microscope (PEM), an optical fault analysis technique for imaging active ICs, beyond the diffraction limit. Our results illustrate the trade-off between the resolution and the collection efficiency of the system. We then derive the full electromagnetic model of the microscope that combines focused light illumination and interaction of the sample with the focused light with the Green's function to model the image of an arbitrary sample.

In Chapter 4, we develop gate classification methods for detecting hardware Trojans. In the first part of this chapter, we develop and present results for a Bayesian classifier that works with low NA spectroscopic measurements of different gate types. We demonstrate that in low NA regimes rapid identification of gates is possible with high accuracy. In the second half of this chapter, we develop a more advanced classification algorithm, based on dictionary learning methods on higher resolution images to increase the classification accuracy. This method complements the former method by trading-off speed for accuracy. We propose a two-stage framework, where the latter algorithm is used in instances where the former algorithm returns low confidence predictions.

In Chapter 5, we consider the problem of illumination with free-form lenses. We propose a shift-variant deconvolution method to enhance the performance of free-form lenses under illumination with an extended light source for scenarios where high energy efficiency is desired. We model the blur kernel of the lens for different regions on the lens and pre-process the target pattern to obtain sharp images. We demonstrate the effectiveness of this method on simulated and experimental data.

Finally, Chapter 6 presents a summary and conclusions of this dissertation and suggests future directions for research.

# Chapter 2 Background and Related Work

In this chapter, we review the problems we consider in this dissertation and provide background information. We start by reviewing different resolution criteria for optical systems, introduce SILs and discuss their use in IC imaging. We next review the related work on hardware Trojan detection. Finally, we discuss different methods for designing free-form lenses for illumination applications.

#### 2.1 Spatial resolution

Spatial resolution of an optical system is a measure of the ability to distinguish two separated point-like objects from a single object, which is often determined by the point spread function (PSF) of the system (Novotny and Hecht, 2012). The PSF is the impulse response of an optical system which defines the spread of a point source.

Widely used resolution criteria utilizing the PSF of a system are the Rayleigh, Sparrow and Houston criteria which are illustrated in Fig. 2.1. The Rayleigh criterion defines the resolution as the distance between the central peak and the first zerocrossing of the PSF (Rayleigh, 1879). In the paraxial limit, the PSF of a system takes the form of an Airy disk with radius  $0.61 \frac{\lambda_0}{NA}$ , where  $\lambda_0$  is the wavelength of the light in free-space, NA =  $n \sin \theta_{\text{max}}$  is the numerical aperture of the system, n is the refractive index of the imaging medium and  $\theta_{\text{max}}$  is the collection angle of the light. This is referred to as the Abbe resolution (Novotny and Hecht, 2012) and gives us the Rayleigh criteria in the paraxial regime.



**Figure 2**.1: (a) Rayleigh, (b) modified Rayleigh, (c) Sparrow and (d) Houston resolution criteria. Obtained from (Köklü, 2010).

The modified Rayleigh criterion is used in the cases where the PSF does not have zero-crossings and defines the resolution as the distance between the peaks of two PSFs when the ratio of their sum at the mid-point to the central peak is equal to 0.81 (Barakat, 1965). The Sparrow criterion defines the resolution to be the minimum distance between the two peaks of the two PSFs when the mid-point becomes visible (Sparrow, 1916). Finally, the Houston criterion defines the resolution as the fullwidth-at-half-maximum (FWHM) of the PSF (Houston, 1927). Throughout this dissertation the resolution of an optical system will be one of the factors determining the performance of the system. We will mostly be using the Houston and Sparrow criteria due to their convenience, especially in the cases where the PSFs do not have zero-crossings.

#### 2.2 Solid immersion lenses for subsurface imaging of integrated circuits

The metallization and opaque metal interconnect layers on the top surface of ICs have necessitated backside imaging methods through the silicon substrate (Serrels et al., 2008). Subsurface imaging through the silicon substrate imposes some limitations on the performance of the system as the band-gap energy of the silicon allows transmission in the near infra-red (NIR) range above  $1.1\mu$ m. Furthermore, as illustrated in Fig.  $2\cdot2(a)$ , due to the boundary conditions at the Si-air interface, the rays originating from the Si medium with angles higher than the critical angle of the Si-air interface will undergo total internal refraction and will not be collected by the objective. In addition, the sub-critical angles that reach the objective will be refracted by the interface and induce spherical aberrations.

#### 2.2.1 Central and aplanatic solid immersion lenses

Due to their ability to overcome the issues with aberrations and total internal reflection stemming from the Si interface, solid immersion lenses (SILs) (Mansfield and Kino, 1990) have been successfully used in imaging ICs. A SIL is a hemisphere placed on the Si substrate of the ICs which transforms the Si substrate into a high refractive index matching medium. It provides high spatial resolution through high numerical aperture (up to  $\approx 3.5$ ) by collecting the light with high angles as illustrated in Fig.  $2\cdot 2$ (b) and (c).

There are two types of SIL designs, called the central SIL (cSIL) and aplanatic SIL (aSIL). In the cSIL, the light is focused to the center of the sphere as shown in Fig.  $2\cdot 2$ (b). The incoming rays at the surface of the sphere arrive at a normal incidence to the surface and do not undergo refraction. The cSIL system has an NA of  $n_{\rm Si} \sin \theta_{\rm obj}^{\rm max}$  and a magnification of  $n_{\rm Si}$ . In the aSIL (Ippolito et al., 2001), the aplanatic point is



**Figure 2.2:** (a) Conventional, (b) cSIL, (c) aSIL subsurface imaging. R denotes the radius of the sphere.

located  $(n_{\rm Si}/n_{\rm air})R$  away from the center of the sphere, where  $n_{\rm Si} \approx 3.5$  and  $n_{\rm air} = 1$ are the refractive indices of Si and air respectively and R denotes the radius of the sphere. In contrast to the cSIL, the incoming rays undergo refraction at the spherical interface of the SIL. The aSIL system has an NA of  $n_{\rm Si}^2 \sin \theta_{\rm obj}^{\rm max}$  and a magnification of  $n_{\rm Si}^2$ . The radius of both SIL designs are determined by the thickness of the Si substrate, as their focal point depends on the radius. A schematic illustrating a typical SIL microscope is presented in Fig. 2·3 for the aSIL geometry. The incident light is reflected by a beam splitter onto the objective, which is focused onto the sample through aSIL. The scattered light from the objects is then collected by the aSIL and focused on the detector.

In IC imaging applications, aSILs are preferred over cSILs due to their ability to achieve higher magnifications. In addition, the cSILs do not allow sufficient working distance for the objective backing the SIL in practical applications, limiting their NA to  $\approx 3$  as opposed to  $\approx 3.4$  in the aSIL. On the other hand, because of the refraction of the rays at the spherical surface, the aplanatic point of the aSIL depends on the wavelength of the light, meaning that in broadband applications it will introduce chromatic aberrations. In contrast, the design and use of the cSILs are universal for



Figure 2.3: Schematic illustrating an aSIL microscope.

any wavelength. The details of the design and application areas of SILs related to imaging photonic and electronic nano-structures are discussed in (Serrels et al., 2008).

#### 2.2.2 Optical model for solid immersion microscopy of integrated circuits

In high NA regimes as provided by SILs, investigation of imaging performance based on detailed electromagnetic model is crucial in determining the limitations of the microscope, as ray tracing models cannot account for certain light behavior such as interference and polarization.

The optical model of high NA imaging systems is usually divided into three main subsystems: (i) focusing of the incident light to the object space, which corresponds to the excitation PSF, (ii) calculation of the scattered light due to the interaction of the focused light with the object of interest and (iii) propagation of the scattered light to the image space, which corresponds to the collection PSF (Török et al., 2008; Novotny and Hecht, 2012).

For modeling the SILs, the vast majority of research is on the focusing of the light while some research on calculating the scattered light and its propagation also exists. In (Vamivakas et al., 2008) a theoretical model for focused light in a cSIL microscope is developed. In (Ippolito et al., 2005), a geometrical model for focused light in an aSIL microscope is derived. (Goh and Sheppard, 2009) presented a vectorial model for the focused field in an aSIL microscope for aSIL with an arbitrary thickness, which models the scenarios when the focal field is not at the aplanatic point. The derivation of the focused light for aSIL for the case when there is a perfect match between the thickness of the substrate and the radius of the SIL is given in (Chen et al., 2012).

Once the model of the focused field is obtained, the calculation of the scattered light does not depend on the geometry of the SIL. To calculate the scattering from an arbitrary structure, rigorous numerical methods such as the Finite Difference Time Domain (FDTD) method (Yee, 1966; Török et al., 2008), Finite Element Method (FEM) (Zienkiewicz, 1977; Chen et al., 2012), or the Method of Moments (MOM) (Abubakar and van den Berg, 2004) can be applied.

In the context of SIL microscopy, the dyadic Green's function that calculates the propagation of the scattered light to the image plane is derived in (Hu et al., 2011). In (Chen et al., 2013) the authors combined these three main subsystems in an efficient algorithm and simulated the images of arbitrary structures for the aSIL microscopy.

So far, the reviewed work in this section considers the object space as a homogeneous medium consisting of only the Si substrate. However, this is not accurate for the ICs as the circuit features such as metal interconnects, resistors and capacitors are surrounded by an insulating medium, typically made of SiO<sub>2</sub> as illustrated in Fig. 2.4. Hence, these models cannot accurately model the ICs as they neglect the reflection and refraction from the Si-SiO<sub>2</sub> interface. In this dissertation we extend the previous work and account for the Si-SiO<sub>2</sub> interface and discuss the effects of this interface.

#### 2.3 Hardware Trojan detection

In this section, we discuss mechanisms for hardware Trojan insertions and review related work on the detection methods. There are two common scenarios for a hardware



**Figure 2.4:** Schematic illustrating the metal layers (M1–M3) of an IC. Obtained from (Wittmann, 2007).

Trojan attack: The first one is by inserting the Trojans through manipulation of the layout at the foundry, resulting in addition, deletion or modification of gates and the second one is by inserting malicious intellectual property (IP) designs to the chips (Rostami et al., 2014). In the latter case the attack can be detected through functional verifications, however in the former case the Trojans are harder to detect as they might not modify the functionality of the chip.

Current Trojan detection techniques can be categorized into side channel analysis and Trojan activation methods (Tehranipoor and Koushanfar, 2010). Side channel analysis methods use timing and power characteristics of the chip to detect Trojans. Power based methods (Rad et al., 2008; Potkonjak et al., 2009) provide information about the activity of the chip, enabling the detection of Trojans without fully activating them. These methods are known to be highly sensitive to noise and and variations in the chip (Nowroz et al., 2014). Timing based methods (Jin and Makris, 2008; Li and Lach, 2008) are based on detecting small changes in the circuit delays through testing along the affected paths. These methods are more robust to noise and variations in the chip, however they are known for their inadequacy to test all possible paths (Nowroz et al., 2014).

Trojan activation methods (Jha and Jha, 2008; Banga and Hsiao, 2008), as their name suggests, rely on being able to activate the Trojan in a chip. These methods are generally combined with power analysis methods to detect Trojans, since the circuit will consume more power with the activation of the Trojan. However, it should be noted that the Trojan circuits are designed to be activated under very specific scenarios, which makes them harder to detect through the activation methods (Tehranipoor and Koushanfar, 2010).

Since the insertion of a Trojan will result in a change in the physical layout of the chip, instead of side channel or activation methods we use the microscopic images of the chips as a direct way to detect hardware Trojans in Chapter 4.

#### 2.4 Free-form lenses for illumination

With the rapid development and broad applications of free-form optics, there is a great effort on designing free-form surfaces for illumination systems. Given a target pattern and light source, such applications aim to design refractive or reflective free-form surfaces that forms the image of the pattern on a projection surface. An example of an illumination system with a refractive lens is illustrated in Fig. 2.5, where the lens forms the image of a letter E pattern on a projection surface.

Most common free-form surface design algorithms can be grouped into supporting ellipsoids (Kochengin and Oliker, 1997; Fournier et al., 2009), brute-force methods (Finckh et al., 2010; Anson et al., 2008), simultaneous multiple surfaces method (Miñano and Gonzalez, 1992; Miñano et al., 2009) and Monge-Ampère approaches



Figure 2.5: Schematic illustrating a free-form lens that forms the image of a target pattern on a projection surface.

(Feng et al., 2013). These methods are reviewed in (Brix et al., 2015). In this section we review a Monge-Ampère equation-based algorithm for designing free-form lenses, developed by Dr. Matthew Brand. While our deconvolution-based framework works with any lens design algorithm, the presented algorithm in this section will be used for designing lenses throughout Chapter 5.

For point sources, given the source input and target output intensity distributions Monge-Ampère methods solve an optimal transportation problem, leading to nonlinear partial differential equations of Monge-Ampère type (Brix et al., 2015). Given the height of the free-form surface p, the transport vector T mapping the light rays from the source to the projection surface can be expressed as T = r(p) where r denotes the refraction from the optical surface, determined by the Snell's law. For a given surface geometry the source energy density  $f_0$  can be propagated in the optical path and similarly assuming that the transport vector is one-to-one, the target energy density  $f_1$  can be propagated backwards. The backpropagated energy density b1 at the optical surface is expressed by

$$b_1 = f_1\left(T^{-1}\right) \cdot \det(\nabla T),\tag{2.1}$$

where  $\nabla$  is the gradient operator. Given the source and target density, the algorithm starts with an initial surface, calculates the backpropagated density and compares it to the source density at the optical surface. The surface heights are then updated according to the mismatch between the two densities using the expression

$$\Delta p \propto (b_1 - f_0) \frac{\mathrm{d}||T||}{\mathrm{d}p}.$$
(2.2)

These steps are repeated for a fixed number of iterations or until convergence. Note that this algorithm extends the optimal transport algorithm in (Chartrand et al., 2009) with the inclusion of the optical surface which imposes refraction on the rays originating from the source.

#### Chapter 3

# Performance of subsurface aplanatic solid immersion microscopy for integrated circuit imaging

In high NA regimes, investigation of imaging performance of solid immersion lenses based on detailed electromagnetic modeling is crucial in determining the limitations of the aSILs for failure analysis applications of ICs. While allowing one to determine the limitations, the model can also be used to determine the changes that can be made in the design of the microscope to increase the performance and it could also be utilized in a model based post-processing techniques to increase the resolution.

In this chapter, we start by deriving the dyadic Green's function of the microscope to model an aSIL microscope. We use the Green's function to investigate the factors that limit the performance of the microscope in imaging ICs. Next we adapt the developed Green's function to the cSIL case and design super-resolving pupil masks to increase the resolution for photon emission microscopy. Finally, we extend the developed model by adding the focused and reflected fields, and formulate the full electromagnetic model of the microscope.

#### 3.1 Green's function derivation for the aSIL microscope

A dipole is the smallest radiation source in electromagnetics and the Green's function expresses the electric field due to a dipole. The electric field  $\vec{E}(\vec{r})$  at the location
$\vec{r} = (x, y, z)$  due to an electric dipole  $\vec{\mu} = (\mu_x, \mu_y, \mu_z)$  located at  $\vec{r}_d = (x_d, y_d, z_d)$  is obtained by the dyadic Green's function  $\overleftrightarrow{G}_0(\vec{r}, \vec{r}_d)$  as

$$\vec{E}(\vec{r}) = \omega^2 \mu_0 \overleftrightarrow{G}_0(\vec{r}, \vec{r}_d) \vec{\mu}$$
(3.1)

where  $\omega$  and  $\mu_0$  are the oscillation frequency of the light and permeability of the free-space, respectively.

A Green's function model for aSIL microscopy has been introduced in (Hu et al., 2011). This model assumes that objects are buried in a homogeneous medium made of Si and does not account for the interface between the insulating medium and the Si substrate of the ICs. Therefore, this model cannot accurately represent the IC geometry and model the interface effects which we discuss in Section 3.2. In this section, we extend the formalism provided in (Hu et al., 2011), and account for the aforementioned interface in our Green's function derivation. Note that we consider the case where there is no thickness mismatch between the substrate and the aSIL, similar to (Hu et al., 2011).



**Figure 3.1:** Schematic of the aSIL system for the Green's function derivation.

In order to derive the Green's function for our set-up as shown in Fig. 3.1, we first start with the derivation in (Novotny and Hecht, 2012), which identifies the Green's function in a homogeneous medium as

$$\overset{\leftrightarrow}{G}_{0}(\vec{r},\vec{r}_{d}) = \frac{i}{8\pi^{2}} \iint_{-\infty}^{\infty} \frac{1}{k_{z,\text{ins}}} \hat{\phi}_{\text{ins}} \hat{\phi}_{\text{ins}}^{\top} + \hat{\theta}_{\text{ins}} \hat{\theta}_{\text{ins}}^{\top} e^{i\vec{k}_{\text{ins}}\cdot(\vec{r}-\vec{r}_{d})} \,\mathrm{d}k_{x,\text{ins}} \,\mathrm{d}k_{y,\text{ins}}$$
(3.2)

where  $\vec{k}_{ins} = (\vec{k}_{x,ins}, \vec{k}_{y,ins}, \vec{k}_{z,ins})$  refers to the wave-vector in the insulating medium,  $(\hat{\cdot})$ denotes the unit vector and  $(\cdot)^{\top}$  denotes the transpose operator. After the refraction from the planar dielectric interface (ins-aSIL), the Green's function can be expressed as

$$\overset{\leftrightarrow}{G}_{aSIL}(\vec{r},\vec{r}_d) = \frac{i}{8\pi^2} \iint_{-\infty}^{\infty} \frac{1}{k_{z,ins}} t^s_{ins} \hat{\phi}_{aSIL} \hat{\phi}^{\top}_{ins} + t^p_{ins} \hat{\theta}_{aSIL} \hat{\theta}^{\top}_{ins} e^{i\vec{k}_{ins} \cdot (\vec{r} - \vec{r}_d)} e^{id\left(k_{z,ins} - k_{z,aSIL}\right)} \, \mathrm{d}k_{x,ins} \, \mathrm{d}k_{y,ins},$$
(3.3)

where d is the distance of the dipole to the aSIL-ins interface and  $t_{ins}^s, t_{ins}^p$  are the Fresnel coefficients for transmission at the interface between the immersion medium and the insulating media for s and p polarizations.

Next step is to propagate the Green's function to the far-field by identifying the spatial Fourier spectrum of the Green's function in Eq. 3.3 and carrying out the algebra as done in (Novotny and Hecht, 2012). In order to propagate the Green's function to the far-field, we make use of the formula

$$\vec{E}_{\infty}(s_x, s_y, s_z) = -i2\pi k_{\text{aSIL}} s_z \hat{\vec{E}}(k_{\text{aSIL}} s_x, k_{\text{aSIL}} s_y; 0) \frac{e^{ik_{\text{aSIL}}r}}{r}, \qquad (3.4)$$

where  $\vec{E}_{\infty}$  is the electric field in the far-field,  $\hat{\vec{E}}$  is the Fourier spectrum at z = 0, r is the distance of the far-field location to the origin and  $(s_x, s_y, s_z)$  is defined as  $\left(\frac{k_{x,aSIL}}{k_{aSIL}}, \frac{k_{y,aSIL}}{k_{aSIL}}, \frac{k_{z,aSIL}}{k_{aSIL}}\right)$ . The reader is referred to (Novotny and Hecht, 2012) for the details of the far-field propagation. In the far-field, inside the aSIL region  $(r \gg \lambda_0$  and  $r \gg |\vec{r_d}|$ , where  $\lambda_0$  is the wavelength of the light in the free-space) the Green's function becomes

$$\overset{\leftrightarrow}{G}_{\mathrm{aSIL}}(\vec{r},\vec{r}_d) = \frac{e^{ik_{\mathrm{aSIL}}r}}{4\pi r} e^{-i\vec{k}_{\mathrm{ins}}\cdot\vec{r}_d} e^{id\left(k_{z,\mathrm{ins}}-k_{z,\mathrm{aSIL}}\right)} \frac{k_{z,\mathrm{aSIL}}}{k_{z,\mathrm{ins}}} \left(t_{\mathrm{ins}}^s \hat{\phi}_{\mathrm{aSIL}} \hat{\phi}_{\mathrm{ins}}^\top + t_{\mathrm{ins}}^p \hat{\theta}_{\mathrm{aSIL}} \hat{\theta}_{\mathrm{ins}}^\top\right).$$

$$(3.5)$$

In the remainder of this section, we follow the steps in (Hu et al., 2011) to obtain the electric field on the Gaussian reference sphere representing the objective (GRS1) and on the detector (GRS2). To obtain the electric field on the Gaussian reference sphere of the objective, we account for the refraction on the spherical surface of the aSIL and express the Green's function as

$$\overset{\leftrightarrow}{G}_{aSIL}(\vec{r},\vec{r}_d) = \frac{e^{ik_{obj}f_{obj}}}{4\pi f_{obj}} e^{-i\vec{k}_{ins}\cdot\vec{r}_d} e^{id\left(k_{z,ins}-k_{z,aSIL}\right)} \frac{k_{z,aSIL}}{k_{z,ins}} \left( t_{ins}^s \hat{\phi}_{obj} \hat{\phi}_{ins}^\top t_{aSIL}^s + t_{ins}^p \hat{\theta}_{obj} \hat{\theta}_{ins}^\top t_{aSIL}^p \right)$$
(3.6)

$$t_{\rm aSIL}^s = \frac{2n_{\rm aSIL}\cos\theta_{\rm obj}}{n_{\rm aSIL}\cos\theta_{\rm obj} + n_{\rm obj}\cos\theta_{\rm aSIL}} \frac{n_{\rm aSIL}}{n_{\rm obj}}$$
(3.7)

$$t_{\rm aSIL}^p = \frac{2n_{\rm aSIL}\cos\theta_{\rm obj}}{n_{\rm aSIL}\cos\theta_{\rm aSIL} + n_{\rm obj}\cos\theta_{\rm obj}} \frac{n_{\rm aSIL}}{n_{\rm obj}},\tag{3.8}$$

where  $k_{\rm obj}$  and  $k_{\rm ins}$  are the wave-numbers of the light in the objective and the insulating media,  $f_{\rm obj}$  is the focal length of the objective,  $k_{z,\rm ins}$  and  $k_{z,\rm aSIL}$  are the longitudinal components of the wave-vectors in the insulating media and the immersion media,  $n_{\rm aSIL}$ and  $n_{\rm obj}$  are the refractive indices of the objective medium and immersion medium, and  $\theta_{\rm aSIL}$  and  $\theta_{\rm obj}$  are the polar angles with respective to the aSIL and the objective coordinate centers.

