# Applications of Artificial Intelligence in Cybersecurity

**Instructor:**

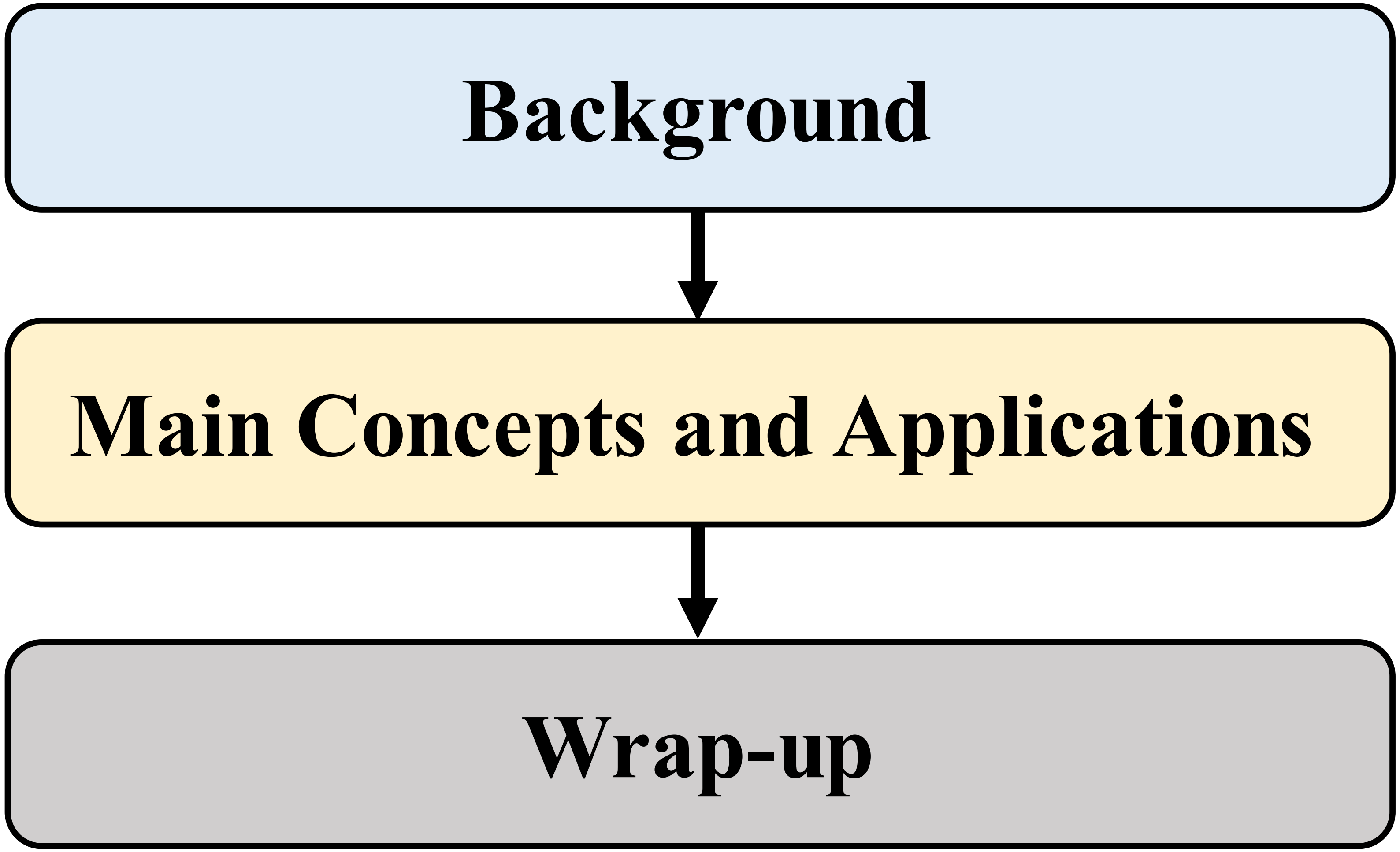
**Dr. Navid Asadi**

**Presenter:**

**Shayan (Sean) Taheri**

Florida Institute for Cybersecurity (FICS) Research
Electrical and Computer Engineering Department
University of Florida (UF)

# Lecture Plan

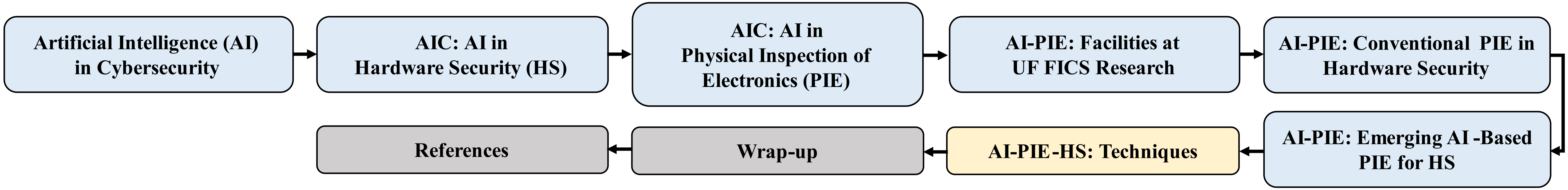


Background

Main Concepts and Applications

Wrap-up

# Details of Lecture Plan



Artificial Intelligence (AI) in Cybersecurity

AIC: AI in Hardware Security (HS)

AIC: AI in Physical Inspection of Electronics (PIE)

AI-PIE: Facilities at UF FICS Research

AI-PIE: Conventional PIE in Hardware Security

AI-PIE: Emerging AI -Based PIE for HS

AI-PIE-HS: Techniques

Wrap-up

References

Background ▪▪▪▪▪▪▪▪▪▪▪▪▪▪▪▪

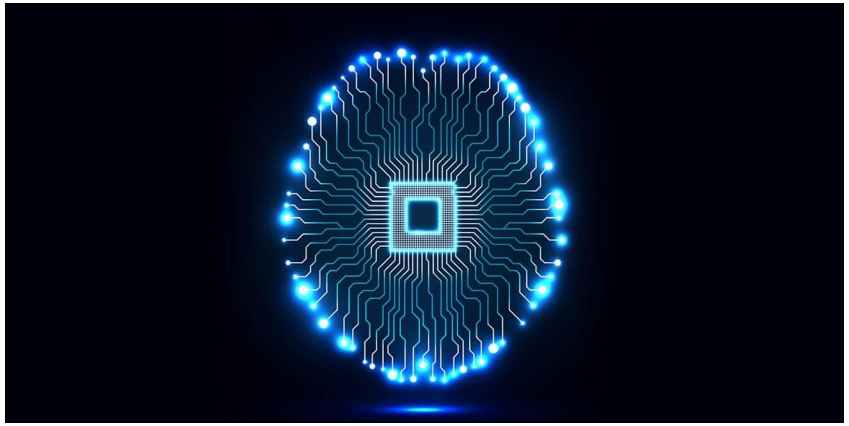
Main Concepts and Applications ▪▪▪▪▪▪▪▪▪▪▪▪▪▪▪▪

Wrap-up ▪▪▪▪▪▪▪▪▪▪▪▪▪▪▪▪

# Artificial Intelligence (AI) in Cybersecurity

- Typical use of AI in Cybersecurity (AIC) has consisted in applying certain AI tools to different **software** or **hardware** problems in Cybersecurity.
- The techniques for AIC may be initiated in this area or stem from other areas/applications and adapted for AIC based on the requirements.
- A branch of AI that has been connected with computer security (part of Cybersecurity) from relatively early days is automated reasoning, particularly as applied to programs and systems.
  - ✓ It was used in creating pattern matching tools that alert analysts to the security issues in their network.
  - ✓ The tools can outpace the ability of human analysts in responding.
  - ✓ More automation is needed in all aspects of Cybersecurity using AI technology.
- AI can reduce the execution time of attacks/defenses while increase their effectiveness and strengths.
  - ✓ The mechanism of attacks/defenses expand from intelligent agents acting humanly to thinking humanly.
- **What problems in Cybersecurity aspects of hardware can be resolved using AI technology?**

# AIC: AI in Hardware Security (HS)



- Hardware security remains an interesting area of study, given the importance of hardware in securing systems (for example, as the root of trust) along with securing the hardware platform itself.

- Research in hardware security spans many facets, including understanding and mitigating vulnerabilities in the integrated circuit (IC) supply chain; counteracting overbuilding, counterfeiting, or reverse-engineering effort; side-channel attacks; and Hardware Trojans.

- The goal is applying AI and machine/deep learning (DL) throughout electronic design, from the system-level, through logic-level design, physical design, and test and validation.

- As AI and DL continues to mature, their impact on various domains continues to grow, including hardware design and computing platforms applications.

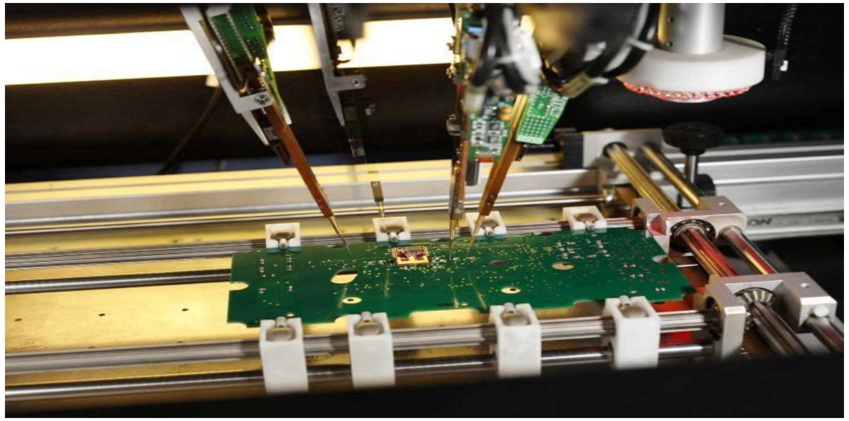
- Defenders can use AI and DL with hardware-based observations to build models of an IC's operation for attack detection (in terms of software, hardware, and environmental conditions).

- Attackers can use AI and DL to extract sensitive information from an IC, breaking trust assumptions in hardware security.

- **What problems in AI-based hardware security is in the interest of UF FICS Research and their ongoing projects?**

# AIC: AI in Physical Inspection of Electronics (PIE)

- The globalization of the semiconductor industry and outsourcing of Integrated Circuit (IC) fabrication to offshore foundries raises certain challenges for the electronics supply chain:
  - ✓ Prevalence of counterfeit electronics.
  - ✓ Ease of cloning and reverse engineering.
  - ✓ Insertion of hardware Trojans.
  - ✓ Development of advanced physical attacks.
  - ✓ Less known or unknown defects and failures.
  - ✓ Less efficiency and applicability of traditional testing methods.



- The physical inspection techniques:
  - ✓ Examine the IC package exterior and interior.
  - ✓ Range from simple visual inspection to high-tech imaging solutions.

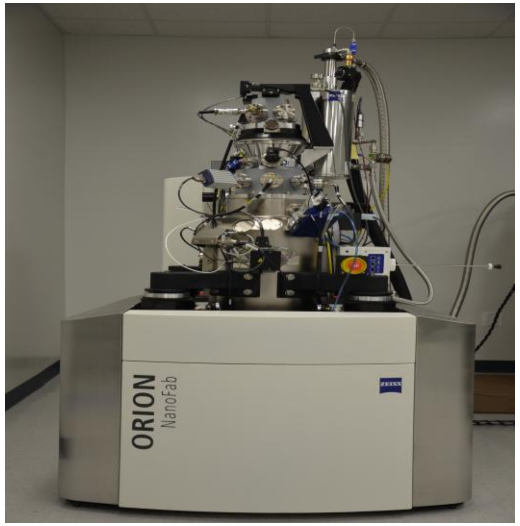
- How to do intelligent calibration of all the microscopy instruments in imaging electronics chips?

- How to make automating the inspection and defect/failure/infection detection process feasible using intelligent microscopy, image processing, computer visions, as well as deep learning algorithms?

- **How do we do physical inspection of electronic components and apply it into the area of hardware security? What facilities do we use? What AI techniques do we apply?**

# AI-PIE: Facilities at UF FICS Research

- **ORION NanoFab**
  - ✓ A multi-ion column system including Helium and Neon that provides a complete sub-10 nanometer nano-fabrication and sub-nanometer imaging solution for research in a wide range of applications.
  - ✓ Great imaging resolution with Helium ion is 0.5 nm, which is not achievable by regular Ga ion Focused Ion Beam (FIB) or scanning electron microscopy (SEM).
  - ✓ Including NanoPatterning and Visualization Engine (NVPE) – an integrated hardware and software control system.
  - ✓ NVPE incorporates a dedicated 16 bit scan generator for each NanoFab column and dual signal acquisition hardware supporting real-time advanced patterning and visualization.



- **PHEMOS-1000**
  - ✓ A high-resolution optical emission microscope in near infrared (NIR) spectrum that localizes failures in semiconductor devices by detecting the light emissions caused by semiconductor device defects.
  - ✓ Its laser scan system allows acquiring high-resolution pattern images.
  - ✓ Different types of detectors are available for various analysis techniques, such as photon emission analysis (PEM), electro-optical probing (EOP), and OBIRCH analysis.
  - ✓ Deployable for reverse-engineering of integrated circuits (ICs) from the backside of the package.

# AI-PIE: Conventional PIE in Hardware Security

- **Conventional PIE**: The examination and verification of various hardware information (e.g. their *physical patterns, connectivities,* and *functionalities*) from their SEM images.
  - ✓ Valuable for other applications such as intellectual property (IP) protection, competitive analysis, and etc.
  - ✓ Infeasible for manual analysis due to the large number of circuit elements involved.
  - ✓ The automated or semi-automated image analysis methods based on classical image processing techniques or conventional automation systems exist which can partially alleviate the burden of manual analysis.
  - ✓ *Challenges*:
    - Slow, inaccurate in the presence of noise, and incomplete.
    - Require large amount of human intervention.
    - The nature of images obtained from nanoscale ICs are inherently unique and challenging.
      - ❖ *Highly repetitive features*, *process variation effects*, and *the lack of adequate images from ICs with different technology nodes and vendors.*

  - ✓ **What is the solution for these challenges?**

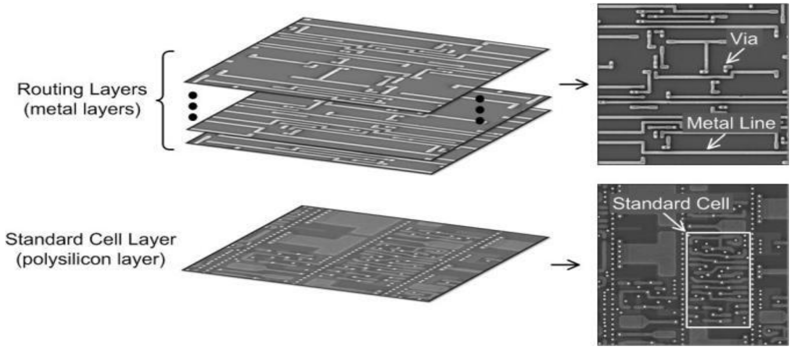
# AI-PIE: Emerging AI-Based PIE for HS

- **Novel AI-based PIE**
  - ✓ Emerging AI/DL-based image analysis framework for hardware assurance of ICs.
    - Examine and verify various hardware information from analyzing its SEM images.
    - Heavy use of AI/DL-based methods at all essential steps of the analysis.
    - Fundamentally new approaches and algorithms for detecting and analyzing complex SEM image features of ICs and make accurate decisions.
    - Reduce the inspection time of modern ICs down to only *few hours* from *months* and improve accuracy significantly.
    - Fast on parallel hardware, accurate against noises, and can automate tasks that were previously performed mainly manually.
    - Make the designs fully on-chip testable with engagement of deep learning methods.
    - Introducing computer vision models into the context of physical inspection of electronics.
    - Scan and authenticate the entire IC with a superlative system performance.
    - Recognition of cells within an IC design (i.e. **genuine**, **defective**, and **malicious**) intelligently and efficiently.
    - Detection of hardware Trojans with high confidence.
    - Incorporate different technologies into this context, such as *grid-type region-based computing, in-memory computing, adversarial learning, transfer learning, reinforcement learning, and hardware accelerators*.