With the obtained Green's function, we can now express the electric field on the Gaussian reference sphere of the objective using the Eq. 3.1 and plugging in the

expressions for  $\hat{\phi}_{\rm ins}$  and  $\hat{\theta}_{\rm ins}$  as

$$\hat{\phi}_{\rm ins} = \begin{bmatrix} -\sin \phi_{\rm ins} \\ \cos \phi_{\rm ins} \\ 0 \end{bmatrix}, \quad \hat{\theta}_{\rm ins} = \begin{bmatrix} \cos \theta_{\rm ins} \cos \phi_{\rm ins} \\ \cos \theta_{\rm ins} \sin \phi_{\rm ins} \\ -\sin \theta_{\rm ins} \end{bmatrix}, \quad (3.9)$$

where  $\phi_{\text{ins}} = \phi_{\text{aSIL}} = \phi$ ,  $\sin \theta_{\text{ins}} = \sin \theta_{\text{aSIL}} \frac{n_{\text{aSIL}}}{n_{\text{ins}}}$  and  $\cos \theta_{\text{ins}} = \cos \theta_{\text{aSIL}} \frac{n_{\text{aSIL}}}{n_{\text{ins}}} \frac{k_{z,\text{ins}}}{k_{z,\text{aSIL}}}$ . The electric field on the Gaussian reference sphere representing the objective in cylindrical coordinates is then expressed as

$$\vec{E}^{\text{GRS1}}(\theta_{\text{aSIL}}, \phi) = \begin{bmatrix} E_{\theta}^{\text{GRS1}} \\ E_{\phi}^{\text{GRS1}} \end{bmatrix}$$

$$= \omega^{2} \mu_{0} \frac{e^{ik_{\text{obj}}f_{\text{obj}}}}{4\pi f_{\text{obj}}} e^{-i\vec{k}_{\text{ins}}\cdot\vec{r}_{d}} e^{id(k_{\text{zins}}-k_{\text{zaSIL}})}$$

$$\begin{bmatrix} \cos\phi\cos\theta_{\text{aSIL}}\Phi^{(2)}t_{\text{aSIL}}^{p} & \sin\phi\cos\theta_{\text{aSIL}}\Phi^{(2)}t_{\text{aSIL}}^{p} & -\sin\theta_{\text{aSIL}}\Phi^{(1)}t_{\text{aSIL}}^{p} \end{bmatrix} \vec{\mu}$$

$$\begin{bmatrix} \sin\phi\Phi^{(3)}t_{\text{aSIL}}^{s} & \cos\phi\Phi^{(3)}t_{\text{aSIL}}^{s} & 0 \end{bmatrix} \vec{\mu}$$
(3.10)

$$\Phi^{(1)} = \frac{n_{\text{aSIL}}}{n_{\text{ins}}} \frac{k_{\text{zaSIL}}}{k_{\text{zins}}} t^p_{\text{ins}}, \quad \Phi^{(2)} = \frac{n_{\text{aSIL}}}{n_{\text{ins}}} t^p_{\text{ins}}, \quad \Phi^{(3)} = \frac{k_{\text{zaSIL}}}{k_{\text{zins}}} t^s_{\text{ins}}$$

Following the steps in (Hu et al., 2011), the Green's function on the Gaussian reference sphere representing the detector can be expressed as

$$\overset{\leftrightarrow}{G}_{det}(\theta_{det}, \phi_{det}) = \frac{e^{ik_{obj}f_{obj}}}{4\pi f_{obj}} e^{-i\vec{k}_{ins}\cdot\vec{r}_d} e^{id\left(k_{z,ins}-k_{z,aSIL}\right)} \frac{k_{z,aSIL}}{k_{z,ins}} \\
\sqrt{\frac{n_{obj}\cos\theta_{det}}{n_{det}\cos\theta_{obj}}} \left(t_{ins}^s\hat{\phi}_{det}\hat{\phi}_{ins}^{\top}t_{aSIL}^s - t_{ins}^p\hat{\theta}_{det}\hat{\theta}_{ins}^{\top}t_{aSIL}^p\right).$$
(3.11)

Inside the detector region at an arbitrary point  $\vec{r}_{det}$ , the Green's function can be obtained using the formula

$$\overset{\leftrightarrow}{G}_{det}(\vec{r}_{det},\vec{r}_{d}) = -\frac{ik_{det}f_{det}e^{ik_{det}f_{det}}}{2\pi} \iint\limits_{\theta_{det}^{max}} \overset{\leftrightarrow}{G}_{det}(\theta_{det},\phi_{det})e^{i\vec{k}_{det}\cdot\vec{r}_{det}}\sin\theta_{det}\,\mathrm{d}\theta_{det}\,\mathrm{d}\phi_{det}.$$

$$(3.12)$$

Plugging in the relevant expressions for  $\hat{\phi}$  and  $\hat{\theta}$ 's into Eq. 3.11 with the equality

 $\phi_{\text{det}} = pi + \phi_{\text{aSIL}} = \pi + \phi$  and taking the integral in Eq. 3.12 results in the final Green's function in Eq. 3.13 for a point on the detector

$$\overset{\leftrightarrow}{G}_{\rm det}(\vec{r}_{\rm det},\vec{r}_{d}) = -\frac{ik_{det}f_{obj}}{8\pi f_{\rm det}} \sqrt{\frac{n_{\rm obj}}{n_{\rm det}}} e^{i(k_{\rm det}f_{\rm det}+k_{\rm obj}f_{\rm obj})} \begin{bmatrix} I_0 + I_{21} & I_{22} & -2iI_{11} \\ I_{22} & I_0 - I_{21} & -2iI_{12} \\ 0 & 0 & 0 \end{bmatrix},$$
(3.13)

where

$$\begin{split} I_{0} &= \int_{0}^{\theta_{\text{obj}}^{\text{max}}} \sin \theta_{\text{obj}} \sqrt{\cos \theta_{\text{obj}}} \left( t_{\text{aSIL}}^{s} \Phi^{(3)} + t_{\text{aSIL}}^{p} \Phi^{(2)} \cos \theta_{\text{aSIL}} \right) J_{0}(\rho) e^{-iz} \, \mathrm{d}\theta_{\text{obj}}, \\ I_{11} &= \int_{0}^{\theta_{\text{obj}}^{\text{max}}} \sin \theta_{\text{obj}} \sqrt{\cos \theta_{\text{obj}}} \left( t_{\text{aSIL}}^{p} \Phi^{(1)} \sin \theta_{\text{aSIL}} \right) J_{1}(\rho) e^{-iz} \cos \varphi \, \mathrm{d}\theta_{\text{obj}}, \\ I_{12} &= \int_{0}^{\theta_{\text{obj}}^{\text{max}}} \sin \theta_{\text{obj}} \sqrt{\cos \theta_{\text{obj}}} \left( t_{\text{aSIL}}^{s} \Phi^{(1)} \sin \theta_{\text{aSIL}} \right) J_{1}(\rho) e^{-iz} \sin \varphi \, \mathrm{d}\theta_{\text{obj}}, \\ I_{21} &= \int_{0}^{\theta_{\text{obj}}^{\text{max}}} \sin \theta_{\text{obj}} \sqrt{\cos \theta_{\text{obj}}} \left( t_{\text{aSIL}}^{s} \Phi^{(3)} - t_{\text{aSIL}}^{p} \Phi^{(2)} \cos \theta_{\text{aSIL}} \right) J_{2}(\rho) e^{-iz} \cos 2\varphi \, \mathrm{d}\theta_{\text{obj}}, \\ I_{22} &= \int_{0}^{\theta_{\text{obj}}^{\text{max}}} \sin \theta_{\text{obj}} \sqrt{\cos \theta_{\text{obj}}} \left( t_{\text{aSIL}}^{s} \Phi^{(3)} - t_{\text{aSIL}}^{p} \Phi^{(2)} \cos \theta_{\text{aSIL}} \right) J_{2}(\rho) e^{-iz} \sin 2\varphi \, \mathrm{d}\theta_{\text{obj}}, \\ \rho &= \sqrt{x^{2} + y^{2}}, \quad \varphi = \tan^{-1}(y/x), \\ x &= -\left(k_{\text{det}} \sin \theta_{\text{det}} x_{\text{det}} + k_{\text{aSIL}} \sin \theta_{\text{aSIL}} x_{d} \right), \\ y &= -\left(k_{\text{det}} \sin \theta_{\text{det}} y_{\text{det}} + k_{\text{aSIL}} \sin \theta_{\text{aSIL}} y_{d} \right), \\ z &= d(k_{z,\text{ins}} - k_{z,\text{aSIL}}) - \left(k_{\text{det}} \cos \theta_{\text{det}} z_{\text{det}} + k_{\text{ins}} \sqrt{1 - \left(\frac{k_{\text{aSIL}}}{k_{\text{ins}}}\right)^{2} \sin^{2} \theta_{\text{aSIL}} z_{d}} \right). \end{split}$$

In the above equations,  $k_{det}$  is the wave number in the detector space,  $f_{det}$  is the focal length of the tube lens  $(f_{det} \gg f_{obj})$ ,  $n_{det}$  is the refractive index of the detector medium,  $\vec{r}_{det} = (x_{det}, y_{det}, z_{det})$  is the location on the detector plane.  $J(\rho)$  refers to

the Bessel functions of a given order. The relationship between the polar angles is given by

$$n_{\rm obj} \sin \theta_{\rm aSIL} = n_{\rm aSIL} \sin \theta_{\rm obj}$$
  
 $f_{\rm det} \sin \theta_{\rm det} = f_{\rm obj} \sin \theta_{\rm obj}$   
 $n_{\rm ins} \sin \theta_{\rm ins} = n_{\rm aSIL} \sin \theta_{\rm aSIL}.$ 

In the next section, we will use the derived Green's function to investigate the performance of an aSIL microscope in terms of its spatial resolution and light collection efficiency for two different IC technologies, bulk silicon and silicon on insulator (SOI) chips. We will start with analyzing the performance of the aSIL microscope for different metal layers in a bulk silicon chip and continue our analysis with the SOI chips with different buried oxide (BOx) thicknesses. We finally combine the two scenarios and investigate the performance for different metal layers in SOI chips.

## **3.2** Performance in bulk silicon chips

In this section, we investigate the performance of the aSIL microscopy for different metal layers in a bulk silicon chip. The ability to image metal layers is important for fault detection since they are crucial for electrical performance. The geometry for the bulk silicon chips consists of the Si substrate and the insulating medium as illustrated in Fig. 3.1, where the metal layers are buried in the insulating medium (denoted by ins), typically made of SiO<sub>2</sub> with  $n_{\rm ins} \approx 1.53$ .

Since the metal layers are located in the insulating medium with a lower refractive index than the immersion medium ( $n_{aSIL} = n_{Si} = 3.5$  and  $n_{ins} \ll n_{Si}$ ), the boundary conditions at the ins-aSIL interface impose that the evanescent waves that originate from the objects transform into propagating waves in the immersion medium at angles higher than the critical angle of the two media ( $\theta_c$ ). Due to the high NA capability of the aSIL microscope, these propagating waves, so-called *forbidden light*, can be collected by the microscope and contribute to the far-field image (Novotny and Hecht, 2012; Yurt et al., 2014b; Karrai et al., 2000). However, due to their evanescent wave origin, the waves with angles larger than the critical angle will have exponentially decaying amplitude in the insulating medium as a function of the distance between the object the interface, until they are transformed into propagating waves at the interface. Therefore, as the objects are located further away from the interface, the performance of the microscope will deteriorate due to the loss of the amplitude of the waves at high angles. This effect is illustrated in Fig. 3.2, where on the left image we are able to collect the forbidden light (red area) since the object is in the proximity of the interface. On the right image, the forbidden light is lost since the amplitude of the evanescent waves decays exponentially until they reach the interface.



Figure 3.2: Detection of evanescent waves. Red and green areas correspond to forbidden light and allowed light regions respectively.

In the following, we will study the characteristics of the forbidden light by first analyzing the field amplitude and phase profile on the objective pupil and analyzing the field profile on the detector for objects buried at different depths in the insulating medium. Unless otherwise stated, we will use the following parameters in the derived Green's function for our analysis:  $n_{aSIL} = n_{Si} = 3.5$ ,  $n_{ins} = n_{SiO_2} = 1.53$ ,  $n_{obj} = n_{det} =$ 1,  $f_{obj} = 10$  mm, free space wavelength  $\lambda_0 = 1340$  nm, NA = 3.4 in aSIL, which corresponds to an objective NA of 0.278. The objects are assumed to be located on the aplanatic point of the SIL ( $z_d = 0$ ) regardless of their distance to the ins-aSIL interface.

In order to investigate the effect of forbidden light on the imaging performance, we start by plotting the electric field intensity and phase profiles on the pupil plane of the objective for horizontal ( $\vec{\mu} = \mu_x \hat{x}$ ) and vertical ( $\vec{\mu} = \mu_z \hat{z}$ ) dipoles using Eq. 3.10. Figure 3.3 illustrates the logarithm of the electric field intensity map for both horizontal and vertical dipoles located d = 0,  $d = \lambda_{\text{ins}}/2 = 437$  nm and  $d = \lambda_{\text{ins}} = 875$ nm away from the dielectric interface (ins-aSIL). The black circle inside the intensity images is inserted to denote the circle corresponding to the critical angle of the total internal reflection corresponding to  $\theta_{\text{obj}} = 6.8^{\circ}$ .

We observe that for both dipoles, the intensity starts dropping rapidly in the forbidden light region (outside the black ring) as the dipole is moved further away from the interface, while the intensity profile stays the same in the allowed light region (inside the black ring) regardless of the distance of the dipole to the interface. This is due to the fact that the intensity of the evanescent waves originating from the dipole with imaginary  $k_z$  values at angles higher than the critical angle of the two media ( $\theta_{aSIL} > \sin^{-1}\left(\frac{n_{SiO_2}}{n_{Si}}\right)$ ) drops exponentially as they travel inside the insulating medium. This means that the intensity of the high NA components (with high angles) will be lost the as the object is moved further away from the interface.

In addition to its effect on the intensity profile, the evanescent wave origin of the forbidden light also causes wave-front aberrations. In order to illustrate that, we first define the phase of a pencil of light at a given polar angle at the pupil as:  $\vec{\Psi}_{\text{pupil}}(\theta) = \tan^{-1}\left(\frac{\text{Im}(\vec{E}^{\text{GRS1}})}{\text{Re}(\vec{E}^{\text{GRS1}})}\right)$ . Since we are interested in only the aberration originated from the forbidden light we subtract the spherical aberration term caused by the dielectric interface  $(\vec{\Psi}_{\text{sph}} = e^{id(k_{z,\text{ins}}-k_{z,\text{aSIL}})})$  from the total phase (Török, 2000) and define  $\vec{\Psi}_{\text{FL}} = \vec{\Psi}_{\text{pupil}} - \vec{\Psi}_{\text{sph}}$ .

Figure 3.4 plots the wave-front aberrations due to the forbidden light as a function of



Figure 3.3: The logarithm of the electric field intensity distribution for horizontal (left column) and vertical dipoles (middle column) for (a) d = 0, (b)  $d = \lambda_{ins}/2$ , (c)  $d = \lambda_{ins}$ . The size of each image is 8 mm by 8 mm. A cross-section of the intensity profile as a function of  $\theta_{obj}$  at  $\phi = 0$  for (d) horizontal, (e) vertical dipole.

the polar angle  $(\theta_{obj})$  and dipole height from the dielectric interface (d) at supercritical angles. In an aberration free system we would expect to have a constant phase profile at the pupil. However, even if we neglect the spherical aberrations, due to the forbidden light we observe a  $\lambda_{ins}/5$  peak-to-valley phase distortion at high angles which will degrade the performance of the system. This is due to the fact that at angles above the critical angles the Fresnel transmission coefficients obtain complex values, which is similar to the Goose-Hänchen shift effect (Goos and Hänchen, 1947).

So far we investigated the effect of forbidden light through analyzing the intensity



**Figure 3.4:** Wave-front aberrations due to forbidden light (in radians) in (a)  $E_{\theta}^{\text{GRS1}}$ , (b)  $E_{\phi}^{\text{GRS1}}$  for horizontal dipole and (c)  $E_{\theta}^{\text{GRS1}}$  for vertical dipole.

and phase profiles on the objective pupil. In the following, we will investigate the effect of forbidden light through analyzing the intensity profiles on a wide-field detector on the image plane and evaluate the performance of the aSIL microscope in terms of its spatial resolution and collection efficiency under various conditions.

We start our analysis by simulating the intensity images on the image plane due to horizontal and vertical dipoles at different depths, which also corresponds to the collection point spread function (PSF) of the aSIL microscope. In order to understand how forbidden light affects the performance, we decompose the PSF into two components, where we observe (1) the allowed light component of the intensity when we collect only the subcritical angles and (2) the forbidden light component of the intensity when we collect only the supercritical angles.

Figure 3.5 illustrates the aforementioned intensity images on a wide-field detector for a horizontal dipole when the dipole is located on the dielectric interface (d = 0)and located  $\lambda_{\text{ins}}$  away from the interface  $(d = \lambda_{\text{ins}} = 875 \text{ nm})$ . When d = 0, we observe that the intensity of the forbidden light component is approximately an order of magnitude larger than the allowed light component. Since we are able to collect the forbidden light component, the overall response is dominated by the supercritical angles, resulting in a spot-size of approximately  $\lambda_{ins}/4 \approx 220$  nm). This is in line with the experimental observations where structures with a pitch value of 252 nm are shown to be resolved with linearly polarized light in (Yurt, 2014). However, when the dipole is located  $\lambda_{ins}$  away from the interface, we observe that the intensity of the allowed light component is approximately two orders of magnitude larger than the forbidden light component which dominates the overall response. Due to the loss of the supercritical angles, we observe a two orders of magnitude drop in the overall intensity compared to the case when the dipole is located on the interface with a spot-size of  $\lambda_{ins}/1.4 \approx 614$  nm). We repeat the same experiments for a vertical dipole in Fig. 3-6 and observe that the characteristics of the intensity distribution is similar to the horizontal dipole case, where the overall response is dominated by the supercritical angles when the dipole is located at the interface, resulting in a tight spot and the contribution from the forbidden light is lost when the dipole is located  $\lambda_{ins}$  away from the interface, resulting in a loss in the overall intensity and a larger spot-size.

In order to evaluate the performance of the aSIL microscope, we next study the spot-size and relative collection efficiency as a function of the dipole distance from the dielectric interface. We define the collection efficiency as the integrated intensity on the detector and define the spot-size as the full-width-at-half-maximum (FWHM) of the peak for the horizontal dipole and FWHM of the dip for the vertical dipole.

In Fig. 3.7 we observe that when the dipole is located at the interface, the ability to collect supercritical angles results in a tighter spot with a spot size of approximately  $0.25\lambda_{ins}$  ( $\approx 220$  nm) for the horizontal dipole and approximately  $0.2\lambda_{ins}$  ( $\approx 185$  nm) for the vertical dipole. However, for the objects located further from the interface, the ability to collect high angles is lost and the we observe an increase in the spot-size. As illustrated by the collection efficiency curves, for subcritical angles (allowed light



Figure 3.5: Normalized wide-field detector images of a horizontal dipole when d = 0 (top row) and  $d = \lambda_{ins}$  (bottom row). Intensity images when the (a,d) full angles, (b,e) only subcritical angles, (c,f) supercritical angles are collected. The size of each image is  $3\lambda_{ins} \times$  Magnification by  $3\lambda_{ins} \times$  Magnification. The intensity values are normalized to the maximum intensity in (a).

component denoted as AL) the collection efficiency is constant regardless of the dipole height, whereas for the supercritical angles (forbidden light component denoted as FL) the efficiency drops more than two orders of magnitude for both horizontal and vertical dipoles as the dipole distance from the interface increases.

Next, we simulate incoherent images of two-dimensional objects similar to the metal wires buried in the insulating medium. We assume a linearly polarized uniform incoherent illumination and use the Green's function for a horizontal dipole to simulate the wide-field images. In Fig. 3.8, we simulated the response of the microscope for a test structure with the objects located at different depths of d = 0,  $d = \lambda_{\text{ins}}/2$  (437 nm),  $d = \lambda_{\text{ins}}$  (875 nm). The line pitch of the each structure ranges from  $0.2\lambda_{\text{ins}}$  (175 nm) (structures labeled as I in the figure) to  $0.8\lambda_{\text{ins}}$  (700 nm) (structures labeled as VII in the figure) with an increment of  $0.1\lambda_{\text{ins}}$  (87.5 nm) between each group. For the



Figure 3.6: Normalized wide-field detector images of a vertical dipole when d = 0 (top row) and  $d = \lambda_{ins}$  (bottom row). Intensity images when the (a,d) full angles, (b,e) only subcritical angles, (c,f) supercritical angles are collected. The size of each image is  $3\lambda_{ins} \times$  Magnification by  $3\lambda_{ins} \times$  Magnification. The intensity values are normalized to the maximum intensity in (a).

objects located at the interface (d = 0), we observe that the smallest objects we can resolve are the second group with a line pitch of 262 nm according to the Sparrow criterion. When  $d = \lambda_{ins}/2$  the smallest objects we can resolve are the fourth group with a line pitch of 437.5 nm and when  $d = \lambda_{ins}$  the smallest objects we can resolve are the sixth group with a line pitch of 612.5 nm. We also note that between d = 0 case and  $d = \lambda_{ins}/2$  there is approximately one order of magnitude drop in the maximum intensity, whereas the drop is more than an order of magnitude in the  $d = \lambda_{ins}$  case, reflecting the exponential decay property of the evanescent waves.

In Fig. 3.9 we simulate two-level metal wires located at different depths as in different metal layers in ICs. The wires have a line pitch of  $\lambda_{\text{ins}}$  and are located at  $d = \lambda_{\text{ins}}/2$  (red wires) and  $d = \lambda_{\text{ins}}$  (blue wires). We note that the wires L1 and L2 are



Figure 3.7: Collection efficiency and spot-size (in x and y axes) as a function of the dipole distance from the dielectric interface for horizontal (left) and vertical (right) dipole. Note that the intensity distribution for the vertical dipole is circularly symmetric, resulting in the same spot-size in x and y axes.



**Figure 3.8:** Simulated images of a test structure when (a) d = 0, (b)  $d = \lambda_{\text{ins}}/2$ , (c)  $d = \lambda_{\text{ins}}$ . The size of each image is  $8.3\lambda_{\text{ins}} \times \text{Magnification}$  by  $17.7\lambda_{\text{ins}} \times \text{Magnification}$ . The intensity of each panel are normalized to the maximum intensity in (a).

resolved according to the Sparrow criterion where the contrast reaches approximately 0.45, while the contrast for L3 and L4 reaches approximately 0.02.



Figure 3.9: (a) Layout and (b) simulated image of a test structure with wires at different depths. L1 and L2 are located at  $d = \lambda_{\rm ins}/2$ , where L2 and L3 are located at  $d = \lambda_{\rm ins}$ . The scalebar in(a) corresponds to a length of  $\lambda_{\rm ins}$ . The size of each image is  $10.11\lambda_{\rm ins} \times {\rm Magnification}$ by  $7.28\lambda_{\rm ins} \times {\rm Magnification}$ . (c) Cross-section of the image taken along the dotted line in (b).

## **3.3** Performance in silicon on insulator chips

In the previous subsection, we studied the performance of an aSIL microscope on bulk silicon chips. An alternative to the bulk silicon chip technology is the fully depleted (FD) silicon on insulator (SOI) chip technology which relies on an ultra-thin layer of silicon over a buried oxide (BOx) layer into which the transistors built. This technology is claimed to be more advantageous compared to the bulk silicon chip technology in terms of their electrical characteristics (Cauchy and Andrieu, 2010). Two commonly used types of SOI chips have (1) a standard BOx thickness of 145 nm or (2) an ultra-thin BOx thickness of 10 nm or 25 nm. A schematic of the SOI technology compared to the bulk silicon technology is illustrated in Fig. 3.10.

It has been experimentally observed that the resolution of the aSIL microscope reduces dramatically for SOI technology with standard BOx thickness (Yurt, 2014). In this subsection we will study the performance of the aSIL microscope for the SOI chips and explain how forbidden light affects the spatial resolution and collection



Figure 3.10: Schematic of the problem for objects located in the substrate and ultra-thin silicon layer for bulk silicon and SOI technology respectively.  $T_{\rm BOx}$  and  $T_{\rm Si}$  refer to the thickness of the BOx region and ultra-thin silicon region, respectively.

efficiency in SOI chips. We will first study the performance for the objects buried in the ultra-thin silicon region (e.g. transistors) and compare the results for bulk silicon chips, SOI chips with an ultra-thin BOx of 10 nm and SOI chips with a standard BOx thickness of 145 nm. Next, we will study the performance for the objects buried in the insulating medium (e.g. metal layers), and provide a comparison for bulk silicon chips and SOI chips.