- **What are the state-of-the-art techniques in the AI-based PIE for HS?**

# AI-PIE-HS: Technique [1] - A

- **Here, there is a DL-based image analysis system for hardware assurance of digital ICs based on stack of information and attributes extracted from IC layout.**
- **Examine and verify various hardware information from analyzing the SEM images of an IC.**
- **Reduction in time, more acceleration in model retraining, and improvement in system accuracy.**
- **It demonstrates the effectiveness of using synthetic data to train a model.**
- Stitch the images using classical phase correlation method for **creating high-resolution** images.
  - ✓ Checking the stitching results using a DL-based method.
  - ✓ A *DL-based object detection model* to detect any *misalignment as a result of noise* induced improper stitching.
  - ✓ Any *unwanted misalignment* may lead to errors in the subsequent analysis steps.


Routing Layers (metal layers)
Via
Metal Line
Standard Cell Layer (polysilicon layer)
Standard Cell

**An illustration of the many layers in a digital IC relevant to hardware assurance (left): metal layers for routing and polysilicon layer with standard cells, and their respective sample SEM images (right).**

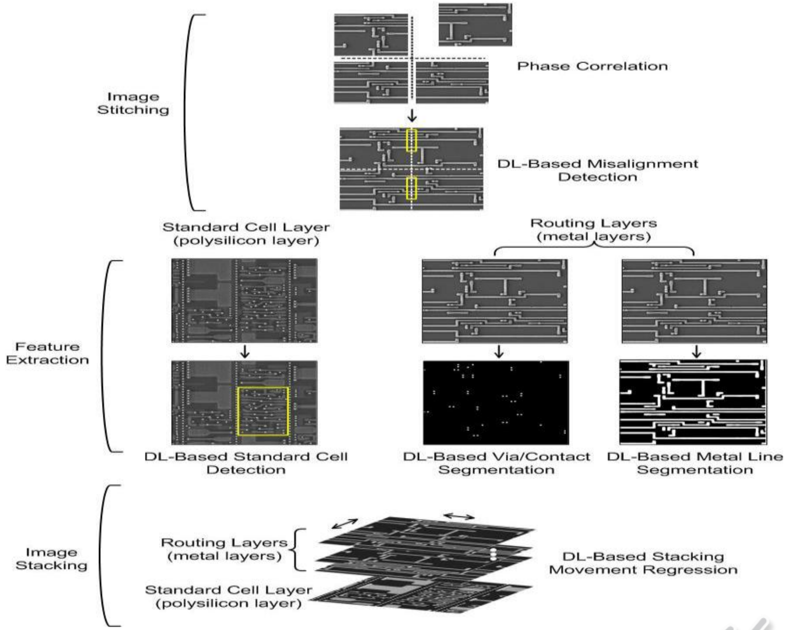


Image Stitching
Phase Correlation
DL-Based Misalignment Detection
Standard Cell Layer (polysilicon layer)
Routing Layers (metal layers)
Feature Extraction
DL-Based Standard Cell Detection
DL-Based Via/Contact Segmentation
DL-Based Metal Line Segmentation
Image Stacking
Routing Layers (metal layers)
Standard Cell Layer (polysilicon layer)
DL-Based Stacking Movement Regression

**Our proposed DL-based image analysis framework for hardware assurance of digital ICs.**

# AI-PIE-HS: Technique [1] - B

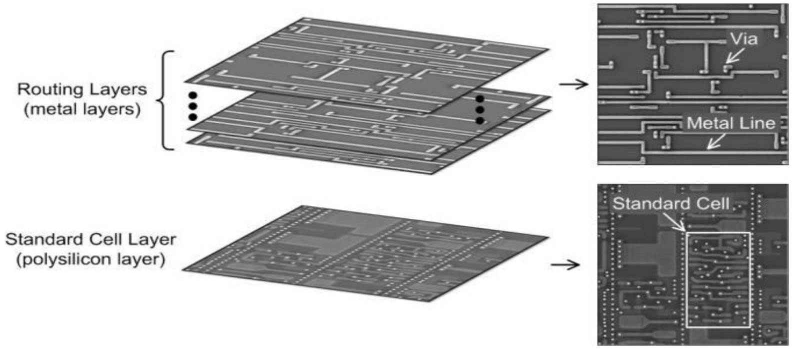
- To detect misalignment, implementing a reported Faster Region-Based Convolutional Neural Networks (R-CNN) object detection model with ResNet-50 backbone.

- Developing a fully automated training data preparation method for detecting misalignment, where randomly cropping image patches from a SEM image, and then cutting and shifting part of the image patch to create synthetic misalignments for training.
  - ✓ Generate large amount of training data in a short time.

- The misalignment detection model may need to be re-trained on a new set of SEM images if they appear different due to difference in technology, sample preparation method, or imaging process.

- Perform feature extraction using entirely DL-based methods.

- Using a DL-based object detection model to detect standard cells from the polysilicon layer and DL-based semantic segmentation models to segment vias and metal lines from the metal layers.


Routing Layers (metal layers)
Via
Metal Line
Standard Cell Layer (polysilicon layer)
Standard Cell

**An illustration of the many layers in a digital IC relevant to hardware assurance (left): metal layers for routing and polysilicon layer with standard cells, and their respective sample SEM images (right).**

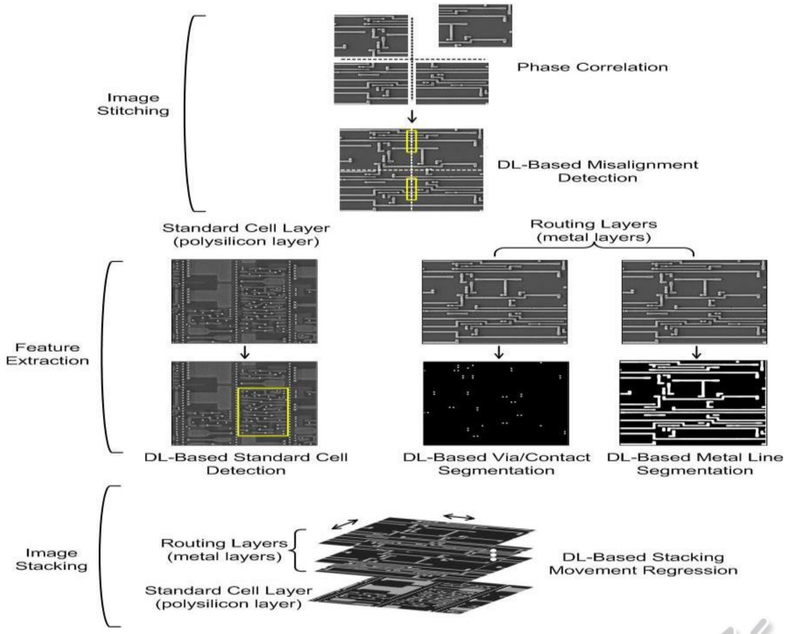


Image Stitching
Phase Correlation
DL-Based Misalignment Detection
Standard Cell Layer (polysilicon layer)
Routing Layers (metal layers)
Feature Extraction
DL-Based Standard Cell Detection
DL-Based Via/Contact Segmentation
DL-Based Metal Line Segmentation
Image Stacking
Routing Layers (metal layers)
Standard Cell Layer (polysilicon layer)
DL-Based Stacking Movement Regression

**Our proposed DL-based image analysis framework for hardware assurance of digital ICs.**

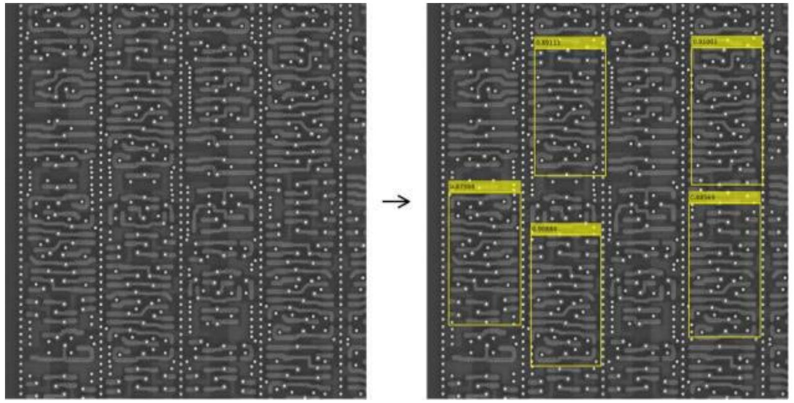
# AI-PIE-HS : Technique [1] - C

- The contacts from the polysilicon layer may also need to be segmented for the subsequent image stacking step and can be implemented using the same segmentation model as for via segmentation.