In Section 3.1 we derived the Green's function of the microscope for a dipolar object located in the vicinity of the aplanatic point of the aSIL for bulk silicon chips. In order to conduct our analysis for the SOI geometry, we generalize the provided Green's function by replacing the transmission coefficients  $(t_{ins}^s, t_{ins}^p)$  with the generalized Fresnel coefficients (Chew, 1995) in order to accommodate for the multi-layer structure of SOI chips.

In the following, the objects are assumed to be located at the aplanatic point

32

of the aSIL and the following parameters are used: refractive indices  $n_{\rm aSIL} = n_{\rm Si} = 3.5$ ,  $n_{\rm ins} = n_{\rm BOx} = 1.53$ , the free space wavelength  $\lambda_0 = 1340$  nm, focal length of the objective  $f_0 = 10$  mm, thickness of the ultra-thin silicon layer  $T_{\rm Si} = 10$  nm, and NA = 3.4 (unless otherwise stated).

In the first stage of our analysis the objects of interest, such as transistors, are buried in the ultra-thin silicon layer sandwiched between two insulating media as shown in Fig. 3.10. We first examine the field amplitude and phase profile of a horizontal dipole on the pupil plane of the objective for bulk silicon chips, SOI chips with an ultra-thin BOx and SOI chips with a standard BOx thickness. In Fig. 3.11 the region corresponding to the critical angle of the Si-BOx interface is denoted by a black ring in the intensity images. We note that for the SOI chips with a standard BOx thickness the intensity profile above the critical angle (outside the black ring) starts dropping dramatically compared to the bulk silicon chips and SOI chips with an ultra-thin BOx. This is similar to what we observed in the previous subsection and can be attributed to the collection of the forbidden light. In this case, the waves originating from the dipole at the angles higher than the critical angle transform into evanescent waves in the BOx medium and are transformed back into propagating waves in the SIL medium, but at a fraction of the original intensity (Uyar et al., 2014b). As the waves travel a longer distance in the BOx region in SOI with standard BOx thickness compared to SOI with ultra-thin BOx, we observe a more rapid drop in the intensity due to the exponential decay property of the evanescent waves, resulting in a loss of light with high NA.

We note that in Fig. 3.11(d) the slight increase in the intensity close to the critical angle for  $T_{\rm BOx} = 145$  nm case is caused by the spherical aberration due to a thicker BOx. In addition to spherical aberration caused by the BOx layer, the evanescent wave nature of the forbidden light also contributes to the distortions in the phase

front. In Fig. 3.11(e) we plot the phase profile for the  $E_{\theta}$  component for the three cases and observe wave-front aberrations caused by both spherical aberration and the aberration due to the forbidden light. For  $T_{\text{BOx}} = 10$  nm, the phase profile is close to the bulk silicon case, however for  $T_{\text{BOx}} = 145$  nm the phase profile is more distorted due to the forbidden light as well as the spherical aberration.



Figure 3.11: The logarithm of the electric field intensity and phase profile for a horizontal dipole. Intensity profile for (a) bulk silicon, (b) SOI with  $T_{\text{BOx}} = 10$  nm, and (c) SOI with  $T_{\text{BOx}} = 145$  nm. The size of each image is 8 mm by 8 mm. A cross section of (d) intensity profile, (e) phase profile (in radians) as a function of polar angle ( $\theta_{\text{obj}}$ ) at azimuthal angle  $\phi = \pi/2$ .

In Fig. 3.12 we study the optical images of a horizontal dipole on a wide-field detector. We observe that the detector image for SOI with  $T_{\text{BOx}} = 10$  nm has a similar intensity profile to the bulk silicon case except for a 15% decrease in the peak intensity. However for SOI with  $T_{\text{BOx}} = 145$  nm there is a 30% increase in the spot size (determined by the FWHM) and 80% decrease in the intensity, caused by the



decrease in the intensity at super-critical angles as illustrated in Fig. 3.11.

Figure 3.12: Normalized wide-field detector images for a horizontal dipole for (a) bulk silicon, (b) SOI with  $T_{\text{BOx}} = 10 \text{ nm}$ , (c) SOI with  $T_{\text{BOx}} = 145 \text{ nm}$  and (d) their line-cuts. The edge length of each image is  $\lambda_{\text{ins}} \times$  Magnification.

In order to assess the imaging performance in terms of the spatial resolution we simulated the incoherent wide field images of two-dimensional objects as shown in Fig. 3.13. The line pitch of the test structures range from 200 nm to 320 nm with 30 nm increments. We observed that only the first set of structures are not resolved in bulk silicon and SOI with  $T_{\rm BOx} = 10$  nm according to the Sparrow criterion. For SOI with  $T_{\rm BOx} = 145$  nm only the last two set of structures are resolved clearly, while the third set of structures have 5% peak-to-dip contrast and we are not guaranteed to resolve them under the presence of noise. Compared to bulk silicon, the resolution for SOI with ultra-thin BOx is not affected, however there is a 15% decrease in the maximum intensity. Moreover, for SOI with standard thickness there is a 30% decrease in the resolution and approximately 75% decrease in the maximum intensity.

So far we investigated the imaging performance of aSIL microscopy for SOI chips at a high NA since the effect of forbidden light is observed at high angles as illustrated in Fig. 3.11. However, the imaging performance is not heavily affected in low NA regimes. We demonstrate this in Fig. 3.14, where we plot the spot-size and the collection efficiency as a function of NA. The intensity image of the dipole is integrated on the



**Figure 3.13:** Simulated images of a test structure for (a) bulk silicon, (b) SOI with  $T_{\text{BOx}} = 10 \text{ nm}$  (c)  $T_{\text{BOx}} = 145 \text{ nm}$ . The size of each image is  $6.99\lambda_{\text{ins}} \times \text{Magnification}$  by  $3.55\lambda_{\text{ins}} \times \text{Magnification}$ .

detector to calculate the collection efficiency. We note that up to 1.55 NA, the imaging performance is not noticeably affected by the BOx thickness. In our case the critical angle of the Si – SiO<sub>2</sub> medium corresponds to approximately 1.55 NA. We observe that the performance of the microscope starts changing at 1.55 NA, which coincides with our expectations due to forbidden light.

We observed that the thickness of the BOx layer in the SOI technology reduces the performance of the microscope for the objects located inside the ultra-thin silicon layer (e.g. transistors) due to the exponential decay property of the evanescent waves inside the BOx layer. Combining this with our observations in Section 3.2, we would expect that the performance will further deteriorate for the structures located inside the insulating medium (e.g. metal layers) (Uyar et al., 2014a). In the remainder of this section, we consider objects located in the insulating medium and briefly analyze the performance of the microscope for the SOI technology with a standard BOx thickness and compare it to the bulk silicon technology. The schematic of the set-up is illustrated in Fig. 3.15.

In Fig. 3.16, we consider a horizontal dipole buried inside the insulating medium



**Figure 3.14:** (a) Collection efficiency and (b) spot size as a function of NA.

and plot the spot-size and collection efficiency as a function of the dipole distance d from the ins-aSIL or ins-Si interface, to investigate the performance for various metal layers for bulk silicon and SOI chips. We note that when the object is at the interface (d = 0), the collection efficiency of SOI is less than 60% of the collection efficiency of the bulk silicon. As the depth of the dipole increases, collection efficiency decreases by approximately 80% in bulk silicon and 30% in SOI within 200 nm. After 200 nm, the forbidden light is mostly lost and the collection efficiency converges to the allowed light level with a slightly higher value for SOI chips due to aberrations. The first metal layer typically lays within 200 nm in 32 nm process nodes and its successors. The performance significantly decreases for metal layers at higher depths as there is more than a three-fold increase in the spot-size for both bulk silicon and SOI within 800 nm. In 200 nm the spot-size increases by approximately 50%, which significantly decreases the resolution.

To evaluate the imaging performance at the detector, we simulate the incoherent wide-field images of metal structures in Fig. 3.17. While the metals at the interface in



**Figure 3.15:** Schematic of the problem for bulk silicon and SOI chips for objects located in the insulating medium.

bulk silicon are clearly resolved according to the Sparrow criterion, there is a significant decrease in the contrast when d = 175 nm in bulk silicon technology. Similarly, in SOI, when the metals are at the interface there is a decrease in the contrast compared to bulk silicon and the metal layer at d = 175 nm is not resolved.

So far we investigated the performance of an aSIL microscope and analyzed its limitations in terms of resolution and collection efficiency under different scenarios. In the next section we will focus on increasing the resolution of the microscope by utilizing the developed model.

# 3.4 Super-resolution through pupil mask engineering

Pupil function engineering aims at modifying the PSF of the optical system through placing masks at the pupil plane of the objective to obtain a smaller spot-size. The idea of using an annular pupil was known to Lord Rayleigh who noted that it is possible to obtain a sharper focus using an annular aperture at the expense of increased side-lobe strength and decreased central intensity (Lindberg, 2012). Later on Toraldo



**Figure 3-16:** Collection efficiency and spot-size as a function of dipole distance from the interface comparing bulk silicon chips and SOI chips with a standard BOx thickness.



Figure 3.17: Simulated images of an example metal layer. (a) Layout and design parameters. Optical images of the object with the metal line width  $\delta = 145$  nm, when the depth (b) d = 0, (c) d = 175 nm for bulk silicon, (d) d = 0, (e) d = 175 nm for SOI with standard BOx thickness.

di Francia's research on pupil filters in the context of optical microscopy (Di Francia, 1952) has laid the groundwork for proceeding research in this area. Following di Francia's work, a common pupil mask engineering method is to represent the pupil function in some complete set of functions and adjust the coefficients of these functions to approximate a pre-specified PSF. These methods are reviewed in (Lindberg, 2012). An example of such methods is to specify the zeros of the PSF to obtain a desired spot-size while pushing the side-lobes of the PSF further away from the optical axis (Boyer and Sechaud, 1973; Yurt, 2014). However, these methods cannot explicitly control the intensity of the side-lobes which might compromise the usefulness of the

resolution enhancement. In addition, the aforementioned methods aim to obtain pupil masks that result in PSFs with given specifications rather than trying to obtain an optimal PSF, e.g., the PSF with the highest resolution for a given central intensity or side-lobe ratio. The latter approach is considered in the work we discuss next.

An alternative line of work for pupil mask engineering relies on black-box optimization methods. Black-box optimization refers to optimization of an objective function through a black-box interface, where the algorithm may query the value of the objective function g(x) for a given x, but it does not obtain gradient information and cannot make any assumptions on the analytic form of g. Recently, a black-box optimization method, namely particle-swarm optimization (PSO) has been used in engineering such pupil masks (Banaee et al., 2014; Jabbour and Kuebler, 2008). The major drawback of the PSO method is the high number of computationally expensive function evaluations until a satisfactory solution is found. One way to speed up this process is using statistical model-assisted black-box optimization methods, where a model of the target function is created from former evaluations and exploited to sample new candidate solutions (Kronfeld and Zell, 2010). Gaussian Process (GP) optimization is an example of such methods, which we propose to use for pupil mask engineering in the context of integrated circuit imaging.

In this section, we focus on improving the resolution of the photon emission microscopy (PEM), which is one of the common techniques used for fault analysis of ICs. This technique is based on the emission of photons due to electrical stimulation, where the transition of electrons from higher to lower energy states results in all or part of the energy difference being emitted as electromagnetic radiation (Phang et al., 2005). While ICs operating in normal conditions also emit photons, faulty locations generally emit a significantly higher number of photons, which is useful for fault detection (Leng, 2009). We note that due to the broadband emission of photons in PEM, using an aSIL would induce chromatic aberrations on the measurements and would need to be corrected, which could be achieved by designing a new objective (Yurt, 2014). Using a cSIL instead is also viable as it does not induce chromatic aberrations and results in a simpler set-up. For this reason, we consider the cSIL configuration to engineer super-resolution masks in this section.

Since the light scattering in PEM is based on the electrical activity of the chip, the object of interest is not illuminated with focused light. Therefore, the Green's function of the cSIL microscope constitutes the overall PSF of the PEM instrument and can be obtained by following the steps in Section 3.1 (ignoring the refraction from the SIL-objective interface). We omit the derivation steps for brevity and present the derived Green's function for a cSIL in Eq. 3.14. Note that the components with aSIL in Eq. 3.13 are replaced with SIL to represent the cSIL geometry. In addition, we consider the reflection scenario instead of the transmission, where the dipole is considered to be located at the cSIL side of the cSIL-ins interface (e.g. transistors) for bulk silicon chips ( $\vec{r}_d = (0, 0, 0)$ ).  $r_{\rm SIL}^s$  and  $r_{\rm SIL}^p$  represent the reflection coefficients for the cSIL-ins interface and R denotes the radius of the cSIL.

$$\overset{\leftrightarrow}{G}_{\rm SIL} = -\frac{ik_{\rm det}f_{\rm obj}}{8\pi f_{\rm det}} \sqrt{\frac{n_{\rm obj}}{n_{\rm ccd}}} e^{i(k_{\rm det}f_{\rm det}+k_{\rm obj}f_{\rm obj})} \begin{bmatrix} I_0 + I_{21} & I_{22} & -2iI_{11} \\ I_{22} & I_0 - I_{21} & -2iI_{12} \\ 0 & 0 & 0 \end{bmatrix}, \quad (3.14)$$

where

$$I_{0} = \int_{0}^{\theta_{\max}} \sin \theta_{\text{obj}} \sqrt{\cos \theta_{\text{obj}}} \left( t_{\text{SIL}}^{s} \Phi^{(3)} + t_{\text{SIL}}^{p} \Phi^{(2)} \cos \theta_{\text{obj}} \right) J_{0}(\rho) e^{i(k_{\text{SIL}} - k_{\text{obj}})R} \, \mathrm{d}\theta_{\text{obj}},$$
$$I_{11} = \int_{0}^{\theta_{\max}} \sin \theta_{\text{obj}} \sqrt{\cos \theta_{\text{obj}}} \left( t_{\text{SIL}}^{p} \Phi^{(1)} \sin \theta_{\text{obj}} \right) J_{1}(\rho) e^{i(k_{\text{SIL}} - k_{\text{obj}})R} \cos \varphi \, \mathrm{d}\theta_{\text{obj}},$$

$$\begin{split} I_{12} &= \int_{0}^{\theta_{\text{max}}} \sin \theta_{\text{obj}} \sqrt{\cos \theta_{\text{obj}}} \left( t_{\text{SIL}}^{p} \Phi^{(1)} \sin \theta_{\text{obj}} \right) J_{1}(\rho) e^{i(k_{\text{SIL}} - k_{\text{obj}})R} \sin \varphi \, \mathrm{d}\theta_{\text{obj}}, \\ I_{21} &= \int_{0}^{\theta_{\text{max}}} \sin \theta_{\text{obj}} \sqrt{\cos \theta_{\text{obj}}} \left( t_{\text{SIL}}^{s} \Phi^{(3)} - t_{\text{SIL}}^{p} \Phi^{(2)} \cos \theta_{\text{obj}} \right) J_{2}(\rho) e^{i(k_{\text{SIL}} - k_{\text{obj}})R} \cos 2\varphi \, \mathrm{d}\theta_{\text{obj}}, \\ I_{22} &= \int_{0}^{\theta_{\text{max}}} \sin \theta_{\text{obj}} \sqrt{\cos \theta_{\text{obj}}} \left( t_{\text{SIL}}^{s} \Phi^{(3)} - t_{\text{SIL}}^{p} \Phi^{(2)} \cos \theta_{\text{obj}} \right) J_{2}(\rho) e^{i(k_{\text{SIL}} - k_{\text{obj}})R} \sin 2\varphi \, \mathrm{d}\theta_{\text{obj}}, \\ \rho &= \sqrt{x^{2} + y^{2}}, \qquad \varphi = \tan^{-1}(y/x), \\ x &= -(k_{\text{det}} \sin \theta_{\text{det}} x_{\text{det}} + k_{\text{SIL}} \sin \theta_{\text{obj}} x_{d}), \qquad y = -(k_{\text{det}} \sin \theta_{\text{det}} y_{\text{det}} + k_{\text{SIL}} \sin \theta_{\text{obj}} y_{d}), \\ \Phi^{(1)} &= e^{-iz_{d}k_{z,\text{SIL}}} + e^{iz_{d}k_{z,\text{SIL}}} r_{\text{SIL}}^{p}, \\ \Phi^{(2)} &= e^{-iz_{d}k_{z,\text{SIL}}} - e^{iz_{d}k_{z,\text{SIL}}} r_{\text{SIL}}^{s}, \\ \Phi^{(3)} &= e^{-iz_{d}k_{z,\text{SIL}}} + e^{iz_{d}k_{z,\text{SIL}}} r_{\text{SIL}}^{s}, \\ t_{\text{SIL}}^{s} &= t_{\text{SIL}}^{p} = \frac{2n_{\text{SIL}}}{n_{\text{obj}} + n_{\text{SIL}}}. \end{split}$$

In this section, our aim is to reduce the spot-size (defined by the FWHM of the central lobe) of the PSF. The pupil masks that we would like to optimize are in the form of concentric annular rings and are placed at the pupil plane of the backing objective as shown in Fig. 3.18.

### 3.4.1 Mask parametrization and objective function

The mask  $M_{r,a}$  is parametrized by the set of radii  $\mathbf{r} = (r_1, r_2, \ldots, r_k)$ , which denote the radii separating different k subsections of the mask as illustrated in Fig. 3.18, and the set of coefficients  $\mathbf{a} = (a_1, a_2, \ldots, a_k)$ , which denote the values the mask take at each of the subsections such that  $M_{r,a}(r) = a_j$  for  $r_{j-1} \leq r \leq r_j$ . Also let  $\mathbf{p} = (\mathbf{r}, \mathbf{a})$ and  $M_{\mathbf{p}} = M_{r,a}$ .

Our aim is to increase the resolution by engineering a pupil mask, however the mask will impose a trade-off by decreasing the intensity of the central peak and



Figure 3.18: Illustration of the pupil mask, its location and parameters.

increasing the intensity of the side-lobes as we discussed previously. Therefore, we define the following three performance parameters of the system: the spot-size of the central lobe divided by the same in the clear aperture case G, peak intensity of the side-lobes divided by the peak intensity of the central lobe L and peak intensity of the central lobe divided by the same in the clear aperture case S (also referred to as the Strehl-ratio). With the defined performance parameters, an example objective function which we aim to maximize will be of the form

$$g(\boldsymbol{p}) = -\alpha_1 G(M_{\boldsymbol{p}}) + \alpha_2 S(M_{\boldsymbol{p}}) - \alpha_3 L(M_{\boldsymbol{p}}), \qquad (3.15)$$

where the  $\alpha$  terms are the tunable weight coefficients. Our aim is to maximize an objective function similar to Eq. 3.15 with predetermined weights, where the weights  $\alpha$  can be increased or decreased depending on which term we would like to emphasize. Here the objective function is presented as an example to illustrate what we would like to achieve with mask optimization. In Section 3.4.3 we will refine this objective function to obtain a more robust framework with a single tuning parameter that trade-offs between the resolution and Strehl-ratio, while controlling the side-lobe intensities.

#### 3.4.2 Gaussian Process optimization

The objective function in Eq. 3.15 does not have a closed-form mathematical expression. It needs to be evaluated for each value of parameters (a and r) if we would like to find the exact optimum solution, which is computationally infeasible. For this reason, we propose to use GP optimization, which is a powerful strategy to optimize (in our case, maximize) cost functions which do not have closed form expressions or that are otherwise expensive to compute (Brochu et al., 2010). GP optimization defines a sequential evaluation strategy, such that the objective function is evaluated at a chosen point in the parameter space and a probabilistic estimate of the function is updated at each iteration. This strategy trade-offs between exploring (where the objective function is expected to be high) the parameter space.

The GP optimization algorithm considers the function  $g(\mathbf{p})$  as a Gaussian random process with mean function  $\mu(\mathbf{p})$  and a covariance function  $k(\mathbf{p}, \mathbf{p}')$  which is selected beforehand. A surrogate function called the acquisition function  $u(\mathbf{p})$  is defined using the conditional mean and standard deviation of the process, conditioned on previously sampled function values. This function is selected such that it is easier to evaluate than the objective function. At each iteration t, the next point to be sampled is determined by the maximizer  $\mathbf{p}_t$  of this function, conditioned on previous samples  $\mathbf{p}_1, \ldots, \mathbf{p}_{t-1}$ . Ideally, we would like the maximum to correspond to a point with high mean (expected to be near the optimum of the underlying function) or high standard deviation (where there is uncertainty about the function value). Afterwards the function is sampled at the maximizer point  $\mathbf{p}_t$  to obtain the function value  $g(\mathbf{p}_t)$ and the mean and covariance of the GP model is updated using  $\mathbf{p}_t$  and  $g(\mathbf{p}_t)$ . These acquisition function maximization and model update steps are repeated until the optimal value among the evaluations do not change for a number of steps (i.e., the optimum is found) or a maximum number of evaluations is reached. The details of the algorithm can be found in (Brochu et al., 2010).

The specific acquisition function we use is called the upper confidence bound and is of the form

$$u(\boldsymbol{x}) = \mu(\boldsymbol{p}) + \kappa \sigma(\boldsymbol{p}),$$

where  $\kappa$  is the trade-off parameter between the mean and the variance. The covariance function that we specify for the mask optimization is

$$k(\boldsymbol{p}, \boldsymbol{p}') = \exp\left(-\frac{1}{2\delta^2}d(M_{\boldsymbol{p}}, M_{\boldsymbol{p}'})\right),$$

where we define

$$d(M_{p}, M_{p'}) = \int_{0}^{r_{k}} |M_{p}(r) - M_{p'}(r)|^{2} dr.$$

An example of how Bayesian optimization works in 1-D parameter space can be found in Fig. 3.19. The dashed line is the underlying objective function, the solid line is the estimated mean of the objective function and the shaded region is the  $\pm 1$ standard deviation interval at each point. At each step, using the new observation  $\boldsymbol{p}$ , the mean and the standard deviation of the objective function is updated and the acquisition function is recalculated for each parameter value. Here, the  $\kappa$  term is equal to 1, meaning  $u(\boldsymbol{p}) = \mu(\boldsymbol{p}) + \sigma(\boldsymbol{p})$ . The new evaluation point is selected as the point that maximizes the acquisition function.

## 3.4.3 Simulation results

For our simulations we start by refining the cost function in Eq. 3.15 to obtain a more robust cost function with a single weight parameter  $\alpha$ , as given in Eq. 3.16. Here we replaced the term related to the side-lobe intensities with a hinge function which encourages the side-lobe intensity ratio L to be smaller than a predetermined threshold  $L_{\rm th}$ . By controlling the side-lobe intensities with the hinge function we can



Figure 3.19: Illustration of Bayesian optimization steps on a 1-D example. Adapted from (Brochu et al., 2010).

modify the weight term  $\alpha$  to observe the trade-off between the resolution and the collection efficiency.

$$g(\mathbf{p}) = -\alpha G(M_{\mathbf{p}}) + (1 - \alpha)\sqrt{S(M_{\mathbf{p}})} - \max(0, L(M_{\mathbf{p}}) - L_{\rm th}).$$
(3.16)

The Strehl-ratio, S, can take values between 0 and 1, and by taking the square root of it we favor the solutions close to 1, by penalizing the solutions close to 0 more heavily. Note that the same cost function would have worked without taking the square root, however we empirically observed that defining the cost function in this manner results in a more efficient characterization of the trade-off by varying  $\alpha$ .

In order to evaluate the cost function for a given mask, we calculate the Green's function of the microscope. The experimental studies on the photon leakage emission indicate the emission wavelength to be between 1.5-2.2  $\mu$ m, peaking at 1.8  $\mu$ m (Kindereit et al., 2012). Therefore, in our calculations we fix the NA of the microscope

to 3 at the peak wavelength and calculate the Green's function for the given wavelength range, considering the change in the refractive indices for the cSIL region (Si) and the insulating region (SiO<sub>2</sub>) and add the resulting intensities at each wavelength incoherently to obtain the overall PSF.