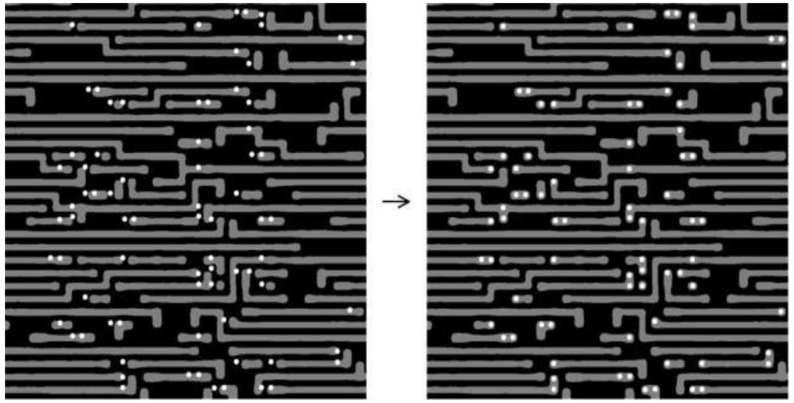
- Implement the same reported Faster R-CNN model with ResNet-50 backbone as the one used earlier for misalignment detection to detect standard cells.

- Randomly crop image patches from a SEM image, and then select and paste standard cells onto the image patch to create synthetic data for training.

- To segment vias and metal lines, implementing two reported Fully Connected Network (FCN) models with VGG-16 backbone.



**Sample DL-based standard cell detection result: multiple instances of a standard cell (in this case, a flip-flop) in the input image (left) were correctly identified by our DL model and annotated with yellow bounding boxes (right)**



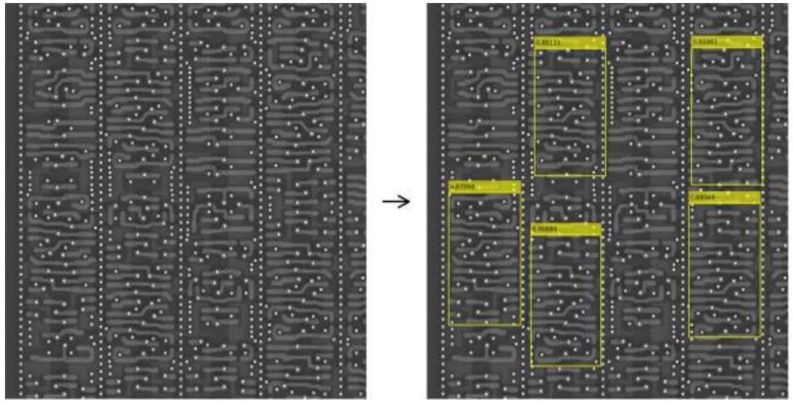
**Sample DL-based stacking movement regression result: stacking movements (in terms of horizontal and vertical movements) in the input image (left) were correctly estimated by our DL model and after stacking movements all vias from the lower layer were aligned properly with the metal lines from the upper layer (right)**

# AI-PIE-HS : Technique [1] - D

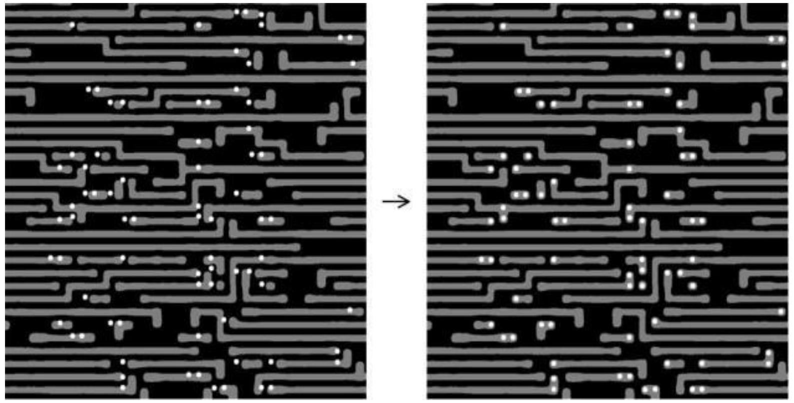
- Develop a semi-automated method in preparing the training data for segmenting vias and metal lines, where we first employ classical image processing methods to segment vias and metal lines and correct any resulting errors manually.
  - ✓ Use this data as the training data to train our models.
  - ✓ This semi-automated training data preparation method greatly reduces the manual effort required in preparing the ground truth of training data.

- Scale and stack the feature images extracted from each layer together.
  - ✓ Perform local stacking movement using a DL-based method.

- A DL-based regression model using VGG-16 backbone to estimate the necessary stacking movements from the stacked feature images and move the layers accordingly to align all the connection points.



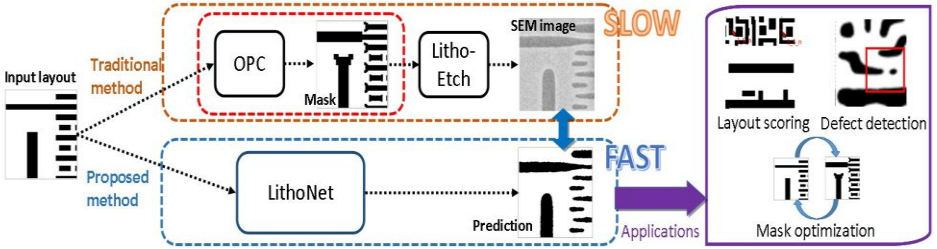
**Sample DL-based standard cell detection result: multiple instances of a standard cell (in this case, a flip-flop) in the input image (left) were correctly identified by our DL model and annotated with yellow bounding boxes (right)**



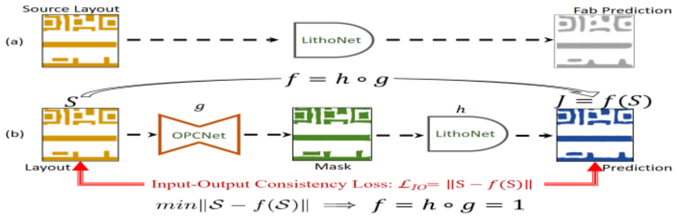
**Sample DL-based stacking movement regression result: stacking movements (in terms of horizontal and vertical movements) in the input image (left) were correctly estimated by our DL model and after stacking movements all vias from the lower layer were aligned properly with the metal lines from the upper layer (right)**

# AI-PIE-HS : Technique [2] - A

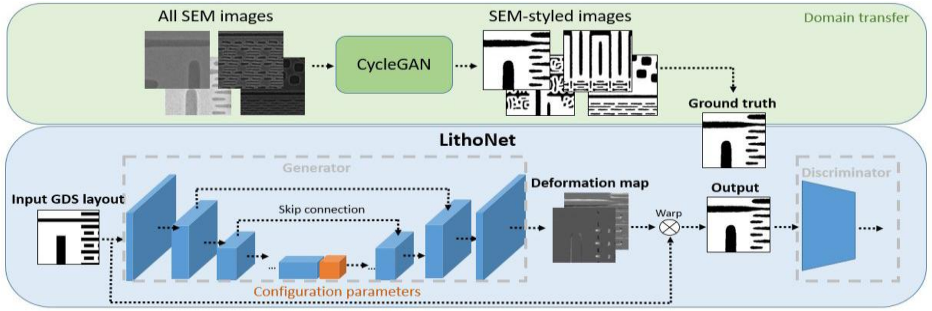
- The shape deformations on a fabricated IC due to the imperfect lithography and etch processes often cause IC defects (e.g., thin wires or broken wires).
- Developing a pre-simulation tool to compensate for the shape distortions caused by the lithography and etch processes.
- A deep learning-based data-driven framework consisting of two convolutional neural networks:
  - i. LithoNet
    - ✓ Learns the shape correspondence between paired training images, IC layout designs and their fabricated IC SEM images.
    - ✓ Predicts the shape deformations/distortions/alterations on a circuit layout due to IC fabrication.
    - ✓ Generates a simulation result for fabricated design.
  - ii. OPCNet
    - ✓ Learns a mask optimization model without ground-truth OPC-based corrected masks based on an input-output consistency loss model.



Relationship among optical proximity correction (OPC) simulation, circuit verification on an SEM image, and the method. The OPC step, highlighted by the red dashed lines, suggests modifications of a layout mask so that the fabricated IC could have nearly the same shape as the original layout pattern. The proposed LithoNet and its applications are highlighted by purple contours.


Source Layout
(a)
LithoNet
Fab Prediction
$f = h \circ g$
$S$
$J = f(S)$
(b)
$g$
OPCNet
$h$
LithoNet
Layout
Mask
Prediction
Input-Output Consistency Loss: $\mathcal{L}_{IO} = \|S - f(S)\|$
$min\|\mathcal{S} - f(\mathcal{S})\| \implies f = h \circ g = 1$

Two scenarios utilizing the proposed LithoNet and OPCNet: (a) A stand-alone LithoNet, and (b) A cascaded LithoNet-OPCNet network.



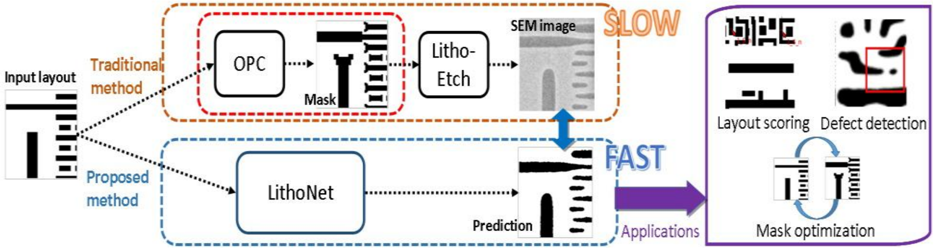
LithoNet Framework: Block diagram of the proposed two-step framework for cross-domain image to-image translation. The upper step adopts CycleGAN to transfer the training SEM images to obtain ground-truth labels. LithoNet then estimates the deformation maps between input layout patterns and their corresponding labels.

# AI-PIE-HS : Technique [2] - B

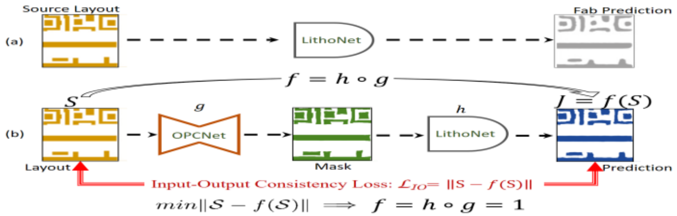
- A deep learning-based data-driven framework consisting of two convolutional neural networks:
  i. OPCNet
    - ✓ Predicts the masks whose lithography simulation images can be matched with the expected layout.
    - ✓ Suggests IC layout corrections to compensate for such shape deformations.

- The LithoNet-OPCNet framework can not only predict the shape of a fabricated IC from its layout pattern, but also suggests a layout correction according to the consistency between the predicted shape and the given layout.

- LithoNet Description
  - ✓ It is a CNN-based lithography simulator.
  - ✓ Takes the wafer fabrication parameters as a latent vector to model the parametric product variations that can be inspected on SEM images.
  - ✓ Consists of a Cycle GAN-based domain transfer network and a deformation prediction network.

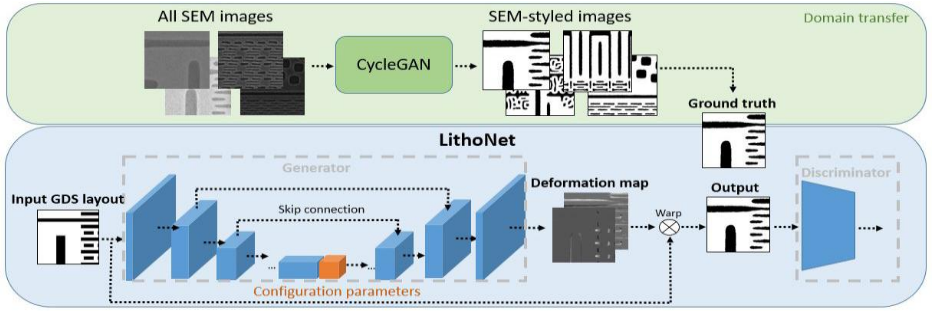


Relationship among optical proximity correction (OPC) simulation, circuit verification on an SEM image, and the method. The OPC step, highlighted by the red dashed lines, suggests modifications of a layout mask so that the fabricated IC could have nearly the same shape as the original layout pattern. The proposed LithoNet and its applications are highlighted by purple contours.



Source Layout
(a)
LithoNet
Fab Prediction
$f = h \circ g$
$S$
$J = f(S)$
(b)
$g$
OPCNet
$h$
LithoNet
Layout
Mask
Prediction
Input-Output Consistency Loss: $\mathcal{L}_{IO} = \|S - f(S)\|$
$min\|\mathcal{S} - f(\mathcal{S})\| \implies f = h \circ g = 1$

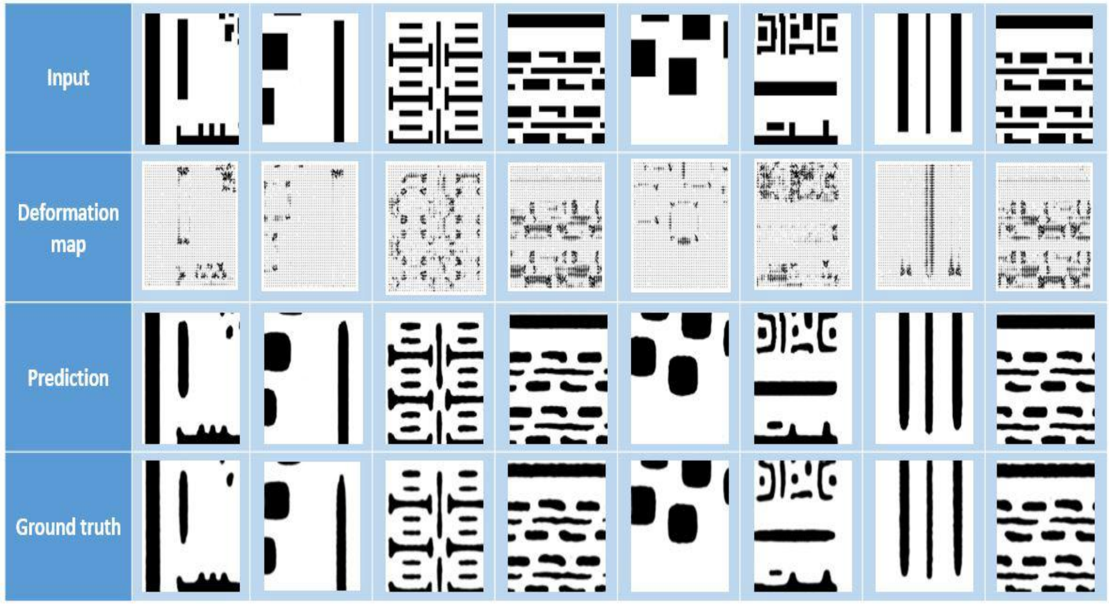
Two scenarios utilizing the proposed LithoNet and OPCNet: (a) A stand-alone LithoNet, and (b) A cascaded LithoNet-OPCNet network.



LithoNet Framework: Block diagram of the proposed two-step framework for cross-domain image to-image translation. The upper step adopts CycleGAN to transfer the training SEM images to obtain ground-truth labels. LithoNet then estimates the deformation maps between input layout patterns and their corresponding labels.