In Fig. 3.20 we illustrate the PSF and its horizontal and vertical cross-sections for a horizontally polarized dipole in the clear aperture case (i.e. without a mask). Note that the PSF is symmetric along the horizontal (x) and vertical (y) axes. The resulting PSF has a FWHM of 312 nm and 306 nm in the x and y axes, respectively. The maximum side-lobe ratio L is found to be 0.06 along the y axis.



**Figure 3.20:** (a) PSF of the PEM instrument for the clear aperture case. (b) Cross-sections of the PSF taken along the x and y axes.

Next, we will investigate the performance of different masks on the resolution. In the calculation of the cost function, the resolution term G is calculated as the maximum of the FWHM along the x and y axes, and the side-lobe term L is calculated to be the maximum of the ratio along the x and y axes. Following (Yurt, 2014), we encourage L to be smaller than 0.15 in all our calculations by setting  $L_{\rm th} = 0.15$ . We consider a complex mask containing 4 rings with binary amplitudes (0 or 1) and phase components (0 and  $\pi$  radians) and run the GP algorithm for 200 iterations. We use  $\kappa = 3$  and  $\delta = 0.3$  in the acquisition and covariance functions. In order to understand the trade-off between the resolution and the Strehl-ratio, we conduct a parameter sweep on  $\alpha$  and plot the resulting curve in Fig. 3.21, with each point corresponding to a different weight parameter  $\alpha$ . We observe a linear increase in the spot-size as a function of the Strehl-ratio which we illustrate with the fitted linear curve in the figure. The figure indicates that it is possible to decrease the spot-size from 312 nm to 240 nm at a Strehl-ratio of 0.05. When implementing such masks, it is important to keep in mind that decreasing the Strehl-ratio will result in a decreased SNR, however even at a Strehl-ratio of 0.5 we can achieve a 280 nm spot-size, which is a 10% improvement over the 312 nm in the clear aperture case.



Figure 3.21: Strehl-ratio vs. spot-size.

In Fig. 3.22, two examples of such masks and their resulting PSFs are illustrated. Note that the masks are circularly symmetric and hence they are illustrated by their cross-sections. We plot the mask cross-sections as a function of  $\theta_{obj}$  where the mask radius r is given by  $r = f_{obj} \sin \theta_{obj}$ . The top row shows an example with a higher Strehl-ratio of 0.7, resulting in a spot-size of 289 nm and a side-lobe ratio of 0.146. The bottom row illustrates another example with a lower Strehl-ratio of 0.22 with a spot size of 255 nm and a side-lobe ratio of 0.16. We note the increase in the side-lobe intensities as the spot-size decreases.



Figure 3.22: Examples of masks and their resulting PSFs. Top row and bottom row plot mask designs with higher and lower Strehl-ratios, respectively. (a,d) Cross-sections of the masks as a function of  $\theta_{obj}$ , (b,e) resulting PSFs, (c,f) cross-sections taken from the PSFs along the xand y axes.

# 3.5 Full electromagnetic model of an aSIL microscope

In addition to super-resolving masks, another approach to increase the resolution is through model-based post-processing methods such as using image reconstruction techniques utilizing the PSF of the system. The importance of having an accurate PSF model for a successful reconstruction is outlined in (Cilingiroglu et al., 2012), where the authors used an approximate model to conduct image reconstructions in the context of IC imaging using an aSIL. The authors concluded that because their approximate model did not fully characterize the optical system, their reconstruction technique did not always perform as well on experimental data as it did on simulated data.

So far, we used the Green's function to investigate and improve the performance

of an aSIL system, which corresponds to the collection PSF of the system. Motivated by the need for a full and an accurate model, in this section we develop the full electromagnetic model of a confocal scanning aSIL microscope. The full model consists of four parts: (1) illumination of the sample with focused light (illumination PSF), (2) interaction of the focused light with the sample (formation of the induced current on the sample), (3) far-field propagation of the induced current to the detector (collection PSF) and (4) image formation on the detector. Throughout this section we will consider the bulk silicon technology, where the objects of interest are buried in the insulating medium. It is possible to generalize the provided model to other geometries such as the SOI technology.

In a scanning confocal microscope, the object is illuminated by a focused spot to form an induced electric current density  $\vec{j}_e(\vec{r})$  in the object. The radiation scattered in the far-field due to this induced current density is then collected by the detector on the collection side. The overall electric field on the detector is expressed by (Novotny and Hecht, 2012)

$$\vec{E}_{\rm det}(\vec{r}_{\rm det}) = \vec{E}_0(\vec{r}_{\rm det}) + \omega^2 \mu_0 \int\limits_V \overleftrightarrow{G}(\vec{r}_{\rm det}, \vec{r}) \vec{j}_e(\vec{r}) \,\mathrm{d}\vec{r}, \qquad (3.17)$$

where  $\vec{r}$  is the position vector of the object,  $\vec{r}_{det} = (x_{det}, y_{det}, z_{det})$  is the position vector on the detector,  $\overleftrightarrow{G}$  is the Green's function of the microscope which corresponds to  $\overleftrightarrow{G}_{aSIL}$  derived in Section 3.1.  $\vec{E}_0$  denotes the homogeneous solution when  $\vec{j}_e = 0$ everywhere. For our microscope, this corresponds to the reflected field due to the focused light, which we denote as  $\vec{E}_{ref}$ . For example, for the bulk silicon technology it corresponds to the reflected field of the focused spot from the aSIL-ins interface.

With the obtained electric field on the detector, a pixel value corresponding to the scan position (a, b) is then obtained by integrating the intensity on the detector over an aperture W, which corresponds to the pinhole placed on the detector for the confocal microscope. The resulting image  $I_{\text{conf}}(a, b)$  is expressed as

$$I_{\rm conf}(a,b) = \iint_{W} |E_{\rm det}(x_{\rm det}, y_{\rm det})|^2 \, \mathrm{d}x_{\rm det} \, \mathrm{d}y_{\rm det}.$$
 (3.18)

Note that each pixel (a, b) is obtained by integrating the intensity of the electric field at the detector while raster scanning the focused field, therefore the induced current  $\vec{j}_e$  in Eq. 3.17 is also a function of (a, b). In the following subsections we will discuss the details of the full model.

## 3.5.1 Focused light

The focused field incident on the objects can be calculated using the angular spectrum representation (ASR) method (Novotny and Hecht, 2012). To simulate the overall image of an object buried in the insulating medium, we only need to calculate the incident field inside the aSIL region. This is because once we obtain the focused field inside the aSIL region, the calculated field will be imported to an FDTD solver which will propagate the light into the insulating medium while carrying out the calculations for the induced electric field on the objects.

The focused field inside the aSIL region is derived in (Chen et al., 2012). We provide the final expression of the focused field for brevity, the details of the derivation can be found in (Chen et al., 2012). For a horizontally polarized (x-polarized) light the focused field at location  $\vec{r}_{aSIL} = (x_{aSIL}, y_{aSIL}, z_{aSIL})$  is given by

$$\vec{E}_{\rm foc}(\vec{r}_{\rm aSIL}) = -\frac{ik_{\rm aSIL}f_{\rm obj}}{2} \sqrt{\frac{1}{n_{obj}}} e^{ik_{obj}f_{obj}} E_0 \begin{bmatrix} I_0^L + I_2^L \cos 2\phi \\ I_2^L \sin 2\phi \\ 2iI_1^L \cos\phi \end{bmatrix},$$
(3.19)

where

$$I_m^L = \int_{0}^{\theta_{\rm obj}^{\rm max}} (\cos \theta_{\rm obj})^{3/2} f_w \tan \theta_{\rm aSIL} J_m (k_{\rm aSIL} \rho \sin \theta_{\rm aSIL}) \Gamma_m^L e^{-ik_{\rm zaSIL} z_{\rm aSIL}} \,\mathrm{d}\theta,$$



Figure 3.23: (a) Focused field and (b) its cross-section at the aplanatic point of the aSIL.

$$\begin{split} \Gamma_0^L &= t_1^s + t_1^p \cos \theta_{\rm aSIL}, \\ \Gamma_1^L &= t_1^s \sin \theta_{\rm aSIL}, \\ \Gamma_2^L &= t_1^s - t_1^p \cos \theta_{\rm aSIL}, \end{split}$$

and  $J_m$  denotes the Bessel function of order m,  $t_1^s$  and  $t_1^p$  are the Fresnel coefficients for transmission at the aSIL interface when the wave is traveling from the objective region to the aSIL region and  $E_0$  is a constant that scales the magnitude of the incident field.  $f_w = e^{-\frac{1}{f_0^2} \frac{\sin^2 \theta_{\text{obj}}}{\sin^2 \theta_{\text{obj}}}}$  is the apodization function of the objective, where  $f_0$  is the filling factor of the incident Gaussian beam (Novotny and Hecht, 2012).

In Fig. 3.23, we illustrate the intensity profile of the focused field at the aplanatic point of the aSIL ( $z_{aSIL} = 0$ ), for an x-polarized light at a wavelength of 1340 nm and NA of 3.4.

#### 3.5.2 Interaction of the light with the sample

In order to calculate the image of an arbitrary structure at the detector, we need to calculate the induced electric current density  $\vec{j}_e$  on the structures, formed due to the
focused light. A closed form solution does not exist to calculate the induced current for structures with arbitrary shapes. For this reason, we use the finite difference time domain (FDTD) method to calculate the induced electric field  $\vec{E}_{ind}$  on the structures (Foreman and Török, 2011). With the obtained induced electric field, the induced current density on the structures is calculated using (Novotny and Hecht, 2012)

$$\vec{j}_e(\vec{r}) = -iw\epsilon_0[\epsilon(\vec{r}) - \epsilon_{\rm ref}(\vec{r})]\vec{E}_{\rm ind}(\vec{r}), \qquad (3.20)$$

where w is the angular frequency of the light,  $\epsilon_0$  is the permittivity of the free space,  $\epsilon$  is the dielectric constant of the whole space,  $\epsilon_{\text{ref}}$  is the dielectric constant of the background (where the object is located),  $\vec{E}_{\text{foc}}$  is the electric field induced on the sample due to the focused light and  $\vec{r}$  is the position vector.

The FDTD method discretizes both space and time and iteratively solves the Maxwell's equations for any arbitrary shape in a predefined boundary until convergence is reached (Schneider, ). We use the commercial software Lumerical FDTD Solutions for the implementation of the FDTD method. One drawback of using the FDTD method is that it is both computationally and memory-wise expensive. Therefore, we do not include the aSIL in the predefined boundary and include only a portion of the silicon substrate of the chips and the insulating medium which contains the objects of interest. For this purpose, we calculate the focused light in the aSIL region and import the incident field to the FDTD solver. The solver then propagates the imported field to the insulating medium to calculate the induced electric field on the structures, which is then used to calculate the induced current density using Eq. 3.20.

#### 3.5.3 Far-field propagation

Once the induced current on the structures is obtained, it is propagated to the far-field to calculate the field scattered by the sample structures. We use the Green's function derived in Section 3.1 for this purpose. We treat each voxel on the object with the given induced current density as a point dipole and take the integral in Eq. 3.17 to calculate the field on the detector.

#### 3.5.4 Image formation on the detector

In order to simulate the image of an object, the electric field on the detector  $\vec{E}_{det}$ in Eq. 3.17 needs to be calculated at each scan position. So far we discussed every component in Eq. 3.17 except for the homogeneous field  $\vec{E}_0$ , which we will refer to as the reflected field  $\vec{E}_{ref}$ . The schematic for calculating the reflected field is shown in Fig. 3.24. The incident beam is first reflected by the beam splitter (BS) and focused on the ins-aSIL interface by the aSIL in the absence of any objects. The reflected light from this interface is then collected by the aSIL and transmitted through the BS and focused on the detector by a second lens.



Figure 3.24: Schematic of the aSIL illustrating the parameters for the derivation of the reflected field.

We start by deriving  $\vec{E}_{ref}$  for a horizontally polarized (x-polarized) light  $\vec{E}_{inc} = E_{inc}\hat{x}$ . In cylindrical coordinates the incident beam is expressed as

$$\vec{E}_{\rm inc} = E_{\rm inc} [\cos\phi\,\hat{\rho}_0 - \sin\phi\,\hat{\phi}]. \tag{3.21}$$

After the refraction at the first lens (GRS1), assuming that the transmission coefficients for the objective lens are equal to one, the electric field becomes (Novotny and Hecht, 2012)

$$E_{\rm inc}[\cos\phi\,\hat{\theta}_{\rm obj} - \sin\phi\,\hat{\phi}]\sqrt{\frac{n_0}{n_{\rm obj}}}\sqrt{\cos\theta_{\rm obj}}.$$
(3.22)

The electric field is then refracted by the aSIL and the field inside the aSIL region is expressed as

$$\vec{E}_{\text{aSIL}} = E_{\text{inc}}[t_1^p \cos\phi \,\hat{\theta}_{\text{aSIL}} - t_1^s \sin\phi \,\hat{\phi}] \sqrt{\frac{n_0}{n_{\text{obj}}}} \sqrt{\cos\theta_{\text{obj}}}, \qquad (3.23)$$

where  $t_1^p$  and  $t_1^s$  are the Fresnel coefficients for transmission from the objective region to the aSIL region. Inside the aSIL region, once the electric field is reflected by the aSIL-ins interface, the reflected field is given by

$$\vec{E}_{\text{ref,aSIL}} = E_{\text{inc}} e^{-2ik_{z,\text{aSIL}}d} \left[ -r_{\text{ins}}^p t_1^p \cos\phi \,\hat{\theta}_{\text{aSIL}} - r_{\text{ins}}^s t_1^s \sin\phi \,\hat{\phi} \right] \sqrt{\frac{n_0}{n_{\text{obj}}}} \sqrt{\cos\theta_{\text{obj}}}, \quad (3.24)$$

where  $r_{\text{ins}}^p$  and  $r_{\text{ins}}^s$  are the Fresnel coefficients for reflection from the aSIL-ins interface, and d is the depth of the interface with respect to the aplanatic point of the aSIL. Next, the field refracted by the aSIL can be expressed as

$$\vec{E}_{\rm ref,obj} = E_{\rm inc} e^{-2ik_{z,\rm aSIL}d} \left[-t_2^p r_{\rm ins}^p t_1^p \cos\phi \,\hat{\theta}_{\rm aSIL} - t_2^s r_{\rm ins}^s t_1^s \sin\phi \,\hat{\phi}\right] \sqrt{\frac{n_0}{n_{\rm obj}}} \sqrt{\cos\theta_{\rm obj}}, \quad (3.25)$$

where  $t_2^p$  and  $t_2^s$  are the Fresnel coefficients for transmission from the aSIL region to the objective region. For simplicity we combine the Fresnel coefficients and denote  $c^p = t_2^p r_{ins}^p t_1^p$  and  $c^s = t_2^s r_{ins}^s t_1^s$ . After the refraction from the aSIL, the field refracted by the objective lens (GRS1) is given by

$$\vec{E}_{\text{ref},0} = E_{\text{inc}} e^{-2ik_{z,\text{aSIL}}d} [-c^p \cos\phi \,\hat{\theta} - c^s \sin\phi \,\hat{\phi}]$$
(3.26)

which propagates in the positive z direction as a collimated beam. After the refraction

from the second lens (GRS2), the reflected field is given by

$$\vec{E}_{\text{ref,det}} = E_{\text{inc}} e^{-2ik_{z,\text{aSIL}}d} \left[ -c^p \cos\phi \,\hat{\theta}_{\text{det}} - c^s \sin\phi \,\hat{\phi} \right] \sqrt{\frac{n_0}{n_{\text{det}}}} \sqrt{\cos\theta_{\text{det}}}.$$
 (3.27)

Plugging in the expressions for  $\hat{\phi}$  and  $\hat{\theta}_{det}$ , the obtained field can be expressed in Cartesian coordinates as

$$\vec{E}_{\rm ref,det} = -E_{\rm inc} e^{-2ik_{z,\rm aSIL}d} \begin{bmatrix} \cos^2 \phi \cos \theta_{\rm det} c^p - \sin^2 \phi c^s \\ \cos \theta_{\rm det} \sin \phi \cos \phi c^p + \sin \phi \cos \phi c^s \\ \sin \theta_{\rm det} \cos \phi c^p \end{bmatrix} \sqrt{\frac{n_0}{n_{\rm det}}} \sqrt{\cos \theta_{\rm det}}.$$
(3.28)

This field is focused on the detector by GRS2 with the relation

$$\vec{E}_{\rm ref} = -ik_{\rm det} f_{\rm det} \frac{e^{ik_{\rm det} f_{\rm det}}}{2\pi} \int_{0}^{\theta_{\rm det}^{\rm max}} \int_{0}^{2\pi} \vec{E}_{\rm ref,det} e^{ik_{\rm det} z_{\rm det} \cos\theta_{\rm det}} e^{i\vec{k}_{\rm det} \cdot \vec{r}_{\rm det}} \sin\theta_{\rm det} \,\mathrm{d}\theta_{\rm det} \,\mathrm{d}\phi_{\rm det}.$$
(3.29)

Combining Eqs. 3.28 with 3.29 and taking the integral results in

$$\vec{E}_{\rm ref} = i \frac{E_{\rm inc}}{2} k_{\rm det} f_{\rm det} e^{ik_{\rm det}f_{\rm det}} \left(\frac{f_{\rm obj}}{f_{\rm det}}\right)^2 \begin{bmatrix} I_0 - I_2 \cos 2\phi \\ -I_2 \sin 2\phi \\ 2iI_1 \cos \phi \end{bmatrix}, \qquad (3.30)$$

where

$$I_{0} = \int_{0}^{\theta_{\rm obj}^{\rm max}} f_{w} \cos \theta_{\rm obj} \sin \theta_{\rm obj} (c^{p} \cos \theta_{\rm det} - c^{s})$$
$$J_{0}(k_{\rm det}\rho \sin \theta_{\rm det}) e^{i(k_{z,\rm det}z_{\rm det} - 2k_{z,\rm aSIL}d)} \frac{1}{\cos \theta_{\rm det}} \,\mathrm{d}\theta_{\rm obj},$$
$$I_{1} = \int_{0}^{\theta_{\rm obj}^{\rm max}} f_{w} \cos \theta_{\rm obj} \sin \theta_{\rm obj} (c^{p} \cos \theta_{\rm det})$$
$$J_{1}(k_{\rm det}\rho \sin \theta_{\rm det}) e^{i(k_{z,\rm det}z_{\rm det} - 2k_{z,\rm aSIL}d)} \frac{1}{\cos \theta_{\rm det}} \,\mathrm{d}\theta_{\rm obj},$$

$$I_{2} = \int_{0}^{\theta_{\rm obj}^{\rm max}} f_{w} \cos \theta_{\rm obj} \sin \theta_{\rm obj} (c^{p} \cos \theta_{\rm det} + c^{s})$$
$$J_{2}(k_{\rm det} \rho \sin \theta_{\rm det}) e^{i(k_{z,\rm det} z_{\rm det} - 2k_{z,\rm aSIL}d)} \frac{1}{\cos \theta_{\rm det}} \,\mathrm{d}\theta_{\rm obj}$$

With the derived reflected field, we have all the components to calculate the image of an object using Eq. 3.17. To summarize the procedure for the simulations, given an object, we first calculate the focused field at a transversal plane close to the aplanatic point inside the aSIL medium. We choose to calculate the field at 100 nm away from the aplanatic point in our simulations. The calculated field is then imported to the FDTD solver. Since this is a confocal microscope, either the object or the incident beam needs to be scanned. Due to the infeasibility of scanning the object, the experimental data is usually obtained by scanning the beam, therefore the aplanatic conditions are not satisfied except for the central position. However, for simplicity we assume that the aplanatic conditions are satisfied at all positions and scan the object. Note that a more rigorous model is needed to model the non-aplanatic conditions.

For a given scan position (a, b), we calculate the induced current density on the object with the FDTD method and conduct the far-field propagation to the detector using the Green's function. The reflected field in Eq. 3.30 is added to the resulting field to obtain  $E_{det}$ . Integrating the intensity of this field over an aperture using Eq. 3.18 gives us the intensity value for the pixel (a, b). Repeating this process for each scan position gives us the overall image.

#### 3.5.5 Simulation results

We first used the full model to calculate the total PSF of the microscope. Note that due to the non-linearity caused by the interference between the scattered and the reflected fields, the PSF of the microscope depends on the size, shape and material of the object and the refractive indices of the surrounding media. As an example, we simulated the image of an aluminum spherical particle with a radius of 25 nm placed on the air side of the aSIL-air interface. Note that so far we considered aSIL-ins interface as shown in Fig. 3.1, here we replace the insulating medium with air. We calculate the image of the particle at an NA of 3.4 and using a wavelength of 1340 nm, a step size of 25 nm for scanning the object and considering the aperture W to be a pinhole with 6  $\mu m$  diameter. The resulting PSF is shown in Fig. 3.25.



Figure 3.25: Point spread function of the microscope for an Al sphere located at the Si-air interface.

Before the full model was developed, the authors in (Cilingiroglu et al., 2012) approximated the PSF using only the reflected field  $E_{\rm ref}$  and used image reconstruction methods to increase the resolution of aSIL images of integrated circuits. As mentioned at the beginning of this section, their method did not perform as well on the experimental data as their simulations suggested since their model did not capture the interference between the field scattered by the objects and the reflected field. However, they were able to show resolution improvements on experimental aSIL data after adapting the PSF developed in this section to their reconstruction framework (Cilingiroglu et al., 2015). This illustrates the importance of having an accurate model in post-processing enhancement methods. We refer the reader to (Cilingiroglu, 2015) for more details on the reconstruction framework. In order to validate our model with experimental data, we simulate the image of a single Al bar located on the air side of aSIL-air interface. The Al bar we consider has a height of 570 nm, width of 150 nm and depth of 50 nm. We use the same parameters used in the generation of the PSF with the Al sphere, and only change the NA from 3.4 to 3.3. Figure 3.26(a) shows the scanning electron microscope (SEM) image of the Al structure. Figures 3.26(b) and 3.26(c) compare the experimental data with our simulated data, and Fig. 3.27 illustrates the cross-sections taken from the center of the experimental and simulated data along the x axis. The intensity of the images are normalized by the intensity of the background. The asymmetry in the experimental data in Fig. 3.26(b) is thought to be caused by the misalignments in the experimental set-up. We observe that the simulation result is similar to the experimental data in terms of location of the dips, followed by the brighter ring around the Al structure. However, we also note differences in the results, such as the higher contrast of the simulated data compared to the experimental data.



**Figure 3.26:** (a) SEM, (b) experimental and (c) simulated image of an Al bar.

The discrepancy between the experimental and the simulated data can be attributed to the mismatch between the assumptions made about the modeled set-up and experimental set-up. For example, the material properties of the deposited Al structure could be different from the ideal properties, which we consider in our simulations. In addition, for simplicity we ignored the air-gap between the aSIL and the substrate of



Figure 3.27: Cross-sections taken from the experimental and simulated image of the Al bar in Figure 3.26.

the integrated circuit and the possible mismatch between the radius of the aSIL and the thickness of the substrate. Similarly, the model assumes that aplanatic conditions are satisfied during the scanning of the object, whereas the experimental data is obtained by scanning the incoming beam in contrast to scanning the object. All these factors contribute to the mismatch between the experimental and simulated data. While a more rigorous model is needed to account for some of the aforementioned mismatches, our model is still capable of capturing the characteristics of the microscope, letting us investigate the effect of various parameters on the performance, as well as making it possible to use pre-processing and post-processing techniques to increase the resolution of the microscope.