# AI-PIE-HS : Technique [2] - C

- **LithoNet** Description
  - ✓ Designed to learn how an IC fabrication process deforms the shape contours of a layout pattern.
  - ✓ Learns the shape correspondences between pairs of layout design patterns and their SEM images of the product wafer.
  - ✓ Simulates the fabrication process to predict the shape deformation for further virtual metrology applications based on:
    1. A given layout.
    2. A set of fabrication parameters.
  - ✓ Predicts the contour shapes by learning the pixel-wise shape correspondence between every paired layout and SEM images.



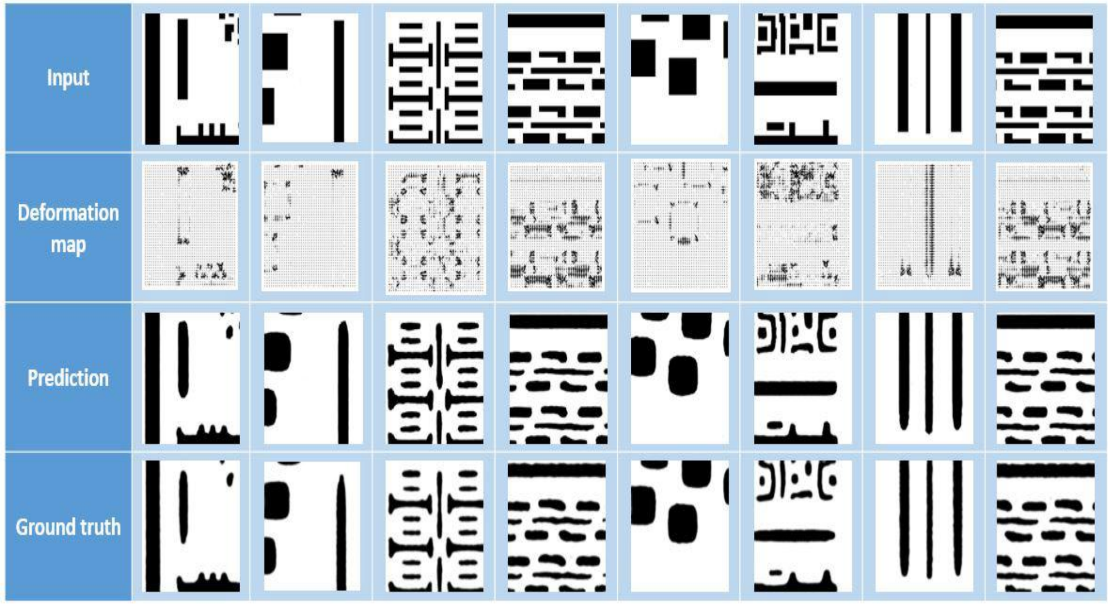
**Comparison of the input layout patterns, the predicted deformation maps, the predictions of fabricated IC shapes based on the deformation maps, and the ground-truths of fabricated IC shapes extracted from their associated SEM images.**

- **OPCNet** Description
  - ✓ Traditional **optical proximity correction (OPC)** methods used to suggest a correction on a lithographic photomask is computationally expensive.

# AI-PIE-HS : Technique [2] - D

- OPCNet Description
  - ✓ It is a CNN-based photomask corrector.
  - ✓ The **OPCNet** mimics the **OPC** procedure and efficiently generates a corrected photomask by collaborating with **LithoNet** to examine if the shape of a fabricated circuit optimally matches its original layout design.
  - ✓ The **OPCNet** is trained and build its knowledge without ground-truth **OPC-based corrected** masks based on an input-output consistency loss model.
  - ✓ In the mask optimization problem, **OPCNet** can correctly predict the mask desirable to achieve the expected layout.

- In the lithography simulation issue, the system outperforms existing image-to-image translation schemes and the standard compact model-based simulation.



**Comparison of the input layout patterns, the predicted deformation maps, the predictions of fabricated IC shapes based on the deformation maps, and the ground-truths of fabricated IC shapes extracted from their associated SEM images.**

# AI-PIE-HS : Technique [3] - A

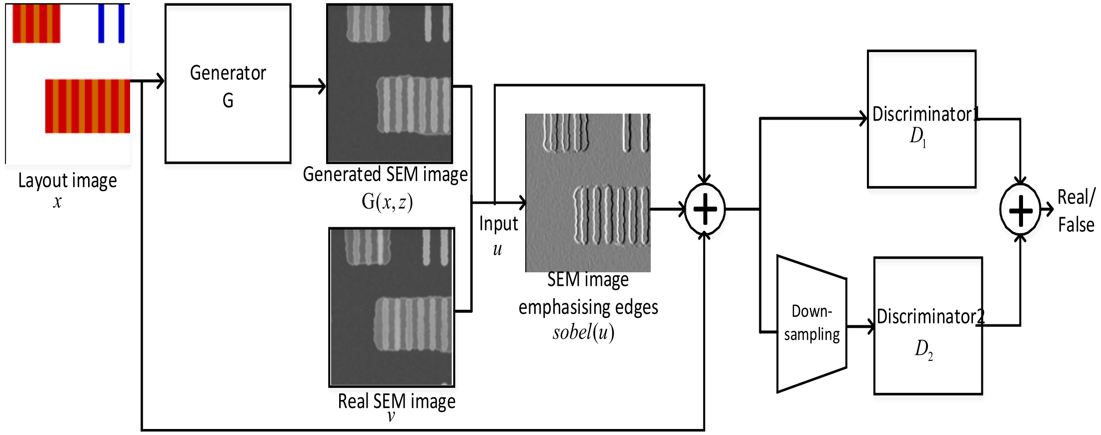
- **SEM images** play an essential role in the analysis and evaluation of the defects of the circuit in advanced integrated circuit manufacturing.

- The **image generation method** is a useful mean to solve the insufficiency of wafer SEM images due to the high cost of getting a large number of labeled SEM images.

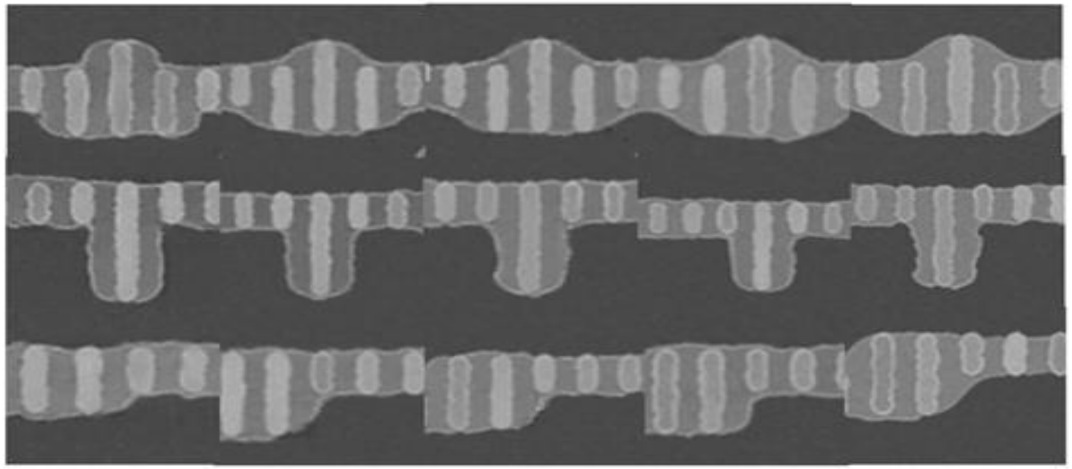
- Here, there is an algorithm based on **conditional generative adversarial network (cGANs)** for SEM image generation.
  - ✓ The model used for the cGAN is based on the Pix2Pix model.

- A *Sobel operator* is used to calculate the gradient information of images to guide the discriminator.

- Apply **two discriminators** to discriminate images of different resolutions.