### 3.6 Conclusions

In this chapter we derived the dyadic Green's function of an aSIL microscope and used it to investigate the performance of the microscope for bulk silicon and SOI chips. We showed that the performance of the microscope deteriorates for higher level metal layers due to the effects of forbidden light. Similarly we observed that the thickness of the BOx layer in SOI chips affects the imaging performance, with thicker BOx layers leading to lower resolution and collection efficiency. In addition, we proposed an optimization framework for designing super-resolving pupil masks. We showed the trade-offs between the resolution and light collection efficiency or side-lobe intensity for different mask designs. Finally, building upon the derived Green's function, we formulated the full electromagnetic model of the microscope including the focused and reflected fields.

We focused on developing an accurate model and utilizing it to increase the resolution in the context of IC imaging. The demand for higher resolution imaging increases with the ever decreasing sizes of the ICs, however improving the resolution of the microscope imposes aforementioned trade-offs. Due to these trade-offs, super-resolution methods such as pupil masks or post-processing techniques cannot keep up with the shrinking sizes of modern circuitry. In the next chapter, we consider an alternative approach where instead of trying to resolve each individual structure in an IC, we consider a gate-level optical measurement system for the application of detecting malicious tampering of ICs.

# Chapter 4

# Gate classification methods for detecting malicious tampering of integrated circuits

In this chapter, we develop classification methods for identifying different types of digital gates in ICs. The ability to identify different gate types is particularly useful in detecting malicious tampering of ICs, termed hardware Trojans, where the insertion of a Trojan often presents itself as insertion, addition or deletion of logic gates as reviewed in Chapter 2. As opposed to utilizing side-channel methods such as time delay or power based algorithms, our method works by imaging the layout of an IC. Since any change in the functionality of an IC would directly correspond to a change in the physical layout of a chip, inspecting the physical layout offers great advantages over side-channel methods in detecting hardware Trojans.

While super-resolution techniques are able to push the limits of optical resolution of aSIL microscopy for IC imaging, as IC dimensions continue to decrease rapidly, these methods are not sufficient to resolve individual structures in a modern chip. In this chapter, instead of trying to resolve individual structures at a high resolution, we focus on lower resolution imaging methods and rely on post-processing techniques to identify each gate in a chip for detecting hardware Trojans. Note that an advantage of imaging in low resolution regimes is the reduced acquisition times for Trojan detection. A modern chip with billions of transistors covers an area on the order of cm<sup>2</sup>. Even at practically impossible MHz acquisition rates, it would take from a few hours up to a few days to image the whole chip using a conventional scanning confocal microscope with step-sizes on the order of 10-100 nm at high resolution.

In the first part of this chapter we develop a gate classification method using a multi-spectral imaging framework. This framework is based on decreasing the resolution of the microscope with a spot-size on the order of a gate-length and collecting one measurement per gate ( $\approx 1\mu$ m) at multiple wavelengths, which speeds up the acquisition compared to the conventional scanning microscopes. In the second part, we develop a more advanced classification method based on higher resolution images to complement the approach in the first part. This method is proposed as a refinement over the first method, to be used in re-evaluating the decisions on the gate types with low confidence values in the former approach.

# 4.1 Rapid identification of gates using multi-spectral reflectance measurements at low resolution

In this section we develop a gate classification algorithm on low resolution gate-level spectroscopic measurements. Our framework exploits the fact that each gate type (such as AND, OR, NAND, etc.) will have a distinct signature when imaged at a given wavelength. These distinct signatures are a result of unique patterns of polysilicon and metal structures of each gate type, which will scatter light differently at different wavelengths. We consider the six basic gate types, namely AND, OR, NAND, NOR, XOR and XNOR, whose dimensions are approximately  $1\mu$ m in a 45 nm node technology (Nangate Inc, ). These gates are the six smallest 2-input gates provided in the Nangate 45 nm open source library. The metal 1 (M1) layers and the contacts of these gates are illustrated in Fig. 4.1.

We select the NA of our imaging system such that the spot-size of the system covers a single gate area to be able to capture the overall characteristics of the whole gate with a single measurement. Using Abbe's approximation on the spot-size  $(0.61\lambda/NA)$ , an



**Figure 4.1:** Layouts for the M1 layer (black lines) and contacts (gray squares) for (a) AND, (b) OR (c) NAND, (d) NOR, (e) XOR and (f) XNOR gates.

NA of 0.8 at  $\lambda = 1340$  nm results in a spot-size of  $\approx 1\mu$ m. This allows us to represent the signature of each gate without the need for dense raster scanning. However, at such low resolutions, measurements at a single wavelength are not sufficient to distinguish between different gates as we will observe in the following sections. For this purpose we use measurements with different wavelength/polarization combinations. Ideally, higher number of measurements provides more information about the gate types, however it should be noted that each additional measurement is a separate experiment and affects the total acquisition time. We empirically observed that 5 wavelength/polarization combinations are sufficient to identify different gates, while ensuring a rapid acquisition. The wavelength/polarization selection process is based on the model of the system, and will be discussed in more detail in Section 4.1.2. In the next section we elaborate on the physical model of the optical system.

#### 4.1.1 Model of the system

We use an FDTD method to simulate the responses of different gate types. The location of the M1 and contact layers is obtained from the NanGate library (Nangate Inc, ) and the M1 layer is placed 100 nm above the SIL-ins (Si-SiO<sub>2</sub>) interface, inside the insulating medium. The M1 layer and the contacts are selected to be copper and tungsten respectively with a height of 130 nm as indicated in the library. In order to obtain observations for our classification framework, we generate 4x5 or 5x5 random tiling of gates in each FDTD simulation and run multiple simulations with different tilings.

For simplicity we use the cSIL configuration, however instead of the focused light we assume a uniform, linearly polarized, normally incident plane wave illumination and use periodic boundary conditions in the lateral plane and absorbing (PML) boundary conditions on the transversal plane. Note that with plane wave illumination we neglect spatial selectivity on the illumination side and over-estimate the interference from the nearby objects. However, this approximation is necessary as it eliminates the need for scanning the focal spot and can generate the responses for multiple gates and wavelengths in one simulation. This means that we can simultaneously generate the responses of approximately 20-25 gates and 60 wavelengths, which would have each necessitated a separate simulation otherwise.

The near-fields of the gates are recorded on a plane inside the aSIL region for a wavelength range of 1–3  $\mu$ m and are propagated to far-field via the near-to-far-field transform using the FDTD solver (Lumerical Solutions Inc, ). Note that this is different from the model we developed in Chapter 3, as in Chapter 3 we collected the induced

current on the objects and used the Green's function for far-field propagation and here we collect the near-field inside the aSIL region and use the solver for propagation. While the latter one is simpler for the cSIL configuration, it would require a more rigorous model for the aSIL configuration. This is because in the cSIL configuration the refraction from the SIL-objective interface can be ignored, but it must be accounted for in the aSIL configuration. With the obtained far-field, the image formed by the system is calculated accounting for the NA of the system using the angular spectrum representation method. Finally, to calculate the response of each gate in the simulation domain, the integrated intensity over the integration window W is normalized by the source power delivered to the same area in the object space. From here on this response will be referred to as the reflectance measurement. While the model of this particular system is not a contribution of this thesis, the steps of the model were described briefly for completeness. The model and the data in this chapter are generated by Dr. Ronen Adato and the interested reader is referred to (Adato et al., 2016) for the details.

#### 4.1.2 Gate identification

Figure 4.2 illustrates the spectral response of infinite tiling of each gate for x and y polarizations at NA = 0.8, with the size of the integration window W selected to be the size of the corresponding gate. We observe that the spectral response of AND/OR, NAND/NOR and XOR/XNOR pairs are similar to each other, which can be attributed to their similar layouts as shown in Fig. 4.1. While we illustrate a single example of the simulated spectra, variations in the measurements such as contributions from different neighboring gates, defocus effects and detector noise will affect the measured signal. For our initial analysis, we assume that such effects will form a zero mean, additive white Gaussian noise with a standard deviation of  $\sigma$  on the measured signal and propose to use a Bayesian classifier to identify different gate types (Duda et al.,





Figure 4.2: Spectral reflectance measurements for the six gates for (a) horizontal (x) polarized (b) vertical (y) polarized illumination at NA = 0.8.

In order to understand the effect of noise on the classification performance, for our initial analysis we compute the accuracies corresponding to Bayes error rates for different noise levels. Before we introduce the formula for the classification accuracy, we define some useful terminology for the classification framework. Given a measurement  $\mathbf{M}$ , our aim is to classify the vector  $\mathbf{M} = [M_1, \ldots, M_K]$  into one of the L(L = 6) classes (gate types), where  $M_j$  is a single measurement (feature) for a given wavelength/polarization and K is the maximum number of features we would like to use. Let  $P(c_l)$  denote the *a priori* class probability of class  $l \in \{1, \ldots, L\}$  and  $P(\mathbf{M}|c_l)$  denote the *likelihood* of the class (the conditional probability density of the measured signal  $\mathbf{M}$  given that it belongs to the class l). The *a posteriori* probability  $P(c_l|\mathbf{M})$  (the probability of the gate belonging to class l given the given measurement  $\mathbf{M}$ ) is given by the Bayes rule

$$P(c_l|\mathbf{M}) = \frac{P(\mathbf{M}|c_l)P(c_l)}{P(\mathbf{M})},$$
(4.1)

where  $P(\mathbf{M})$  is the probability of the given measurement. Bayesian classifier assigns the given measurement  $\mathbf{M}$  to the class  $c_l$  with the highest a posterior probability. The accuracy of the Bayesian classifier is then calculated using the formula

$$p_{\rm acc} = \sum_{l=1}^{L} \int_{C_l} P(\mathbf{M}|c_l) P(c_l) \,\mathrm{d}\mathbf{M},\tag{4.2}$$

where  $C_l$  denotes the region where class l has the highest posterior (Tumer and Ghosh, 2003). Note that since we assume that the noise is independent at each wavelength/polarization combination, the likelihood probability can be expressed as

$$P(\mathbf{M}|c_l) = P(M_1|c_l)P(M_2|c_l)\dots P(M_K|c_l).$$
(4.3)

Next, we investigate the total accuracy as a function of number of features for a fixed noise level of  $\sigma = 0.05$ , assuming a uniform distribution on the prior probabilities. For selecting a discriminative set of features we propose a greedy selection process, where we start from the feature that gives us the highest accuracy and continue adding the feature that obtains the maximum increase in the accuracy until the desired number of features is reached. Note that ideally, the accuracy should be calculated for each combination of wavelength and polarization measurements for selecting the features that result in the highest accuracy, however evaluating the multi-variate integral in Eq. 4.2 is computationally expensive for all combinations, hence we use the described greedy selection algorithm for feature selection. Using the selected features for  $\sigma = 0.05$ , we then calculate the accuracy for different noise levels. Figure 4.3(a) illustrates the classification accuracy as a function of number of features for  $\sigma = 0.05$ . We observe that increasing the number of features increases the accuracy with a drop in the rate of increase such that selecting one feature results in an accuracy of approximately 60% and we can achieve approximately 95% accuracy by increasing the number of features to 5. In Fig. 4.3(b), we use the same features we obtain in 4.3(a) and illustrate the classification accuracy as a function of the noise level. The results show that for noise levels  $\sigma < 0.03$  we can achieve accuracies above 99% and

as the noise level increases to  $\sigma = 0.1$  we observe a drop in the accuracy, where at  $\sigma = 0.1$  we can achieve a 70% accuracy.



Figure 4.3: Effect of the number of features and the noise level on the classification performance. Classification accuracy (a) as a function of number of features at noise level  $\sigma = 0.05$  (b) as a function of noise level using 5 features. Selected features are illustrated with dashed black lines for (c) *x*-polarization (d) *y*-polarization (legends same as in Fig. 4.2).

So far our simulations indicated that it is possible to identify different gates with high accuracy even at higher levels of noise (e.g.  $\sigma = 0.1$ ), where the noise is assumed to be zero-mean additive white Gaussian. Possible factors that can contribute to the variations in the measured signals include cross-talk between adjacent gates, sample alignment, defocus issues and detector noise. It is possible to overcome the issues related to defocus and sample alignment by engineering around them such as by using alignment markers. Therefore, considering our low resolution set-up with the spot-size on the order of the sizes of the gates, the prominent factor contributing to the variations in the measured signal will be the cross-talk between the neighboring gates in addition to the detector noise. In the remainder of this section we consider the detector noise and the cross-talk between the neighboring gates and evaluate the performance of our system.

In order to investigate the effect of cross-talk between the adjacent gates, 4x4 or 5x4 tiling of randomly selected gates are generated and their images are simulated using a 0.8 NA objective for a wavelength range of 1-3  $\mu$ m. Repeating this process multiple times with different tiles resulted in an average of approximately 60 observations for each gate type. For a given technology, the height of all the gates are fixed (so that the VDD and VCC rails that powers the chip are aligned), therefore a fixed number of gates in the vertical dimension (selected to be 4) are used for our simulations. However, since the gate widths are different in the horizontal dimension, the tiles are generated with the constraint that all the rows must have a fixed length in x, so that they are compatible with the periodic boundary conditions. The details of the constraints are explained in (Adato et al., 2016). Overall, 20 different tilings are generated that resulted in 22 observations each for the XOR and XNOR gates, and approximately 75 observations for each of the remaining gates that we consider. An example of such a tiling is shown in Fig. 4.4, where in Fig. 4.4(a) we illustrate a 4x4 tiling of the gates in the object space, in Fig.  $4 \cdot 4(b)$  we illustrate the simulated image of the gate for y-polarized illumination at  $\lambda = 1.22 \mu m$  and in Fig. 4.4(c) we illustrate the low resolution reflectance measurements of the tile with the integration window Wselected to be 1400 nm  $\times$  760 nm (height of the gates  $\times$  median width of the gates).

With the simulated data containing the reflectance measurements for multiple tilings, our aim is to propose a classification method using the reflectance measurements and evaluate its performance. So far our simulated data includes the variations caused by the interference due to the neighboring gates. In addition to this we also account for the detector noise and approximate it with an additive zero-mean white Gaussian. In (Adato et al., 2016) it is shown that it is possible to achieve a signal-to-noise ratio (SNR) of 100 in our set-up. Therefore, in order to account for the detector noise, we



**Figure 4.4:** Example tiling of the gates. (a) Layout of the 4x4 tiling, (b) Simulated 0.8 NA image of the layout, (c) simulated reflectance measurement for each of the gate in the tile for y-polarized illumination at  $\lambda = 1.22 \mu m$ . Scale bars in (a) and (b) correspond to 1  $\mu m$ .

add a series of random Gaussian noise with a standard deviation  $\sigma = 0.01$  to our simulated data.

We propose to use the maximum a posteriori (MAP) classifier which maximizes  $P(c_l|\mathbf{M})$  as defined in Eq. 4.1 over different classes  $l \in \{1, \ldots, L\}$ . To compute the posterior probability, we first need to obtain an estimate of the likelihood  $P(\mathbf{M}|c_l)$  for each class. We randomly split our data to use 2/3 of it as the training data to estimate the likelihood and the remaining 1/3 of it as the test data to calculate the accuracy of our system. Using the training data we can build the normalized histogram to obtain the likelihoods  $P(\mathbf{M}|c_l)$  as shown in Fig. 4.5. The prior probabilities  $P(c_l)$  are assumed to be uniform, however given a chip layout it is also possible to use the number of occurrences of each gate as a better estimate. We also include a feature selection step in our training procedure as in our previous analysis to pick the most discriminative set of features. As in our previous analysis we assume that the measurements are statistically independent across different wavelength and polarizations conditioned on the class label and compute the likelihood estimate using Eq. 4.3. The MAP classifier

with the conditional independence assumption is also referred to as the naive Bayes classifier.



**Figure 4.5:** Likelihood of the measurement for each class shown for x and y-polarized illumination. Intensity level illustrates the probability distribution. The discontinuities in some of the spectra are artifacts of the periodic boundary conditions caused by diffraction orders.

For the feature selection process, the training data is also randomly split into 2/3 and 1/3 partitions for conducting cross-validation. The likelihoods are estimated from the 2/3 of the training data and the greedy selection process that we described in our previous analysis is applied using the remaining 1/3 of the training data, which we call the cross-validation set. This is done by evaluating each candidate feature's performance on the cross-validation set and selecting the one with the best accuracy using Eq. 4.2. Then we repeat this procedure to add a new feature to the set of previously chosen ones until we obtain a total of 5 features.

Given a partition of the training data (into likelihood estimation and cross-validation sets), we obtain one set of 5 features using the above described procedure. To be more robust to the particular partitioning of the data, we repeat this process 10 times with different random partitions and choose the set of features with the highest cross-validation accuracy as our final feature set. The best performing 5 features (with the order they are selected) are found to be:  $\lambda = 1.22 \mu m$  with x-polarized illumination,  $\lambda = 1.22 \mu \text{m}$  with y-polarized illumination,  $\lambda = 1.36 \mu \text{m}$  with y-polarized illumination,  $\lambda = 1.09 \mu \text{m}$  with y-polarized illumination,  $\lambda = 1.59 \mu \text{m}$  with x-polarized illumination. Note that the selected features have shorter wavelengths than what is predicted with the analytical approach in Fig. 4.2; this is because the interference of the field scattered from the neighboring gates will be more prominent at longer wavelengths as the size of the point spread function of the microscope will be larger. Therefore, while our initial analysis helped us understand the limitations of our classification approach (e.g. the increase in performance as a number of features used and the decrease in the performance as a function of noise level), we can argue that it was not accurate in modeling the effect of the cross-talk between the neighboring gates.

Figure 4.6 illustrates the cross-sections taken from the likelihoods in Fig. 4.5 along the vertical direction at the selected features. From the plots we observe that with each



Figure 4.6: Likelihood of the measurement for each class at the 5 selected features with the order that they are selected. (a)  $\lambda = 1.22 \mu \text{m}$  x-polarized illumination, (b)  $\lambda = 1.22 \mu \text{m}$  y-polarized illumination, (c)  $\lambda = 1.36 \mu \text{m}$  y-polarized illumination, (d)  $\lambda = 1.09 \mu \text{m}$  y-polarized illumination, (e)  $\lambda = 1.59 \mu \text{m}$  x-polarized illumination.

selected feature we gain more information about the gates. For example, we note that the first selected feature in Fig. 4.5(a) is able to discriminate the XOR/XNOR pair from the rest of the gates, however the likelihoods of the remaining gates are similar to each other. This also confirms that we need more than one feature to reliably identify each gate. The second and third features in Fig. 4.5(b) and (c) are able to discriminate the XOR gate from the XNOR gate and OR gate from the NOR gate, respectively. Investigating the fourth and fifth features in Fig. 4.5(d) and (e), we observe that while they still provide information about the gate types, the likelihoods of each gates are closer to each other compared to the first three features. This explains our observation on the drop in the rate of increase in the classification accuracy with each added feature, which we will discuss next.

In Fig. 4.7(a) we present the mean accuracy and the standard deviation of the 10 cross-validation experiments as a function of number of features. We will refer to these accuracies as the training accuracies. We observe that selecting one feature results in approximately 48% accuracy and the accuracy increases with the increased number of features. With four features we can obtain an 82% accuracy, and increasing it to five features results in an 85% accuracy. This phenomenon of diminishing gains is similar to what we observed with the analytical accuracies in Fig. 4.3 and is the reason for selecting a total of five features for our framework.

In order to evaluate the performance of our classification framework and investigate how our method generalizes to an unseen set of data we perform classification on the test data with the selected features and present the outcome in Fig. 4.7(b), which we refer to as the test accuracy. We note that the test accuracies are very similar to training accuracies, however they are slightly lower overall. Using a single feature we can obtain a 42% and with 5 features we can achieve a 82% accuracy. This illustrates the robustness of our algorithm and confirms that our framework generalizes well to a new set of data. Furthermore, the slight decrease in the accuracies is expected as the features are selected to be the ones that perform the best on the same data (training set) for which the accuracies are measured on.

Next, we plot the confusion matrix for the test data in Fig. 4.8 to investigate the frequently misclassified gates. The diagonal cells in the confusion matrix show how many and what percentage of the examples (considering all gates) are classified correctly. The off-diagonal cells show the misclassified examples. For example, by looking at the diagonal cell for the AND gate we observe that 23 examples are classified correctly, corresponding to 19% of all 121 gates. Two of the examples for the AND gate



**Figure 4.7:** Classification accuracies as a function of number of features. (a) Training accuracies showing the mean and standard deviation for 10 cross-validations, (b) test accuracies.

are misclassified as OR, one as NAND and two as NOR gates. Overall, we can conclude that OR gate is usually misclassified as AND, NAND gate is usually misclassified as NOR and XOR gate is usually misclassified as XNOR gate. As mentioned earlier in this chapter, this is due to the similarity between the layouts of the three pairs.

In this section, we presented a framework for rapidly identifying different gate types which is useful for detecting hardware Trojans. The presented framework utilizes the physical model of the system to determine the most discriminative wavelength and polarization pairs to use, eliminating the need for implementing a complex experimental set-up for a large number of wavelengths. With the simulated data we can obtain a library of gate responses and build the histogram for the likelihoods to experimentally measure a chip and determine whether a gate has been replaced. We have shown that this system can achieve a 85% accuracy in identifying different gate types while being  $10^2-10^3$  times faster than imaging with a conventional high NA microscope.

While 85% accuracy is impressive for detecting hardware Trojans in a matter of few minutes, replacing a few gates among billions of gates is sufficient to alter the functionality of the chip. This suggests that higher accuracy classification methods



Figure 4.8: Confusion matrix illustrating the number of gates that are correctly and incorrectly classified.

may be necessary, which could be achieved by utilizing high NA imaging methods. We note that with the increased NA there will be a trade-off between the acquisition speed and the accuracy, however high NA imaging can be used to complement the low NA imaging method presented here such that only a few gates with low confidence values can be tested again with increased resolution. In the following section, we investigate a more advanced classification method with high resolution images to detect hardware Trojans.

# 4.2 Identification of gates with improved accuracy using high resolution imaging

In order to improve the accuracy of our previous set-up, we propose to use high NA imaging in conjunction with the low NA set-up as mentioned above. The set-up is the same as what we used in the previous section, however instead of obtaining

a single spatial reflectance measurement for each gate, we increase the NA of our system and obtain multiple spatial measurements for each gate with decreased step size as in a conventional confocal microscope. Furthermore, instead of taking multiple measurements per gate with different polarization and wavelength configurations, we propose to use a single wavelength and polarization for a simpler experimental set-up as we will obtain more information about the gate with the increased resolution and number of spatial measurements compared to the previous set-up. We use the first selected wavelength/polarization pair in the previous set-up at 1.22  $\mu$ m with x-polarized illumination as we expect it to be the most discriminative feature.

We use the same model as the one used in the previous section and use the high resolution images simulated with the same tiling procedure for our training and test data. For simplicity we use the high NA images simulated with the plane wave illumination instead of using confocal measurements. Note that the images scanned with a confocal microscope will be able to achieve a higher resolution, therefore the accuracies we will present serve as a conservative indicator of the accuracy of the confocal set-up.

Increasing the resolution of the system will result in a better classification performance, however we still want limit our NA to a moderate level for easier implementation such as by using a cSIL instead of an aSIL. For this purpose we use an NA of 2 as we empirically observed it to be capable of achieving high classification accuracies. Furthermore, for smaller technology nodes there is still possibility for increasing the NA to achieve a comparable performance. The image of the same tiling in Fig. 4.4 at an NA of 2 is illustrated in Fig. 4.9.