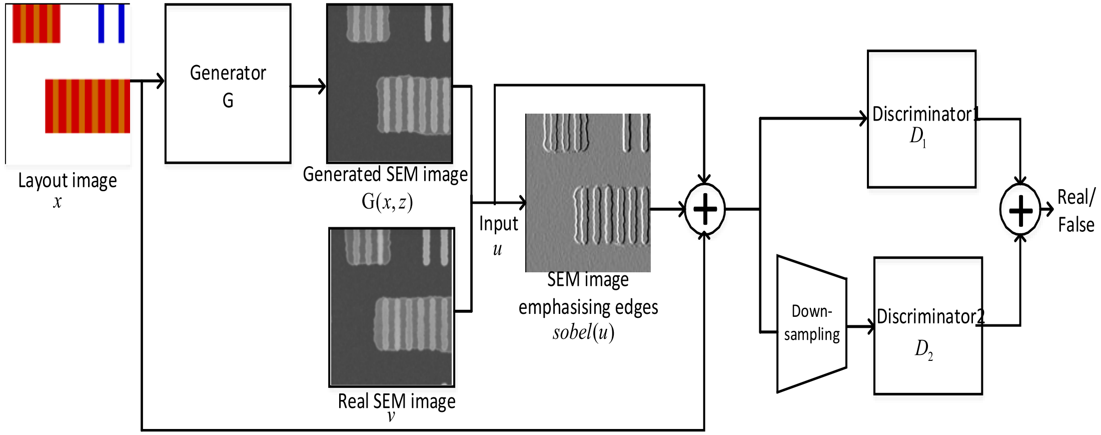


**The framework of algorithm for wafer SEM image generation.**

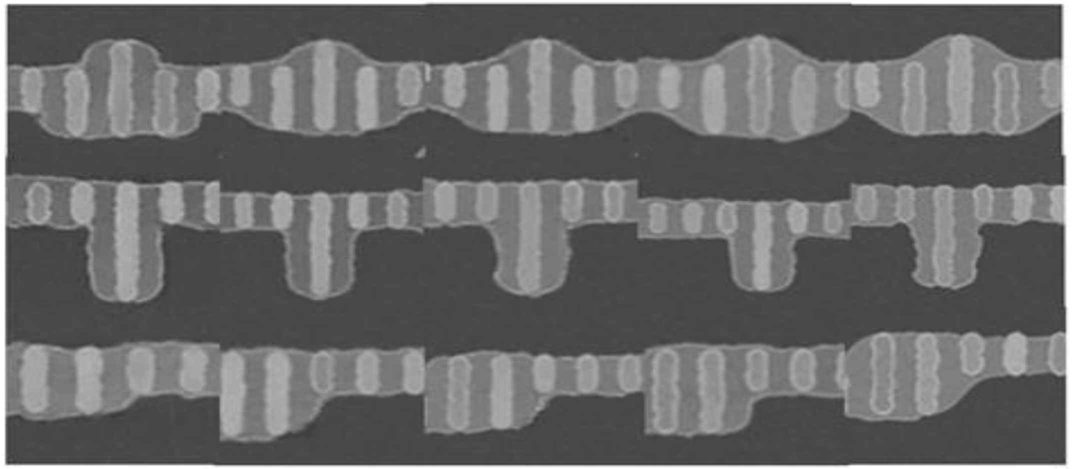


# AI-PIE-HS : Technique [3] - B

- Wasserstein distance and smooth L1 loss functions are applied to accelerate network convergence.
- Able to **learn** to **mimic** the distribution of wafer SEM image data effectively.
- The system generates great quality images.
- Improvement in 1-Nearest-Neighbour (1-NN) classification score in compare to other data generation methods.
- Alleviation of the shortage of wafer SEM images with realistic look samples and consistent with the requirement of high-dimensional features in the original samples.



**The framework of algorithm for wafer SEM image generation.**



# AI-PIE-HS: Technique 4 – General View (A)

- **IC's Authenticity is determined according to the status of its logical blocks.**

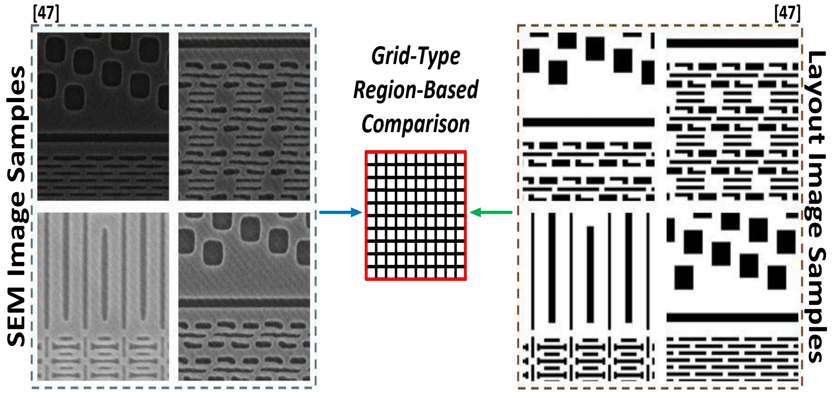
- **General Computing Process for this system is defined as:**
  - ✓ **Gridding for regions of interest extraction.**
  - ✓ **Block detection in the extracted regions.**
  - ✓ **Analyzing the detected blocks based on their attributes (e.g. *shape, location, width, and length*).**
  - ✓ **Recognizing detected blocks.**
  - ✓ **Assessing the blocks validity based on the recognition and the analysis reports, and flag possible Trojans.**

- Nanoscale dimensions of logic cells and hardware Trojans in addition to the noise in IC images pose *unique challenge* to image processing and visual inspection.

- Leveraging the traditional and modern computer vision (CV) algorithms to address image classification challenges belonging to PIE is a new research direction to study.

Computing Process

1. *Image Processing: The grid-type regions from each sample are extracted and their images are processed.*
2. *Block Detection: The blocks are detected in every region.*
3. *Block Analysis: The blocks from every region are analyzed.*
4. *Block Recognition: The blocks from every region are recognized.*
5. *Decision Making: The validity of the the blocks is assessed and a Hardware Trojan is flagged if it exists.*



*Grid-Type Region-Based Comparison of IC Blocks for Hardware Trojan Detection*

**An abstract visualization of the proposing system for block detection and recognition of the ICs and their physical assurance.**

# AI-PIE-HS: Technique 4 – General View (B)

- **Hardware Trojans** are identifiable through the unique features, attributes, and other properties of the IC objects/cells as well as their dimensions.

- The **unique features and properties to extract from an IC SEM image** should represent variations in the ***fabrication process, defects, dimensions, noise, and common distortions*** in order to achieve a more **accurate recognition and classification**.

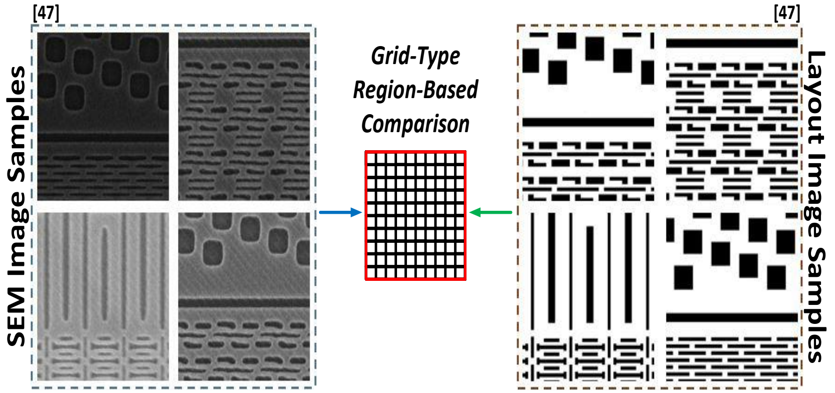
- The knowledge of analyzing **repetitive structures** in an IC SEM image must be incorporated in feature extraction and recognition computations.

- Due to the advancements of "**object detection**" and "**recognition**" methods, they are promising methods for physical assurance.

- Any *emerging method in different applications* including face detection, pedestrian detection, and vehicle detection can be introduced as a **baseline framework** for the **IC physical assurance**.