Compared to the previous framework, we are working with multiple spatial measurements at a single wavelength/polarization for each gate instead of a single spatial measurement with multiple wavelengths/polarizations. This results in a larger number



Figure 4.9: Example tiling of the gates. (a) layout of the 4x4 tiling, (b) Simulated 2 NA image of the layout for x-polarized illumination at  $\lambda = 1.22 \mu m$ . Scale bars in (a) and (b) correspond to 1  $\mu m$ .

of measurements with a stronger correlation between each measurement. Note that the conditionally independent measurements assumption we made in the previous analysis can be justified for detector noise across different wavelength and polarizations, however this may not be the case when there is cross-talk between the neighboring gates. Nevertheless, this assumption led to a more computationally efficient algorithm with high accuracy. To exploit the correlation between the spatial measurements, in this framework we propose to use more advanced feature extraction and statistical learning methods instead of the naive Bayes classifier.

In addition to exploiting the spatial nature of the measurements, we also want to explicitly account for the effects of cross-talk between the neighboring gates. In the previous method we were able to learn the effects of cross-talk for tiling patterns that are present in the training data through the likelihood estimation step, however due to the large number of possible gate configurations it is difficult to capture the effects of all possible tilings. Therefore, it is important to have a learning algorithm that can generalize to tilings not present in the training data. To accomplish this, we learn a sparse representation for the spatial measurements using dictionary learning.

#### 4.2.1 Dictionary learning

The goal of dictionary learning is to express a measurement  $\mathbf{M}$  of dimension n as a linear combination of small number of signals from a predetermined library, called the dictionary (Tošić and Frossard, 2011). Let us denote a dictionary of p elements as an  $n \times p$  matrix  $\mathbf{D}$  and its elements as unit-norm columns  $d_i$  of dimension n,  $i = 1, \ldots, p$ . With the dictionary elements, it is assumed that the measured signal  $\mathbf{M}$  can be expressed as

$$\mathbf{M} = \mathbf{D}\mathbf{a} + \epsilon = \sum_{i=1}^{p} a_i d_i + \epsilon, \qquad (4.4)$$

where  $\epsilon$  is observation noise and  $a_i$ 's are the sparse coefficients of the dictionary elements, meaning only a small number  $(k \ll p)$  of them are non-zero.

In the context of our framework, we argue that we can find such a sparse dictionary representation where a single gate with index s and its corresponding spatial measurements  $M^{(s)}$  can be expressed as  $M^{(s)} = \mathbf{Da}^{(s)} + \epsilon^{(s)}$ , where  $\epsilon^{(s)}$  represents detector noise that is statistically independent across measurements and gates. Note that the dictionary  $\mathbf{D}$  is shared across all gates. We further argue that some elements  $d_i$  of the dictionary will constitute the intrinsic signatures for the gates in the absence of noise (including cross-talk between the gates or the detector noise) and some will correspond to the effects due to the interference from the neighboring gates. The intrinsic signatures of the gates can be represented by a single dictionary element or a linear combination of multiple elements, which we will confirm empirically in the rest of this section. With this in mind, we expect that the learning method we use will be able to learn the dictionary indices corresponding to the intrinsic signatures and ignore the indices corresponding to interference, given the coefficients  $\mathbf{a}^{(s)}$  for each gate s. This is because the coefficients  $\mathbf{a}^{(s)}$  for gates s from the same class (gate type) are expected to have large components at these intrinsic indices. We note that the dictionary learning framework also has a de-noising property, since the detector noise is captured by the term  $\epsilon^{(s)}$ .

For learning the dictionary that will best represent our data we use the well known K-SVD algorithm (Aharon et al., 2006). Given a set of training data, K-SVD algorithm seeks the dictionary that leads to the best representation for each element in the training set under strict sparsity constraints. It is an iterative method that alternates between sparse coding of examples given a dictionary and an update step of the dictionary elements to better fit the data. For the sparse coding stage, given a dictionary it solves the optimization problem

$$\min_{\mathbf{a}^{(s)}} ||\mathbf{M}^{(s)} - \mathbf{D}\mathbf{a}^{(s)}||_2^2 \quad \text{subject to} \quad ||\mathbf{a}^{(s)}||_0 \le k$$
(4.5)

for each example s, where k is the sparsity parameter determining the maximum number of dictionary elements that represents a measurement. We use the nonnegative orthogonal matching pursuit (OMP) algorithm (Bruckstein et al., 2008) to solve this optimization problem in our framework, where we additionally have a non-negativity constraint on the coefficients due to the assumed additive nature of reflectance measurements. We choose k = 7 to incorporate the gate's intrinsic signature, contribution from the neighboring gates and additional variations that might be present in the image. Given the coefficients  $\mathbf{a}^{(s)}$  K-SVD algorithm then uses a singular value decomposition based update for updating the dictionary **D**. Similar to the sparse coding stage, we would like to constrain the dictionary elements to be non-negative, thus we use a non-negative variant of K-SVD for which the details can be found at (Aharon et al., 2005).

We now investigate empirically how well the dictionary learning framework is able to decompose the measurements. As we will discuss in more detail in the following sections, we split our data into 2/3 and 1/3 parts as training and test data respectively as we did in the previous set-up. Using the training set, we trained a dictionary using p = 25 dictionary elements, for which the distribution of the coefficients across the training set are illustrated in Fig. 4.10. First, we can observe the sparsity of the coefficients since most coefficients have a median value of zero for all classes. Secondly, we observe the concentration of coefficients on certain dictionary elements, which are in addition unique for each gate type. For instance, we can see that AND gates have a large coefficient corresponding to the second dictionary element, while the same is true for OR gates and the 19th dictionary element. We observe a similar pattern for other gate types. This separation of coefficients, as we expected, is promising since this implies a unique representation for each gate type which leads to easier classification.

Next, we look at some of the dominant dictionary elements for the gate types and compare with the measurements corresponding to that gate. Looking at the coefficient distribution for AND gates, we see that the dictionary element with index 2 appears frequently in the dictionary representations. Fig. 4·11 illustrates the dictionary element with index 2 along with three randomly selected sample images of AND gates. Similarly, for the NOR gates we plot the dictionary element corresponding to index 8 and three sample images in Fig. 4·12. In both cases, we see that just one dictionary element can represent the joint intrinsic signature of the samples from that gate type accurately. Note that the intensity of the dictionary elements are not directly related to the intensity of the measurements since the dictionary elements are multiplied by the corresponding coefficient in the dictionary decomposition. As another example, we plot the two dominant dictionary elements with indices 20 and 15 together with three sample images from the XOR class in Fig. 4·13. On the sample images, we see mostly three bright spots: on the top, middle-left and bottom-right of the image. Although the dictionary elements are similar, we see that the first one emphasizes the bright





spot on the bottom-right while the second one emphasizes the spot on the top. This implies that the two dictionary elements together can serve as a good representation for the intrinsic signature of XOR gates.



**Figure 4.11:** (a) Dictionary element with index 2, (b,c,d) randomly selected measurement images for AND gates, sharing the same colorbar. Each image corresponds to an area of 1400 nm  $\times$  760 nm.



**Figure 4.12:** (a) Dictionary element with index 8, (b,c,d) randomly selected measurement images for NOR gates, sharing the same colorbar. Each image corresponds to an area of 1400 nm  $\times$  760 nm.

Looking at Fig. 4.10, we can also note that some gate pairs have some amount of intersection between the coefficient distributions, such as the AND-OR pair. For instance gates from both classes may have large coefficients on indices 16, 21, 22 or 23. This is in line with our previous observations that these pairs have similar measurements and may be harder to distinguish between compared to other pairs.



Figure 4.13: (a,b) Dictionary element with indices 20 and 15, (c,d,e) randomly selected measurement images for XOR gates, sharing the same colorbar. Each image corresponds to an area of 1400 nm  $\times$  760 nm.

#### 4.2.2 Gate classification using dictionary coefficients

We now describe the classification procedure using the extracted dictionary coefficients and the training and testing set-up. For performing the classification, we use support vector machines (SVMs) (Cristianini and Shawe-Taylor, 2000) which are widely used for various machine learning tasks. The SVM algorithm aims to find a linear separator between data samples in two different classes such that the gap between the separator and the samples are maximal. It can also perform non-linear classification by implicitly mapping the data points to a higher dimension before finding a linear separator, using a kernel mapping. We use the radial basis function (RBF) kernel and the libsvm library for the SVM implementation (Chang and Lin, 2011) with C-SVC type SVM.

As in the previous set-up, we randomly divide our measurements in each class to 2/3 and 1/3 partitions for training and test data respectively. We then divide the training data further to 2/3 and 1/3 partitions for the cross-validation process, which we refer to as *cv-train* and *cv-test* respectively. To account for the detector noise, we add white Gaussian noise to the *cv-test* images with standard deviation  $\sigma = 0.01$ , which corresponds to the SNR that we considered in the previous setup. We perform training and testing over these partitions for different choices of p (number



**Figure 4.14:** Cross validation accuracies for different number of dictionary elements p.

of dictionary elements), C (cost parameter for C-SVC SVM) and  $\gamma$  (RBF kernel parameter). To accomplish this, we perform dictionary learning with p elements using the *cv-train* partition and estimate coefficients with the obtained dictionary for the *cv-test* partition using OMP. We then train an SVM with the *cv-train* partition and given parameters C,  $\gamma$  and obtain an accuracy with the *cv-test* partition. We repeat the cross-validation procedure 10 times with random *cv-train/cv-test* partitions for each parameter combination. We illustrate the cross-validation accuracies for different p in Fig. 4.14. To obtain these accuracies we choose the parameters C and  $\gamma$  that maximize average accuracy over 10 runs, separately for each choice of p. We observe that most parameter choices performed similarly well and the number of dictionary elements with highest mean at lower standard deviation is found to be p = 25.

Once we have obtained the parameters p, C and  $\gamma$  that maximize the average cross-validation accuracy, we perform training and testing using these parameters in order to estimate the performance of our system on previously unseen data. To accomplish this, we use the original partitioning to training (consisting of *cv-train* and *cv-test*) and test data, with white Gaussian noise of  $\sigma = 0.01$  added to the images in the test partition as measurement noise. The training step involves dictionary learning with chosen number of elements p and training an SVM using the dictionary coefficients with the chosen C and  $\gamma$ , with the training partition. We then use OMP to obtain the coefficients for the test partition corresponding to the learned dictionary and evaluate the accuracy of the SVM by testing using the dictionary coefficients of the testing data.

The distribution of the dictionary coefficients for the training partition are given in Fig. 4.10 in the previous section. The distribution of the dictionary coefficients for the test partition are illustrated similarly in Fig. 4.15. We observe similar distributions with the training set, with similar coefficients being dominant for the corresponding classes.

The final accuracy we obtain with the test data is 96.77%, for which the confusion matrix is illustrated in Fig. 4.16. We observe that the erroneous samples are a few OR and NAND gates that are classified as AND gates. Again, this is similar behavior to what we observed in the previous section, where AND and OR gates were harder to distinguish.

In this section we proposed a gate classification framework using higher resolution imaging and multiple spatial measurements on a single wavelength for each gate. We have shown that it is possible to improve identification accuracy to about 97% from about 85% in the previous framework, using a robust dictionary representation and support vector machines for classification. While this set-up requires more measurements thus is slower in practice compared to the previous set-up, it can be used as a second stage analysis for parts of the circuitry for which the former analysis returns predictions with low confidence. We also note that while we used an NA of 2 in this analysis, it is possible to use higher NA values to either improve accuracy to higher than 96%, or to extend the framework to smaller process nodes and maintain similar accuracy.



**Figure 4.15:** Box plots for dictionary coefficients corresponding to each dictionary element estimated using OMP, for different gate classes in the test set with 29 AND, 27 OR, 27 NAND, 25 NOR, 8 XOR and 8 XNOR gates.

## 4.3 Conclusions

In this chapter, we first demonstrated the use of a multi-spectral imaging approach with a SIL microscope for rapid identification of gates in a chip. With the advances


Figure 4.16: Confusion matrix illustrating the number of gates that are correctly and incorrectly classified.

in IC technology, the traditional high NA imaging methods that are mainly used for fault analysis are becoming limited in resolving the small structures present in a gate. Instead of resolving these small structures, the multi-spectral approach aims at capturing the signature of each gate type at a considerably low NA of 0.8 to distinguish between each gate type in a matter of few minutes. It benefits from the model of the system to determine which features provide the most unique signature for different gate types. Without the model, it would be necessary to experimentally acquire the signatures for the gates at a large number of different wavelengths, which requires either a spectrometer or many different lasers. With the model, we can pre-determine a small number of wavelengths for sufficient accuracy and eliminate the need for experimental measurements at most wavelengths.

In the second part of this chapter, we demonstrated the use of higher NA imaging to achieve an increased accuracy. This method requires a denser spatial sampling of the chip and hence has a slower acquisition speed, however the dense sampling at higher NAs allow us to achieve a higher accuracy while still not necessitating resolving individual structures. We propose this method to be used in conjunction with the multi-spectral imaging at low NAs, specifically in the instances where the first method returns lower confidence values. With the combination of two methods, we showed that accuracies above 96% are possible for identification of different gate types.

We note that the accuracy of this framework can be improved by further utilizing the layout of the chip. In this work we did not assume knowledge of the true identities of the gates from the layout when identifying different gate types, except for their center locations. To increase the detection accuracy, the prior information from the neighboring gates could be incorporated into likelihood calculations. Similarly, the prior probability distribution for gate types at each location can be modified to put a higher weight on the true gate type, assuming that the gate is not replaced with high probability. This would result in a better performance in the proposed Trojan detection application, where the aim is to confirm whether the true gate is present (or replaced) as opposed to the problem of gate identification without prior knowledge of the chip.

## Chapter 5

## Free-form lens illumination with extended light sources

In previous chapters we considered modeling and enhancement of imaging systems specifically for the application of IC imaging and showed that modeling and modelaware methods are useful in analyzing and improving the capabilities of imaging systems. In this chapter we consider a different problem domain for model-based enhancement in *non-imaging* optical systems and show that model-aware methods can similarly improve the performance. As an example of a non-imaging optical system, we focus on the problem of free-form lens design for forming prescribed illumination patterns on a projection surface, as introduced in Chapter 1.

Common methods for designing free-form lenses consider the input to be a point source (cf. Section 2.4), however achieving light sources with small effective sizes is impractical in compact and energy-efficient systems. While extended light sources such as LEDs are commonly utilized in such applications, using extended light sources with lenses designed for point sources leads to significant blurring in the resulting illumination pattern, as the design algorithms does not account for the rays originating from extended light sources. This effect is illustrated in Fig.  $5\cdot 1$ .

In this chapter, we develop a deconvolution-based framework to eliminate the blurring effects of extended light sources. Given a free-form lens designed for a point source, we first use the physical model of the lens and estimate spatially-varying blur kernels that capture the effects of an extended light source on the illumination pattern.



Figure  $5 \cdot 1$ : The direction of a ray from the point source in (a) compared o the direction of the rays with an LED in (b). Adapted from (Luo et al., 2010).

We then use a shift-variant deconvolution operation to deconvolve the target image with the obtained kernels and design a new lens for the deconvolved target image. We demonstrate that when the new lens is illuminated with an extended light source, the deconvolution operation cancels out the blurring and results in a sharper image closer to the original target pattern.

We use a specific notion of resolution as the performance criterion for this problem. While the resolution is defined as the measure of spread of a point source determined by the PSF in an imaging system, in this non-imaging application we consider the effective spread of the obtained illumination pattern compared to the original target due to the joint effect of the optimized lens and extended light source. Specifically, we estimate the line spread function (LSF) of the projected patterns from their edges and compute their FWHM as given by the Houston criterion.

## 5.1 Shift-variant deconvolution framework

In this section, we present the details of our shift-variant framework. Note that in scenarios where the light source and the projection screen is far away from the lens, the system can be approximated as a shift-invariant system (Ma et al., 2015; Kiser and Pauly, 2012). However, in compact and energy efficient systems the shift-variant nature of the system must be taken into account. This requires obtaining a separate blur kernel for each point on the lens and deconvolving the target image with the corresponding blur kernels, which is computationally inefficient. Instead, we assume that the blur kernel changes slowly between adjacent points on the lens and partition the lens into different sub-regions containing similar characteristics. We then estimate a single blur kernel for each sub-region, assuming that the system is shift-invariant inside these sub-regions and perform the deconvolution on the original target with the estimated blur kernels.

#### 5.1.1 Partitioning the lens

In order to partition the lens into sub-regions, we use the simple linear iterative clustering (SLIC) super-pixel algorithm (Achanta et al., 2012). This algorithm is originally used for partitioning images to spatially localized sub-regions that contain pixels with similar features, such as intensity or color values. It is an iterative algorithm that alternates between computing cluster means and assigning pixels to clusters with similar features determined by a distance metric. In this sense it is similar to the K-means clustering algorithm (Macqueen, 1967), however in the assignment step the search space is constrained to the pixels around the cluster means. In the image domain this allows the discovered partitions to be spatially localized.

In this work, we use the geometric properties of the lens as a feature to characterize sub-regions since we are working with lenses (which are characterized by their height maps) instead of intensity or color images. The curvature of the lens determines the angle that the light is refracted with respect to the optical axis, therefore the shape and size of the blur kernel depends on the curvature. This indicates that the sub-regions with similar curvatures will result in similar blur kernels. To use the curvature of the lens as a feature in the super-pixel algorithm, we represent each point on the lens by a positive semidefinite (PSD) matrix M formed by using the major and minor curvatures on each point. Specifically, we represent the directions of the curvatures as the eigenvector matrix and the rates of growth of an extended ray when passing through the lens along the optical axis as the eigenvalues of M. Given the curvature of the lens, the rates of growth  $r_{\text{max}}$ ,  $r_{\text{min}}$  are expressed as

$$r_{\max/\min} = 1 - (n-1)d_p \kappa_{\max/\min},$$
 (5.1)

where n is the refractive index of the lens,  $d_p$  is the distance of the lens to the projection plane and  $\kappa_{\max/\min}$  are the curvatures of the lens along the major and the minor axes respectively. With these parameters, the matrix M is then expressed as

$$M = \begin{bmatrix} | & | \\ v_{\max} v_{\min} \\ | & | \end{bmatrix} \begin{bmatrix} r_{\max} & 0 \\ 0 & r_{\min} \end{bmatrix} \begin{bmatrix} | & | \\ v_{\max} v_{\min} \\ | & | \end{bmatrix}^{T},$$
(5.2)

where  $v_{\text{max/min}}$  are the 2×1 column vectors denoting the directions of the curvatures of the major and minor axes and  $[\cdot]^T$  is the matrix transpose operator.

Once we form a PSD matrix for each point on the lens using the above formulation, we cluster them using the SLIC algorithm. Note that the algorithm works by calculating the distance between different features, as well as calculating the mean of given feature points. For calculating the distance between two PSD matrices  $M_1$  and  $M_2$  we utilize the distance metric proposed by (Förstner and Moonen, 2003)

$$d_m(M_1, M_2) = \sqrt{\sum_{i=1}^n \ln^2 \lambda_i(M_1, M_2)},$$
(5.3)

where  $\lambda_1(M_1, M_2), \ldots, \lambda_n(M_1, M_2)$  are the generalized eigenvalues of  $M_1$  and  $M_2$ . In addition, given a set of N PSD matrices, we calculate their mean using the gradient

descent algorithm (Pennec et al., 2006)

$$\bar{M}^{t+1} = \left(\bar{M}^t\right)^{\frac{1}{2}} \exp\left(\frac{1}{N} \sum_{i=1}^N \log\left(\left(\bar{M}^t\right)^{-\frac{1}{2}} M_i \left(\bar{M}^t\right)^{-\frac{1}{2}}\right)\right) \left(\bar{M}^t\right)^{\frac{1}{2}}, \quad (5.4)$$

where the mean matrix is initialized as the identity matrix. It is shown in (Pennec et al., 2006) that this algorithm typically converges in approximately 10 iterations, which is also the number of iterations we used in our experiments.

#### 5.1.2 Blur kernel estimation

Once the partitioning is done, the blur kernel corresponding to each partition is estimated for the central point of each sub-region. For each central point, placing a virtual pinhole on the lens and tracing the image of the LED on the projection surface would give us the blur kernel. However, to reduce the computational burden, for a square LED (which we consider in this work) we assume that the image of the LED will form a quadrilateral on the projection surface. With this assumption, we consider the rays originating from the four corners of the LED travelling to the central point of the partition and trace their projected locations on the projection surface for each sub-region using the thin lens approximation. We then estimate the blur kernel by fitting a quadrilateral with corners at the projected locations, assuming a homogeneous intensity distribution over the kernel as illustrated in Fig. 5.2 for a single point on the lens.

#### 5.1.3 Deconvolution

In order to deconvolve the target image with the estimated blur kernels, we assume that the target image is smooth and consider a regularized linear inverse problem using a weighted Tikhonov regularization (Tikhonov and Arsenin, 1977) on the gradient of



Figure 5.2: Blur kernel estimation for a single point on the lens.

the convolved image to enforce smoothness. We formulate the optimization problem

$$d^* = \underset{d \ge 0}{\arg\min} L(h * d, t) + \lambda \| W \circ \nabla(h * d) \|_2^2,$$
(5.5)

where d is the deconvolved target image, \* is the shift-variant convolution operator, h is the shift-variant blur operator, t is the target image and L(h \* d, t) is a data fidelity term measuring the similarity between the blurred underlying image and target image which we will define in detail later on.  $\lambda$  is the regularization parameter,  $\circ$  is the element-wise (Hadamard) product and  $\nabla$  is the gradient operator. W is the weighting term given by  $W_i = (1 - s_i)$  where s is the normalized and dilated edge field of the target image t, such that if the pixel i is close to the edge the weight becomes zero. This removes the regularization on pixels near the edges in the target image to ensure that the edges of the convolved image are not smoothed out.

To solve the above formulation, we derive the Richardson and Lucy (RL) algorithm (Richardson, 1972; Lucy, 1974) with the regularization on the convolved image. The RL method is an expectation maximization algorithm which computes the maximum likelihood estimate of the underlying image assuming Poisson statistics on the observation. Without the regularization term, the algorithm minimizes the negative log likelihood for a Poisson distributed observation (Dey et al., 2006)

$$L(d) \triangleq L(h * d, t) = \int_{x} \left[ (h * d)(x) - t(x) \cdot \log(h * d)(x) \right] dx, \tag{5.6}$$

which corresponds to the data fidelity term L(h \* d, t) in Eq. 5.5 and x is the spatial location parameter. We include the regularization term in Eq. 5.5 and express the final cost function as

$$L_2(d) = \int_x \left[ (h * d)(x) - t(x) \cdot \log(h * d)(x) \right] dx + \lambda \int_x |W(x)\nabla(h * d)(x)|^2 dx \quad (5.7)$$
$$\triangleq L(d) + \lambda L_{\text{Tik}}(d). \quad (5.8)$$

The optimum solution for this cost function can be obtained by setting the derivative of  $L_2$  to zero for all directions s, where the directional derivative is given by

$$\nabla_s L_2 = \lim_{\rho \to 0} \frac{L_2(d+\rho s) - L_2(d)}{\rho}.$$
(5.9)

The derivation of this algorithm for the unregularized case and for Tikhonov regularization on the underlying image is given in (Dey et al., 2006), therefore we only calculate the derivative of the regularization term  $J_{\text{Tik}}$ . A small perturbation  $\rho s$  on the regularization term changes the regularization cost to

$$L_{\text{Tik}}(d + \rho s) = \int |(W \circ \nabla (h * d + \rho h * s))(x)|^2 \, dx$$
(5.10)  
= 
$$\int \left[ |(W \circ \nabla (h * d))(x)|^2 + \rho^2 |(W \circ \nabla (h * s))(x)|^2 + 2\rho (W \circ \nabla (h * d))(x) (W \circ \nabla (s * h))(x) \right] \, dx.$$
(5.11)

For a small  $\rho$ , the perturbed cost function can be approximated as

$$L_{\text{Tik}}(d+\rho s) \approx L_{\text{Tik}}(d) + 2\rho \int (W \circ \nabla(h*d))(x)(W \circ \nabla(h*s))(x) \,\mathrm{d}x \qquad (5.12)$$

$$= L_{\text{Tik}}(d) + 2\rho \langle W \circ \nabla(h * d), W \circ \nabla(h * s) \rangle$$
(5.13)

$$= L_{\text{Tik}}(d) + 2\rho \langle \hat{h} * \hat{\nabla} W^2 \circ \nabla(h * d), s \rangle$$
(5.14)

$$= L_{\text{Tik}}(d) - 2\rho \langle \hat{h} * \operatorname{div} \left( W^2 \circ \nabla(h * d) \right), s \rangle, \qquad (5.15)$$

where  $(\hat{\cdot})$  denotes the adjacent operator,  $\hat{h}(x) = h(-x)$ ,  $\hat{\nabla} = -\text{div}$  and div is the divergence operator. From now on we will replace the term  $W^2$  with W for simplicity as in our formulation the weights are zero or one.

Combining the derivatives of the unregularized term from (Dey et al., 2006) and our regularization term and setting their sum to zero, we have the equality

$$\int_{x} \hat{h}(x) - \hat{h} * \frac{t}{h * d}(x) - 2\lambda \,\hat{h} * \operatorname{div}(W \circ (\nabla h * d))(x) \,\mathrm{d}x = 0.$$
(5.16)

Assuming that the blur kernels h are normalized to one, we have  $\int_x \hat{h}(x) dx = 1$ . Therefore, following the steps in (Dey et al., 2006) a multiplicative iterative algorithm to find d(x) satisfying Eq. 5.16 is found as

$$d^{(n+1)} = \frac{d^{(n)}}{1 - 2\lambda \left[\hat{h} * \operatorname{div} \left(W \circ (\nabla h * d^{(n)})\right)\right]} \circ \left(\hat{h} * \frac{t}{(h * d^{(n)})}\right),$$
(5.17)

where  $d^{(n)}$  is the estimated deconvolved target at the n<sup>th</sup> iteration.

Note that given a non-negative initial estimate, the unregularized RL algorithm  $(\lambda = 0)$  outputs non-negative estimates at each iteration. However, with the regularization the denominator could take zero or negative values, violating the non-negativity property of the algorithm. To avoid this, we use the stabilized version of the algorithm given in (Welk, 2016) referred to as regularized RL. For the shift-variant convolution

operation \* we use the overlap and add method as described in (Nagy and O'leary, 1997).

We note that the non-negativity constraint on the deconvolved target in Eq. 5.5 limits the performance of the deconvolution framework. More specifically, in signage applications where the target is generally a smooth and binary image and the blur kernels have homogeneous intensity distribution, the deconvolved target image produced by the algorithm will typically consist of a set of discrete points such that when convolved with the blur kernel, the resulting image will be a tiling of the blur kernels. This means that the performance of the deconvolution framework will depend on the shape and size of the target pattern relative to the shape and size of the blur kernel. With this tiling property of the framework in mind, the target patterns can be selected carefully to obtain a better performance. We will discuss this tiling property in further detail in the following sections.

### 5.2 Results and discussion

#### 5.2.1 Physical set-up and parameters

Throughout this section we use the following set-up and parameters unless otherwise stated. For a given target pattern, we consider a uniform light source collimated along the optical axis and optimize a lens for a given focal length with the algorithm described in Section 2.4. In order to simulate the image formed by the lens with an LED, we switch from the collimated set-up to the diverging set-up by using the thin lens equation

$$\frac{1}{f} = \frac{1}{d_s} + \frac{1}{d_p},$$
(5.18)

where f is the focal length of the lens,  $d_s$  is the distance of the light source to the lens and  $d_p$  is the distance of the projection surface to the lens. To optimize a lens, we use a focal length of 3 units where 1 unit is the height of the lens, spatially discretized to  $512 \times 512$  pixels. For the divergent set-up we consider  $d_s = 4$  units and  $d_p = 12$  units, and simulate the target image with a square Lambertian LED with a height of 0.1 units using the ray tracing software Persistence of Vision Raytracer (POVRay). The target patterns are 8-bit images with values ranging from 0 to 255.

Given the optimized height map of the lens for the original target image, to partition the lens into sub-regions we use the SLIC algorithm as described in Section 5.1.1 with modifications to the implementation of (Kovesi, ). We partition the lens into 64 sub-regions and set the compactness parameter in (Achanta et al., 2012) to zero to emphasize the similarity between two pixels as opposed to their spatial proximity to one another in the distance calculation. The SLIC algorithm does not enforce connectivity of super-pixels and to enforce this we relabel the disjoint superpixels and merge any sub-regions with area smaller than 4 pixels with their adjacent regions, following (Kovesi, ). With the obtained sub-regions on the lens, we calculate their corresponding regions on the projection screen to be used in the deconvolution algorithm.

Given the centers of each sub-region and the size of the LED, we calculate the blur kernel for each region as described in Section 5.1.2. We note that due to the scattering, first and higher order reflections on the lens or the imperfections on the surface of the lens (Kiser and Pauly, 2012) (which we do not account for) the size of the blur will be larger compared to our calculations. This would present a problem especially when the deconvolution algorithm results in a tiling of the blur kernel, as the tiles might overlap if the size of the estimated blur is smaller than the actual blur size. To account for these possible scenarios, we calibrate the size of the blur kernels empirically with the observed simulation results. For the signage application with the given parameters, on average the dimensions of the blur kernels are found to be approximately 40 pixels before magnification and as will be discussed in the next section, our simulations showed that dilating the blur kernel by 3 pixels to calibrate their dimensions to approximately 43 pixels gives the best performance.

Once the blur kernels are calculated for each sub-region on the target image, we use the regularized RL algorithm to solve Eq. 5.5 and perform deconvolution on the target image. We run the RL algorithm for 250 iterations with  $\lambda = 10$  and s as the binary edge field of the target image dilated by 2 pixels used to calculate the weights W = 1 - s.

#### 5.2.2 Experimental and simulation results

As discussed in Section 5.1.3, the performance of the deconvolution framework depends on the shape and size of the target pattern due to the tiling property of the algorithm. In order to best utilize this property we start with a target pattern of letter E in Fig.  $5\cdot3(a)$ , where we carefully pick the height and width of the pattern according to the size of the blur. We optimize a lens for the target image and illustrate the height map (overlaid with its contour plot) of the lens and the resulting blurry image when the lens is illuminated with an LED in Fig. 5.3. The colorbars next to the height-maps in Figs.  $5\cdot3(b)$  and  $5\cdot3(e)$  indicate the heights on the lenses in lens units.

With the height map of the lens for the original target (illustrated in Fig. 5·3(e)), we partition the lens into 64 sub-regions, calculate the blur kernel for each region and deconvolve the target image with the obtained blur kernels. Figures  $5\cdot4(a)$ ,(b) illustrate the partitions on the lens overlaid with the log-magnitude and orientations of the minimum and maximum curvatures. We observe that the SLIC algorithm is able to group regions with similar curvatures into the same partition, except for the regions at the boundaries of the lens. This is due to fact that the boundaries have small thickness and may be corrected by using a larger number of partitions or initializing the partitions more intelligently in the SLIC algorithm. The projection of these partitions on the projection plane overlaid with the target image is illustrated



Figure 5.3: Letter E pattern. (a) Original target pattern, (b) height map of the lens, (c) simulated LED image of the target on the projection surface, (d) deconvolved target pattern, (e) height map of the new lens, (f) simulated LED image of the new target. The contrast of the deconvolved target is enhanced to increase visibility.

in Fig. 5.4(c). We observe that these partitions clearly separate the dim and bright areas of the illumination pattern, which is expected as the blur kernels corresponding to these regions would be different.

The deconvolved target image is shown in Fig.  $5 \cdot 3(d)$ . It is important to note that since the original target image is a smooth binary image, the deconvolved target consists of delta functions which tiles the blur kernel when illuminated with an LED. As noted before, we picked the size of the original target pattern to make sure that the tiles fit inside the letter. When a new lens is obtained for the deconvolved target image, we simulate its image with an LED and obtain the sharper image on the projection screen, as illustrated in Fig.  $5 \cdot 3(f)$ .



**Figure 5.4:** Partitioning into sub-regions for the letter E pattern. Partitioning on the lens overlaid with the log-magnitude and orientation of (a) the major curvature, (b) the minor curvature. (c) Partitions as projected to the projection surface. Colors in (a,b) denote the logmagnitude of the curvatures and arrows indicate the orientation of the curvature axes. The blue grid denotes the boundaries of each partition.

In order to quantitatively evaluate the performance of our framework we use the FWHM of the line spread function (LSF) of the system. We obtain the LSF by taking a cross-section from an edge of the projected image and fitting a Gauss error function to it, which gives us the edge spread function (ESF) defined as the spread of an edge. Taking the derivative of the ESF results in the LSF of the system. The FWHM of the LSF is calculated to be 33 pixels and 14.5 pixels for the resulting images of the



**Figure 5.5:** Comparison of experimental and simulated data for the letter E pattern. (a) Original target pattern simulated with a point source, (b) deconvolved target pattern simulated with an LED, (c) photograph of the pattern created by the fabricated lens illuminated with an LED.

original and the deconvolved targets respectively, resulting in a 56% increase in the sharpness.

To demonstrate the effectiveness of our framework on experimental data, we fabricated the lens optimized for the deconvolved target image. Fig. 5.5(c) illustrates the projected image when the fabricated lens is illuminated with an LED, where the lens and the reflection of the light source on the lens are visible on the bottom right of the image. We compare it to the simulated projected patterns, when the original lens is illuminated with a point source in Fig. 5.5(a) and the new lens designed for the deconvolved target is illuminated with an LED in Fig. 5.5(b). We observe that the experimental performance matches our expectations set by the simulated projected pattern.

We have shown that this framework produces sharp images when the deconvolved target image is illuminated with an LED, for a carefully chosen target pattern. However, it is not possible to perfectly tile every target pattern. We illustrate this with a new target pattern of letter a in Fig. 5.6, which contains edges in different orientations and does not have constant width or length like the letter E. We use the same parameters



in the previous experiment for the simulations.

**Figure 5.6:** Letter a pattern. (a) Target pattern, (b) height map of the lens, (c) LED image of the target, (d) deconvolved target, (e) convolved image of the new target and the blur operator and (f) LED image of the new target. The contrast of the deconvolved target is enhanced to increase visibility.

Figure 5.6 illustrates the resulting height map of the lens and the projected image of the target illuminated with an LED. We then follow the same procedure as letter E to deconvolve the new target pattern, where we partition the lens into 64 sub-regions, estimate the blur kernel for each sub-region and deconvolve the target image with the estimated blur kernels to obtain a new target image. The partitions on the lens overlaid with the log-magnitude and directions of the minimum and maximum curvatures, and the projections of these partitions on the projection surface overlaid with the target pattern are illustrated in Fig. 5.7(c).

We note that the deconvolved target in Fig. 5.6(d) consists of stripes in addition to



**Figure 5.7:** Partitioning into sub-regions for the letter a pattern. Partitioning on the lens overlaid with the log-magnitude and orientation of (a) the major curvature, (b) the minor curvature. (c) Partitions as projected to the projection surface. Colors in (a,b) denote the logmagnitude of the curvatures and arrows indicate the orientation of the curvature axes. The blue grid denote the boundaries of each partition.

delta functions since it is not possible to perfectly tile the target image with the blur kernels. The resulting image when the deconvolved target image is illuminated with the LED is shown in Fig. 5.6(f). We observe gaps and overlaps around the regions where the blur kernels are not tiled perfectly due to the changing height and width of the letter. Even though the resulting image is not as uniform as it was in the letter E pattern, it is 58% sharper compared to the projected image of the original target, where the FWHM of the LSF is decreased from 31 pixels to 13 pixels.

So far we worked with a larger blur kernel where the size of the LED is 0.1 units. Since the size of the blur kernel is large, it is more difficult to tile the blur kernel and this results in the gaps and overlaps observed in Fig.  $5 \cdot 6(f)$ . If we use a smaller LED, tiling the blur kernel will be easier with deconvolution and the resulting image will be smoother when the deconvolved target image is illuminated with an LED. We illustrate this in Fig. 5.8, where we decrease the size of the LED to 0.05 units. We follow the same deconvolution procedure above with the same parameters and only change the parameter used in the calibration of the blur kernels. With the smaller LED, the calculated size of the blur is found to be 20 pixels and our simulations showed that dilating the blur kernels by 1 pixel gives the best result. After deconvolving the target image with the blur kernels and simulating the LED image of the deconvolved target, we observe that the resulting image with a smaller LED in Fig. 5.8(c) is smoother and more uniform compared to the result with larger LED in Fig.  $5\cdot 6(f)$ . With the new size for the LED, there is a 37.5% increase in the sharpness with the deconvolved target compared to the original target, where the FWHM of the LSF is decreased from 16 pixels to 10 pixels.



Figure 5.8: Deconvolution results. (a) Deconvolved target, (b) LED image of the original target for comparison, (c) LED image of the deconvolved target. The contrast of the deconvolved target is enhanced to increase visibility.

We next investigate the effect of the regularization parameter  $\lambda$  in Eq. 5.5 on the projected images. In Fig. 5.9 we illustrate the projected patterns for  $\lambda = 0$ (unregularized),  $\lambda = 10$  (what we used so far) and  $\lambda = 25$  for an LED size of 0.1 units. We observe that with regularization the interior of the patterns become slightly smoother compared to the unregularized case. Even though the difference between  $\lambda = 10$  and  $\lambda = 25$  is not significant, we observe that some edges such as the top right edge of the letter is slightly blurrier in the  $\lambda = 25$  case.



Figure 5.9: Effect of regularization parameter on the projected images. (a)  $\lambda = 0$ , (b)  $\lambda = 10$ , (c)  $\lambda = 25$ .

We remark that the performance of this framework is adversely affected when the estimated blur size does not match the size of the actual blur. This could happen due to the first or higher order reflections inside the lens or scattering of light due to the roughness of the fabricated lens surface. As mentioned in Section 5.2.2, when the algorithm chooses to tile the blur kernel the separation between two delta functions depends on the size of the blur kernel. Therefore, if the size of the blur kernel is not calculated correctly, it would result in gaps or overlaps in the final image. To illustrate this, we simulate a new target pattern of letter E in Fig. 5.10 with a different size than the previous example. We use the same parameters as our original example with the size of the blur kernels bur kernels and use the uncalibrated blur kernels with an average size of 40 pixels

instead. The size of the original target pattern is also selected accordingly to match the assumed size of the blur kernel. The height map and the LED image of this target is shown in Fig. 5.10.

Following the rest of the procedure, we deconvolve the target pattern with the estimated blur kernels and expect that the resulting image will be perfectly tiled when the deconvolved target is illuminated with an LED, since we assume that the size of the blur kernel is correct. However, since the size of the actual blur kernel is larger than the estimated blur kernel, the tiles in the final image overlap, yielding a non-uniform image on the projection screen as shown in Fig.  $5 \cdot 10(f)$ . This example demonstrates the need for calibrations on the size of the blur kernels.



Figure 5.10: Letter E, illustrating the overlapping of the tiles when the blur kernels are not calibrated. (a) Target image, (b) height map of the lens, (c) LED image of the target, (d) deconvolved target, (e) height map of the new lens, (f) LED image of the new target. The contrast of the deconvolved target is enhanced to increase visibility.

#### 5.2.3 Discussion

In our experiments we discussed the tiling property of our framework and its effect on the resulting patterns, and showed that the success of the deconvolution depends on the size and shape of the target pattern with respect to that of the blur kernels. Note that given any lens, the effect of the LED on the resulting pattern can be represented as a space-variant convolution h \* t of the blur kernels h with the original target pattern t. In this work we posed our framework as an optimization over the deconvolved target pattern d, given the blur kernels  $h_t$  that are derived from the lens designed for the original target pattern, that would result in the image  $h_t * d \approx t$ . When we design a new lens for the deconvolved target pattern d, the corresponding blur kernels  $h_d$  will have been changed from the kernels  $h_t$  considered in the optimization, leading to the pattern  $h_d * d$ . Thus, this suggests that a joint optimization over both the lens design and the deconvolved pattern should be performed, which is not trivial. We remark that our framework can be thought of as a one cycle of an alternating optimization framework for the two variables. While this procedure can be repeated multiple times, nevertheless we have shown that one cycle is successful in generating sharp images at the output.

It is noteworthy that even if we solve the joint optimization problem, due to the convolutional nature of this projection with the LED the resulting patterns will be a tiling or smearing of the blur kernels. Therefore, it might not be possible to generate arbitrary patterns and the nature of the blur kernel must be taken into account when designing target patterns. It is also noteworthy in this context that the literature on designing free-form lenses with extended light sources generally aim at generating uniform rectangular illumination patterns (Wester et al., 2014; Luo et al., 2010), whereas in this work we illustrated a method that is capable of generating regular and irregular shaped patterns with sharp edges.

## 5.3 Conclusions

In this chapter, we proposed a deconvolution-based framework to create sharp illumination patterns using free-form lenses with extended light sources. Our framework estimates the blur kernels on the lens due to the extended light source and deconvolves the target pattern using the estimated kernels. We demonstrated through both simulations and experiments that we can eliminate the blurring due to the extended light source and obtain a sharp image when the lens designed for the deconvolved target is illuminated with an extended light source for certain target patterns. We discussed the limitations of generating prescribed illumination patterns with extended light sources due to the convolutional nature of this problem.

# Chapter 6 Conclusion

## 6.1 Summary and Conclusions

In this dissertation we presented methods for modeling and model-aware enhancement of imaging and non-imaging optical systems. In particular, we considered three frameworks in the area of IC imaging and designing free-form lenses for illumination. For the IC imaging application, we derived an electromagnetic model for the aSIL microscope and proposed enhancement methods for fault analysis. Furthermore, we developed gate classification methods for reliably detecting hardware Trojans inserted in ICs. For the free-form lens design application, we developed a modelbased deconvolution method that is capable of creating sharp patterns under LED illumination, despite the blurring effects of the LED.

In Chapter 2, we provided background information and presented the related work on the applications areas we consider in this dissertation. We reviewed different resolution criteria which we used for evaluating the performance of different optical systems. We introduced SILs and their uses in backside imaging of ICs and presented the existing literature on modeling SIL microscopes. We then discussed the mechanisms for inserting hardware Trojans into ICs and reviewed the work on their detection techniques. Finally, we discussed the methods for designing free-form optical surfaces for illumination applications, and reviewed the algorithm we used for designing freeform lenses.

In Chapter 3, we derived the Green's function of the aSIL microscope for subsurface

imaging and analyzed the effects of forbidden light on the performance of the microscope for metal layers buried in the insulating dielectric medium. We concluded that the performance of the microscope deteriorates for higher level metal layers in bulk silicon chips. We then extended our Green's function formalism to model SOI chips and demonstrated that increased BOx thickness results in a decreased performance in terms of resolution and light collection efficiency. Next, using the derived Green's function we proposed an optimization framework for designing super-resolving pupil masks and discussed the trade-offs in designing such masks. Finally, we derived the full electromagnetic model of the aSIL microscope that models the image of an arbitrary structure. The developed model has been used by (Cilingiroglu et al., 2015) to increase the resolution of the aSIL microscope through post-processing techniques.

In Chapter 4, we developed two classification methods for identification of digital gate types to detect hardware Trojans. The first method is based on a multi-spectral imaging approach that represents the signature of each gate with a few reflectance measurements obtained for different wavelengths and polarizations at low resolution. We used a Bayesian classifier to identify different gate types. Since each gate is represented by a few measurements, this method can rapidly detect if a chip has been tampered within a matter of minutes. The second method trade-offs speed for accuracy and uses higher resolution images and utilizes advanced learning algorithms including dictionary learning and support vector machines. We propose the second method to complement the first one due to the its comparatively lower acquisition speed.

In Chapter 5, we considered the problem of free-form lens design for forming prescribed illumination patterns on a projection screen. We discussed the blurring effect stemming from using extended light sources with free-form lenses and developed a deconvolution-based method that eliminates the blur. We discussed the limitations of generating sharp illumination patterns with extended light sources and demonstrated the effectiveness of our framework on both simulated and experimental data for different target patterns.

### 6.2 Future directions

In this section we propose future directions for research. In Chapter 3, we discussed the modeling of aSIL microscopy and noted certain mismatches between the model and the experimental set-up. To improve the modeling accuracy, the air-gap between the immersion lens and the substrate of the chips can be incorporated into the model. Similarly, the thickness mismatch between the SIL and the substrate can be modeled as well, along with the refractive index mismatch between the two media in cases where the material of the SIL is different than the material of the substrate. Another possible direction could be the modeling the techniques for imaging active circuits such as laser voltage imaging (LVI), which is an optical fault analysis technique that images the active regions in ICs (Ng et al., 2010). Being able to model the electro-optic dynamics of active ICs could be useful in analyzing and improving the performance of these techniques.

For detecting hardware Trojans, the accuracy of the detection techniques can be further improved. For example, the layouts of the gates can be modified to enhance their spectral responses by engineering optical nano-antenna structures. These structures can be optimized such that the spectral signatures of the gates can be distinguished more easily and the sensitivity of the classification framework to measurement noise is decreased.

While it is not a contribution of this dissertation, we performed a preliminary analysis on integrating nano-antenna structures into different gate types, in collaboration with Dr. Ronen Adato. As explained in Chapter 4, considering that the spectral



Figure 6.1: Spectral response of (a) bare gates, (b) gates labeled with nano-antennas for x-polarized illumination. Near-field intensity distributions of (c) bare AND gate, (d) AND gate with a nanoantenna label (bottom) at  $\lambda = 1.25 \mu m$ . (e) Error rates as a function of noise level with and without the antenna labels. Adapted from (Adato et al., 2015)

responses of certain gate pairs (i.e. AND/OR, NAND/NOR, XOR/XNOR) are similar, we engineered nanorod antennas to increase the diversity of the spectral responses of these gate pairs (Adato et al., 2015). Figures 6·1(a) and 6·1(b) illustrate the spectral response of 6 bare basic gates (without the antenna labels) and the same gates with the antenna labels under x-polarized illumination. As can be seen from the figure, the spectral responses of aforementioned gate pairs are more distinguishable from each other with the help of the nano-antennas. Figures 6·1(c) and 6·1(d) illustrate the near field image of the bare AND gate and the AND gate with an antenna label at a wavelength of 1.25  $\mu$ m, where the nanorod antenna is placed at the bottom of the layout in Fig. 6·1(d).

Following the procedure in Section 4.1.2, we computed the Bayes error rates for classification under different noise levels, while selecting the most discriminative 4 wavelengths for both the bare gates and gates with antenna labels. The dashed black lines in Figs.  $6 \cdot 1(a)$  and  $6 \cdot 1(b)$  illustrate the selected wavelengths for each case. Figure  $6 \cdot 1(e)$  illustrates the Bayes error rates as a function of noise level for bare gates and gates with antenna labels. We observe that the error rate for gates with antenna

labels is smaller than the error rate for the bare gates at all noise levels. For example at a noise level of  $\sigma = 0.05$  the classification error is decreased from 20% to 10% with the antenna labels. This preliminary analysis shows that integrating nano-antenna structures to gates is promising for accurately identifying different gate types in an IC. It should be noted that the classification accuracy can be further increased by designing more complex antenna labels instead of single nanorod antennas.

For the free-form lens design problem, an immediate direction for improvement could be removing the thin-lens assumption in blur kernel calculation. While this assumption holds in cases where the focal length of the lens is large, this approximation may not be accurate for compact systems with small focal lengths. Thus removing this assumption could lead to a better performance. Another direction could be considering more energy efficient systems that utilizes LED collimators. In such systems the blur kernels could have different characteristics requiring more rigorous estimation techniques.

## References

- Abubakar, A. and van den Berg, P. M. (2004). Iterative forward and inverse algorithms based on domain integral equations for three-dimensional electric and magnetic objects. *Journal of Computational Physics*, 195(1):236–262.
- Achanta, R., Shaji, A., Smith, K., Lucchi, A., Fua, P., and Susstrunk, S. (2012). SLIC superpixels compared to state-of-the-art superpixel methods. *IEEE Transactions* on Pattern Analysis and Machine Intelligence, 34(11):2274–2282.
- Adato, R., Uyar, A., Zangeneh, M., Zhou, B., Joshi, A., Goldberg, B., and Unlu, M. (2016). Rapid mapping of digital integrated circuit logic gates via multi-spectral backside imaging. ArXiv e-prints.
- Adato, R., Uyar, A., Zangeneh, M., Zhou, B., Joshi, A., Goldberg, B., and Unlu, S. (2015). Integrated nanoantenna labels for rapid security testing of semiconductor circuits. In *Frontiers in Optics*, pages FTh1B–2. Optical Society of America.
- Aharon, M., Elad, M., and Bruckstein, A. (2006). K-SVD: An algorithm for designing overcomplete dictionaries for sparse representation. *IEEE Transactions on Signal Processing*, 54(11):4311–4322.
- Aharon, M., Elad, M., and Bruckstein, A. M. (2005). K-SVD and its non-negative variant for dictionary design. In *Optics & Photonics 2005*, pages 591411–591411. International Society for Optics and Photonics.
- Anson, O., Seron, F. J., and Gutierrez, D. (2008). NURBS-based inverse reflector design. In Congress Espanol de Informatica Grafica. The Eurographics Association.
- Banaee, M. G., Unlü, M. S., and Goldberg, B. B. (2014). Sub-λ/10 spot size in semiconductor solid immersion lens microscopy. Optics Communications, 315:108– 111.
- Banga, M. and Hsiao, M. S. (2008). A region based approach for the identification of hardware Trojans. In *IEEE International Workshop on Hardware-Oriented Security and Trust*, pages 40–47. IEEE.
- Barakat, R. (1965). Rayleigh wavefront criterion. Journal of the Optical Society of America, 55(5):572–573.

- Boyer, G. and Sechaud, M. (1973). Superresolution by Taylor filters. Applied Optics, 12(4):893–894.
- Brix, K., Hafizogullari, Y., and Platen, A. (2015). Solving the Monge–Ampère equations for the inverse reflector problem. *Mathematical Models and Methods in Applied Sciences*, 25(05):803–837.
- Brochu, E., Cora, V. M., and De Freitas, N. (2010). A tutorial on Bayesian optimization of expensive cost functions, with application to active user modeling and hierarchical reinforcement learning. arXiv preprint arXiv:1012.2599.
- Bruckstein, A. M., Elad, M., and Zibulevsky, M. (2008). Sparse non-negative solution of a linear system of equations is unique. In *International Symposium on Communications, Control and Signal Processing*, pages 762–767. IEEE.
- Cauchy, X. and Andrieu, F. (2010). Questions and answers on fully depleted SOI technology for next generation CMOS nodes. Report, SOI industry consortium.
- Chang, C.-C. and Lin, C.-J. (2011). LIBSVM: A library for support vector machines. *ACM Transactions on Intelligent Systems and Technology*, 2:27:1–27:27. Software available at http://www.csie.ntu.edu.tw/~cjlin/libsvm.
- Chartrand, R., Wohlberg, B., Vixie, K., and Bollt, E. (2009). A gradient descent solution to the Monge-Kantorovich problem. *Applied Mathematical Sciences*, 3(22):1071–1080.
- Chen, R., Agarwal, K., Sheppard, C. J., Phang, J. C., and Chen, X. (2013). A complete and computationally efficient numerical model of aplanatic solid immersion lens scanning microscope. *Optics Express*, 21(12):14316–14330.
- Chen, R., Agarwal, K., Zhong, Y., Sheppard, C. J., Phang, J. C., and Chen, X. (2012). Complete modeling of subsurface microscopy system based on aplanatic solid immersion lens. *Journal of the Optical Society of America A*, 29(11):2350–2359.
- Chew, W. C. (1995). Waves and Fields in Inhomogeneous Media, volume 522. IEEE Press New York.
- Cilingiroglu, B., Koklu, H., Ramsay, E., Lu, Y., Yurt, A., Karl, C., Konrad, J., Goldberg, B., and Unlu, S. (2012). Image reconstruction techniques for high numerical aperture integrated circuit imaging. In *Proceedings from the 38th International Symposium for Testing and Failure Analysis*. ASM International.
- Cilingiroglu, T. B. (2015). A Sparsity-Based Framework for Resolution Enhancement in Optical Fault Analysis of Integrated Circuits. PhD thesis, Boston University.

- Cilingiroglu, T. B., Uyar, A., Tuysuzoglu, A., Karl, W. C., Konrad, J., Goldberg, B. B., and Ünlü, M. S. (2015). Dictionary-based image reconstruction for superresolution in integrated circuit imaging. *Optics Express*, 23(11):15072–15087.
- Cristianini, N. and Shawe-Taylor, J. (2000). An Introduction to Support Vector Machines and Other Kernel-based Learning Methods. Cambridge University Press.
- Dey, N., Blanc-Feraud, L., Zimmer, C., Roux, P., Kam, Z., Olivo-Marin, J.-C., and Zerubia, J. (2006). Richardson–Lucy algorithm with total variation regularization for 3D confocal microscope deconvolution. *Microscopy Research and Technique*, 69(4):260–266.
- Di Francia, G. T. (1952). Super-gain antennas and optical resolving power. Il Nuovo Cimento (1943-1954), 9:426–438.
- Duda, R. O., Hart, P. E., and Stork, D. G. (2012). Pattern Classification. John Wiley & Sons.
- Feng, X., Glowinski, R., and Neilan, M. (2013). Recent developments in numerical methods for fully nonlinear second order partial differential equations. SIAM Review, 55(2):205–267.
- Finckh, M., Dammertz, H., and Lensch, H. P. (2010). Geometry construction from caustic images. In *European Conference on Computer Vision*, pages 464–477. Springer.
- Foreman, M. R. and Török, P. (2011). Computational methods in vectorial imaging. Journal of Modern Optics, 58(5-6):339–364.
- Förstner, W. and Moonen, B. (2003). A metric for covariance matrices. In Geodesy-The Challenge of the 3rd Millennium, pages 299–309. Springer.
- Fournier, F. R., Cassarly, W. J., and Rolland, J. P. (2009). Designing freeform reflectors for extended sources. In SPIE Optical Engineering Applications, pages 742302–742302. International Society for Optics and Photonics.
- Goh, S. H. and Sheppard, C. J. (2009). High aperture focusing through a spherical interface: Application to refractive solid immersion lens (RSIL) for subsurface imaging. *Optics Communications*, 282(5):1036–1041.
- Goos, F. and Hänchen, H. (1947). Ein neuer und fundamentaler versuch zur totalreflexion. Annalen der Physik, 436(7-8):333–346.
- Houston, W. V. (1927). A compound interferometer for fine structure work. *Physical Review*, 29(3):478.

- Hu, L., Chen, R., Agarwal, K., Sheppard, C. J., Phang, J. C., and Chen, X. (2011). Dyadic Green's function for aplanatic solid immersion lens based sub-surface microscopy. *Optics Express*, 19(20):19280–19295.
- Ippolito, S., Goldberg, B., and Unlü, M. (2005). Theoretical analysis of numerical aperture increasing lens microscopy. *Journal of Applied Physics*, 97(5):053105.
- Ippolito, S. B., Goldberg, B., and Unlü, M. (2001). High spatial resolution subsurface microscopy. Applied Physics Letters, 78(26):4071–4073.
- Jabbour, T. G. and Kuebler, S. M. (2008). Particle-swarm optimization of axially superresolving binary-phase diffractive optical elements. *Optics Letters*, 33(13):1533– 1535.
- Jacobsen, J. and Cassarly, W. (2016). Optical design: Software tools design freeform optics for illumination. *Laser Focus World*.
- Jha, S. and Jha, S. (2008). Randomization based probabilistic approach to detect Trojan circuits. In *IEEE High Assurance Systems Engineering Symposium*, pages 117–124. IEEE.
- Jin, Y. and Makris, Y. (2008). Hardware Trojan detection using path delay fingerprint. In *IEEE International Workshop on Hardware-Oriented Security and Trust*, pages 51–57. IEEE.
- Karrai, K., Lorenz, X., and Novotny, L. (2000). Enhanced reflectivity contrast in confocal solid immersion lens microscopy. *Applied Physics Letters*, 77(21):3459– 3461.
- Kindereit, U., Weger, A. J., Stellari, F., Song, P., Deslandes, H., Lundquist, T., and Sabbineni, P. (2012). Near-infrared photon emission spectroscopy of a 45 nm soi ring oscillator. In *IEEE International Reliability Physics Symposium*, pages 2D–2. IEEE.
- Kiser, T. and Pauly, M. (2012). Caustic art. Technical report, Ecole Polytechnique Federale de Laussane, EPFL.
- Kochengin, S. A. and Oliker, V. I. (1997). Determination of reflector surfaces from near-field scattering data. *Inverse Problems*, 13(2):363.
- Köklü, F. H. (2010). *High Numerical Aperture Subsurface Imaging*. PhD thesis, Boston University.
- Kovesi, P. D. MATLAB and Octave functions for computer vision and image processing. Available from: <a href="http://www.peterkovesi.com/matlabfns/>">http://www.peterkovesi.com/matlabfns/</a>.

- Kronfeld, M. and Zell, A. (2010). Gaussian process assisted particle swarm optimization. In *Learning and Intelligent Optimization*, pages 139–153. Springer.
- Leng, T. S. (2009). Near Infra-red Photon Emission Microscopy and Spectroscopy. PhD thesis, National University of Singapore.
- Li, J. and Lach, J. (2008). At-speed delay characterization for IC authentication and Trojan horse detection. In *IEEE International Workshop on Hardware-Oriented Security and Trust*, pages 8–14. IEEE.
- Lindberg, J. (2012). Mathematical concepts of optical superresolution. Journal of Optics, 14(8):083001.
- Lucy, L. B. (1974). An iterative technique for the rectification of observed distributions. *The Astronomical Journal*, 79:745.
- Lumerical Solutions Inc. Lumerical, FDTD solutions. https://www.lumerical. com/tcad-products/fdtd/. Accessed: 2016-03-31.
- Luo, Y., Feng, Z., Han, Y., and Li, H. (2010). Design of compact and smooth free-form optical system with uniform illuminance for led source. *Optics Express*, 18(9):9055–9063.
- Ma, D., Feng, Z., and Liang, R. (2015). Deconvolution method in designing freeform lens array for structured light illumination. *Applied Optics*, 54(5):1114–1117.
- Macqueen, J. (1967). Some methods for classification and analysis of multivariate observations. In Proceedings of the Fifth Berkeley Symposium on Mathematical Statistics and Probability, volume 1, pages 281–297. University of California Press.
- Mansfield, S. M. and Kino, G. (1990). Solid immersion microscope. Applied Physics Letters, 57(24):2615–2616.
- Miñano, J. C., Benítez, P., Lin, W., Infante, J., Muñoz, F., and Santamaría, A. (2009). An application of the sms method for imaging designs. *Optics Express*, 17(26):24036–24044.
- Miñano, J. C. and Gonzalez, J. C. (1992). New method of design of nonimaging concentrators. Applied Optics, 31(16):3051–3060.
- Mitra, S., Wong, H.-S. P., and Wong, S. (2015). Stopping hardware Trojans in their tracks. *IEEE Spectrum*.
- Moore, G. E. (1998). Cramming more components onto integrated circuits. *Proceed-ings of the IEEE*, 86(1):82–85.

- Nagy, J. G. and O'leary, D. P. (1997). Fast iterative image restoration with a spatially varying PSF. In *Optical Science, Engineering and Instrumentation*, pages 388–399. International Society for Optics and Photonics.
- Nangate Inc. Nangate freepdk45 open cell library. http://www.nangate.com/
  ?page\_id=2325. Accessed: 2016-03-30.
- Ng, Y. S., Lundquist, T., Skvortsov, D., Liao, J., Kasapi, S., and Marks, H. (2010). Laser voltage imaging: A new perspective of laser voltage probing. *Proceedings* from the 40th International Symposium for Testing and Failure Analysis, pages 5–13.
- Novotny, L. and Hecht, B. (2012). *Principles of Nano-Optics*. Cambridge University press.
- Nowroz, A. N., Hu, K., Koushanfar, F., and Reda, S. (2014). Novel techniques for high-sensitivity hardware Trojan detection using thermal and power maps. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, 33(12):1792–1805.
- Pennec, X., Fillard, P., and Ayache, N. (2006). A Riemannian framework for tensor computing. *International Journal of Computer Vision*, 66(1):41–66.
- Phang, J. C. H., Chan, D. S. H., Tan, S. L., Len, W. B., Yim, K. H., Koh, L. S., Chua, C. M., and Balk, L. J. (2005). A review of near infrared photon emission microscopy and spectroscopy. In *Proceedings of the 12th International Symposium* on the Physical and Failure Analysis of Integrated Circuits, pages 275–281.
- Potkonjak, M., Nahapetian, A., Nelson, M., and Massey, T. (2009). Hardware Trojan horse detection using gate-level characterization. In *Design Automation Conference*, pages 688–693. IEEE.
- Rad, R., Plusquellic, J., and Tehranipoor, M. (2008). Sensitivity analysis to hardware Trojans using power supply transient signals. In *IEEE International Workshop on Hardware-Oriented Security and Trust*, pages 3–7. IEEE.
- Rayleigh, L. (1879). Xxxi. investigations in optics, with special reference to the spectroscope. The London, Edinburgh, and Dublin Philosophical Magazine and Journal of Science, 8(49):261–274.
- Richardson, W. H. (1972). Bayesian-based iterative method of image restoration. Journal of the Optical Society of America, 62(1):55–59.
- Rostami, M., Koushanfar, F., and Karri, R. (2014). A primer on hardware security: Models, methods, and metrics. *Proceedings of the IEEE*, 102(8):1283–1295.

- Rutkauskas, M., Farrell, C., Dorrer, C., Marshall, K. L., Lundquist, T. R., Vedagarbha, P., and Reid, D. T. (2015). High-resolution subsurface microscopy of CMOS integrated circuits using radially polarized light. *Optics Letters*, 40(23):5502–5505.
- Schneider, J. B. Understanding the finite-difference time-domain method. http: //eecs.wsu.edu/~schneidj/ufdtd. Accessed: 2016-03-30.
- Schwierz, F. (2010). Graphene transistors. Nature Nanotechnology, 5(7):487–496.
- Serrels, K. A., Ramsay, E., Dalgarno, P. A., Gerardot, B., O'Connor, J., Hadfield, R. H., Warburton, R., and Reid, D. (2008). Solid immersion lens applications for nanophotonic devices. *Journal of Nanophotonics*, 2(1):021854–021854.
- Sparrow, C. M. (1916). On spectroscopic resolving power. The Astrophysical Journal, 44:76.
- Tehranipoor, M. and Koushanfar, F. (2010). A survey of hardware Trojan taxonomy and detection. *IEEE Design Test of Computers*, 27(1):10–25.
- Tikhonov, A. N. and Arsenin, V. Y. (1977). Solutions of Ill-posed Problems. W.H. Winston.
- Török, P. (2000). Propagation of electromagnetic dipole waves through dielectric interfaces. *Optics Letters*, 25(19):1463–1465.
- Török, P., Munro, P., and Kriezis, E. (2008). High numerical aperture vectorial imaging in coherent optical microscopes. *Optics Express*, 16(2):507–523.
- Tošić, I. and Frossard, P. (2011). Dictionary learning. IEEE Signal Processing Magazine, 28(2):27–38.
- Tumer, K. and Ghosh, J. (2003). Bayes error rate estimation using classifier ensembles. International Journal of Smart Engineering System Design, 5(2):95–109.
- Uyar, A., Yurt, A., Cilingiroglu, T. B., Goldberg, B. B., and Unlü, M. S. (2014a). Effect of forbidden light on subsurface IC imaging. In *Frontiers in Optics 2014*, page FTu1G.2. Optical Society of America.
- Uyar, A., Yurt, A., Cilingiroglu, T. B., Goldberg, B. B., and Unlü, M. S. (2014b). Imaging performance of aSIL microscopy on subsurface imaging of SOI chips. In Proceedings from the 40th International Symposium for Testing and Failure Analysis. ASM International.
- Vamivakas, A. N., Younger, R. D., Goldberg, B. B., Swan, A. K., Unlü, M. S., Behringer, E. R., and Ippolito, S. B. (2008). A case study for optics: the solid immersion microscope. *American Journal of Physics*, 76(8):758–768.

- Welk, M. (2016). A robust variational model for positive image deconvolution. Signal, Image and Video Processing, 10(2):369–378.
- Wester, R., Müller, G., Völl, A., Berens, M., Stollenwerk, J., and Loosen, P. (2014). Designing optical free-form surfaces for extended sources. *Optics Express*, 22(102):A552– A560.
- Wittmann, R. (2007). Miniaturization Problems in CMOS Technology: Investigation of Doping Profiles and Reliability. PhD thesis, Technische Universität Wien.
- Yee, K. (1966). Numerical solution of initial boundary value problems involving Maxwell's equations in isotropic media. *IEEE Transactions on Antennas and Propagation*, 14:302–307.
- Yurt, A. (2014). Subsurface Optical Microscopy of Semiconductor Integrated Circuits. PhD thesis, Boston University.
- Yurt, A., Grogan, M. D., Ramachandran, S., Goldberg, B. B., and Unlü, M. S. (2014a). Effect of vector asymmetry of radially polarized beams in solid immersion microscopy. *Optics Express*, 22(6):7320–7329.
- Yurt, A., Uyar, A., Cilingiroglu, T. B., Goldberg, B. B., and Unlü, M. S. (2014b). Evanescent waves in high numerical aperture aplanatic solid immersion microscopy: Effects of forbidden light on subsurface imaging. *Optics Express*, 22(7):7422–7433.
- Zienkiewicz, O. C. (1977). *The Finite Element Method*, volume 3. McGraw-Hill London.
## Aydan (Uyar) Aksoylar

8 Saint Mary's St.	phone: $+1$ (857) 234-0704
Boston, MA 02215	email: aydan@bu.edu

EDUCATION

2010-Present	Boston University, Boston, MA Ph.D. in Electrical Engineering Expected graduation: September 2016 Dissertation: Modeling and model-aware signal processing methods for enhancement of optical sys- tems Advisors: Prof. M. Selim Ünlü and Prof. Bennett B. Goldberg
2005–2010	<ul> <li>Sabanci University, Istanbul, Turkey</li> <li>B.S. in Electronics Engineering</li> <li>Minor Area: Mathematics</li> <li>Graduation Project: Body part based human tracking system</li> <li>GPA: 3.83 / 4.00</li> </ul>

## Work and Research Experience

#### 2012–PRESENT Optical Characterization and Nanophotonics Lab, Boston University, Boston, MA Research Assistant

- *Hardware Trojan Detection* Developing optical methods and machine learning algorithms for detecting malicious circuitry in integrated circuits.
- Electromagnetic Modeling of Aplanatic Solid Immersion Lens Microscope Performed electromagnetic modeling of an aplanatic solid immersion lens microscope for failure analysis of integrated circuits.
- Interferometric Imaging of Viruses Developed image reconstruction algorithms to enhance microscopic imaging of viruses.

May-Dec 2015	Mitsubishi Electric Research Labs (MERL), Cambridge, MA Research Intern
	• Computational Illumination with Free-form Lenses Developed image processing and reconstruction algo- rithms to improve the performance of free-form lenses which form a desired image on a projection screen. Designed a prototype of the set-up.
2010-2014	Electrical and Computer Engineering, Boston University, Boston, MA Graduate Teaching Assistant
	• Courses: Electric Circuit Theory I & II, Electromag- netic Theory I & II and Senior Design II
June–Sept 2009	Computer Vision for Human-Computer Interaction Research Group, Karlsruhe Institute of Technology, Karlsruhe, Germany Intern
	• Activity Recognition Using Space Time Interest Points Implemented computer vision and machine learning algorithms for activity recognition.

### PUBLICATIONS

- M. Brand, A. Aksoylar, "Sharp images from freeform optics and extended light sources," accepted to Frontiers in Optics, 2016.
- R. Adato, A. Uyar, M. Zangeneh, B. Zhou, A. Joshi, B. B. Goldberg, M. S. Ünlü, "Integrated nanoantenna labels for rapid security testing of semiconductor circuits," Frontiers in Optics, October 2015, San Jose, CA.
- T. B. Cilingiroglu, A. Uyar, A. Tuysuzoglu W. C. Karl, J. Konrad, B. B. Goldberg, M. S. Ünlü, "Dictionary-based image reconstruction for superresolution in integrated circuit imaging," Optics Express, 2015.
- B. Zhou, R. Adato, M. Zangeneh, T. Yang, A. Uyar, B. B. Goldberg, M. S. Ünlü, A. Joshi, "Detecting hardware Trojans using backside optical imaging of embedded watermarks," Design Automation Conference (DAC), June 2015, San Francisco, CA.

- T. B. Cilingiroglu, M. Zangeneh, A. Uyar, W. C. Karl, J. Konrad, A. Joshi, B. B. Goldberg, M. S. Ünlü, "Dictionary-based sparse representation for resolution improvement in laser voltage imaging of CMOS integrated circuits," Design, Automation and Test in Europe (DATE), March 2015, Grenoble, France.
- A. Uyar, A. Yurt, T. B. Cilingiroglu, B. B. Goldberg, M. S. Ünlü, "Imaging performance of aSIL microscopy on subsurface imaging of SOI chips," International Symposium for Testing and Failure Analysis (ISTFA), November 2014, Houston, TX. (Ranked among top 10 abstracts).
- A. Uyar, A. Yurt, T. B. Cilingiroglu, B. B. Goldberg, M. S. Ünlü, "*Effect of forbidden light on subsurface imaging*," Frontiers in Optics, October 2014, Tucson, AZ.
- A. Yurt<sup>†</sup>, A. Uyar<sup>†</sup>, T. B. Cilingiroglu, B. B. Goldberg, M. S. Ünlü, "Evanescent waves in high numerical aperture aplanatic solid immersion microscopy: Effects of forbidden light on subsurface imaging," Optics Express, 2014. (<sup>†</sup>equal contribution)

#### PATENT APPLICATIONS

• M. Brand, A. Aksoylar, "Freeform optics for extended light sources," U.S. Patent Application, filed May 16, 2016.

#### Selected Course Projects

- "Super-resolution through blur kernel estimation," Image reconstruction and restoration, Spring 2014
- "Object tracking using Ensemble tracking algorithm," Computer vision, Spring 2012
- "Example based image retrieval using region covariance descriptors," Digital image processing, Fall 2010

#### Scholarships and Awards

2013 DRS Technologies Student Infrared Imaging Competition Finalist with "Temperature profiling of high power laser diodes" project

2010-Present	Boston University Graduate Research Assistantship and Teaching Fellowship
Summer 2009	European Union Erasmus Internship Mobility Program Grant
2005 - 2010	Sabanci University Merit Scholarship.

# Skills

COMPUTER: MATLAB, Python, C/C++, OpenCV, Lumerical FDTD Solutions, POVRay,  ${\rm I\!AT}_{\rm E}\!X,$  Unix/Linux.