Computing Process

1. *Image Processing: The grid-type regions from each sample are extracted and their images are processed.*
2. *Block Detection: The blocks are detected in every region.*
3. *Block Analysis: The blocks from every region are analyzed.*
4. *Block Recognition: The blocks from every region are recognized.*
5. *Decision Making: The validity of the the blocks is assessed and a Hardware Trojan is flagged if it exists.*



*Grid-Type Region-Based Comparison of IC Blocks for Hardware Trojan Detection*

**An abstract visualization of the proposing system for block detection and recognition of the ICs and their physical assurance.**

# AI-PIE-HS: Technique 4 – General View (C)

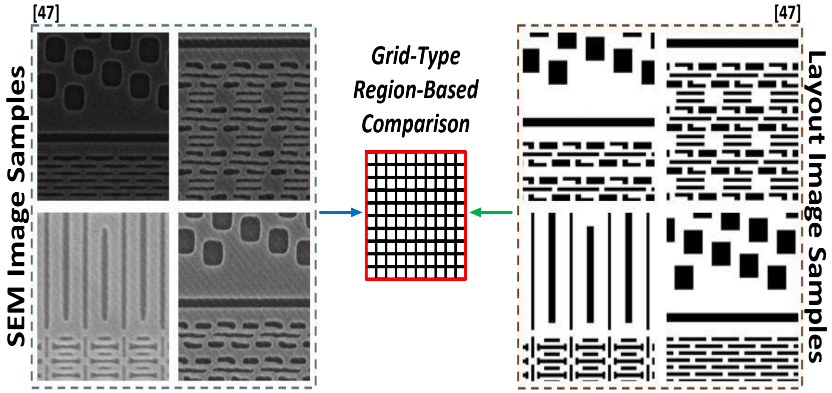
- A **CV-based system for physical assurance/inspection** can be built based on:
  - ✓ The **logic cells** are extracted in the **detection phase**.
  - ✓ The **detected cells** are analyzed in terms of their shape and structure in the **recognition phase**.
  - ✓ Logic cells are distinguishable objects based on their patterns and structures, location, shape, and dimensions.

- So, there is need in **developing** a novel **object detection and recognition system** for this problem, where the **objects** are logical blocks (i.e. logical gates/cells) and their **status** (i.e. **authentic, defective, and malicious**) is discovered based on the detection and recognition computing processes.

- **The system** needs to satisfy **a number of requirements**:
  a) Low execution time and high performance operation.
  b) Able to detect blocks of different shapes and at every location on the IC images.

Computing Process

1. *Image Processing: The grid-type regions from each sample are extracted and their images are processed.*
2. *Block Detection: The blocks are detected in every region.*
3. *Block Analysis: The blocks from every region are analyzed.*
4. *Block Recognition: The blocks from every region are recognized.*
5. *Decision Making: The validity of the the blocks is assessed and a Hardware Trojan is flagged if it exists.*



*Grid-Type Region-Based Comparison of IC Blocks for Hardware Trojan Detection*

**An abstract visualization of the proposing system for block detection and recognition of the ICs and their physical assurance.**

# AI-PIE-HS: Technique 4 – Detailed View (A)

- **The system** needs to satisfy **a number of requirements**:
  - c) Great capability in **feature extraction** and understanding.
  - d) Novel methods for **understanding data samples**, **preprocessing**, **pruning**, and **utilizing** them in detection and recognition.
  - **e) Discard or recover** the blocks with damages.
  - **f) Generate synthetic data** using an image-to-image translation system that helps overcome data shortage.
  - g) Highly **accurate and trusted recognition**.
  - h) Demonstrating **desirable functionality and performance** based on the state-of-the-art measures.

- The **general architecture of the system** includes two major sections:
  - i. Image Acquisition.
  - ii. Block Detection and Classification/Recognition System.

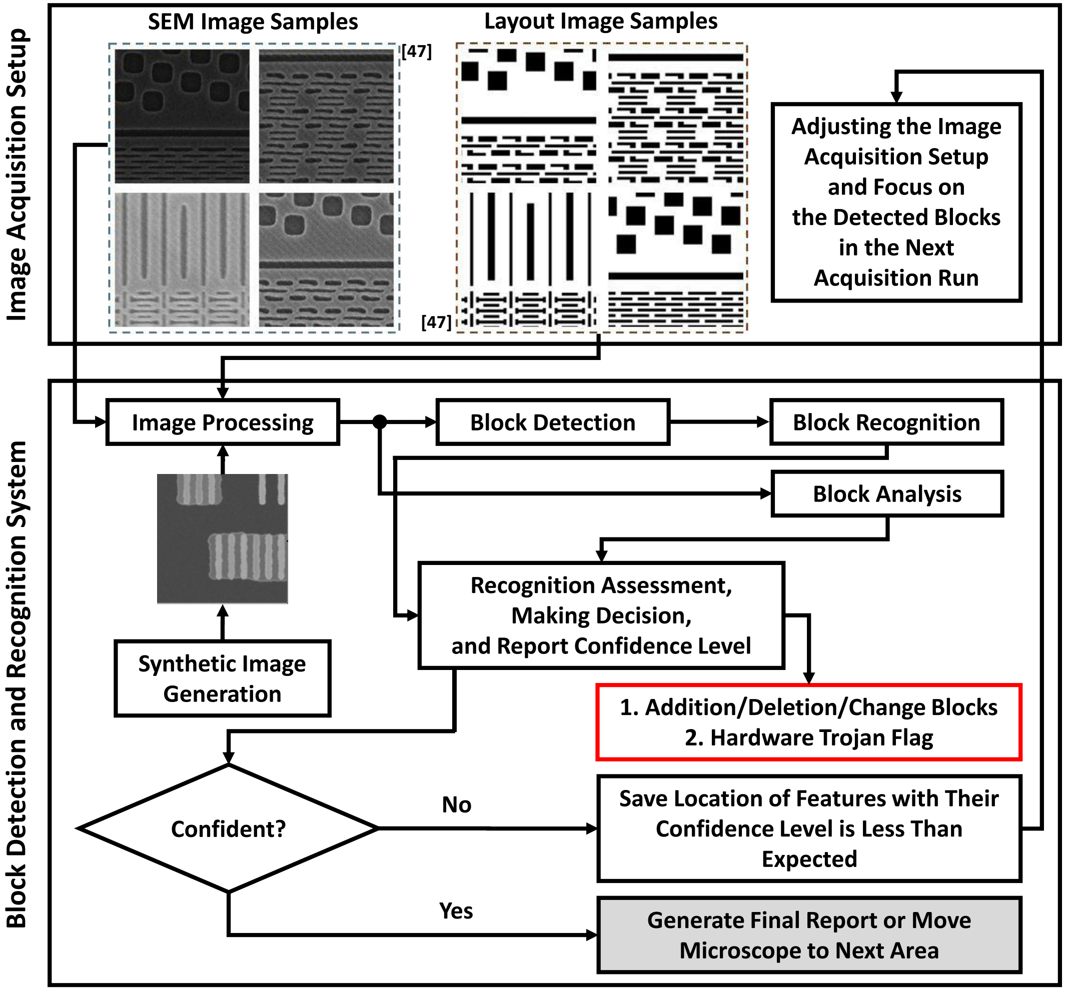


Image Acquisition Setup
SEM Image Samples
[47]
Layout Image Samples
[47]
Adjusting the Image Acquisition Setup and Focus on the Detected Blocks in the Next Acquisition Run
Block Detection and Recognition System
Image Processing
Block Detection
Block Recognition
Block Analysis
Recognition Assessment, Making Decision, and Report Confidence Level
Synthetic Image Generation
1. Addition/Deletion/Change Blocks
2. Hardware Trojan Flag
Confident?
No
Save Location of Features with Their Confidence Level is Less Than Expected
Yes
Generate Final Report or Move Microscope to Next Area

**The general system architecture for block detection and recognition of the ICs and their physical assurance.**

# AI-PIE-HS: Technique 4 – Detailed View (B)

- The **block detection and recognition system** includes **five major parts** including:
  1. **Image processing.**
     - The synthetic image generation unit is considered inside the image processing unit.
  2. **Block detection.**
  3. **Block analysis.**
  4. **Block recognition.**
  5. **Recognition assessment and decision-making.**

- The outcome of these major parts is **discovering addition, deletion, or change of blocks** as well as **flagging the existence of hardware Trojan** in the IC.

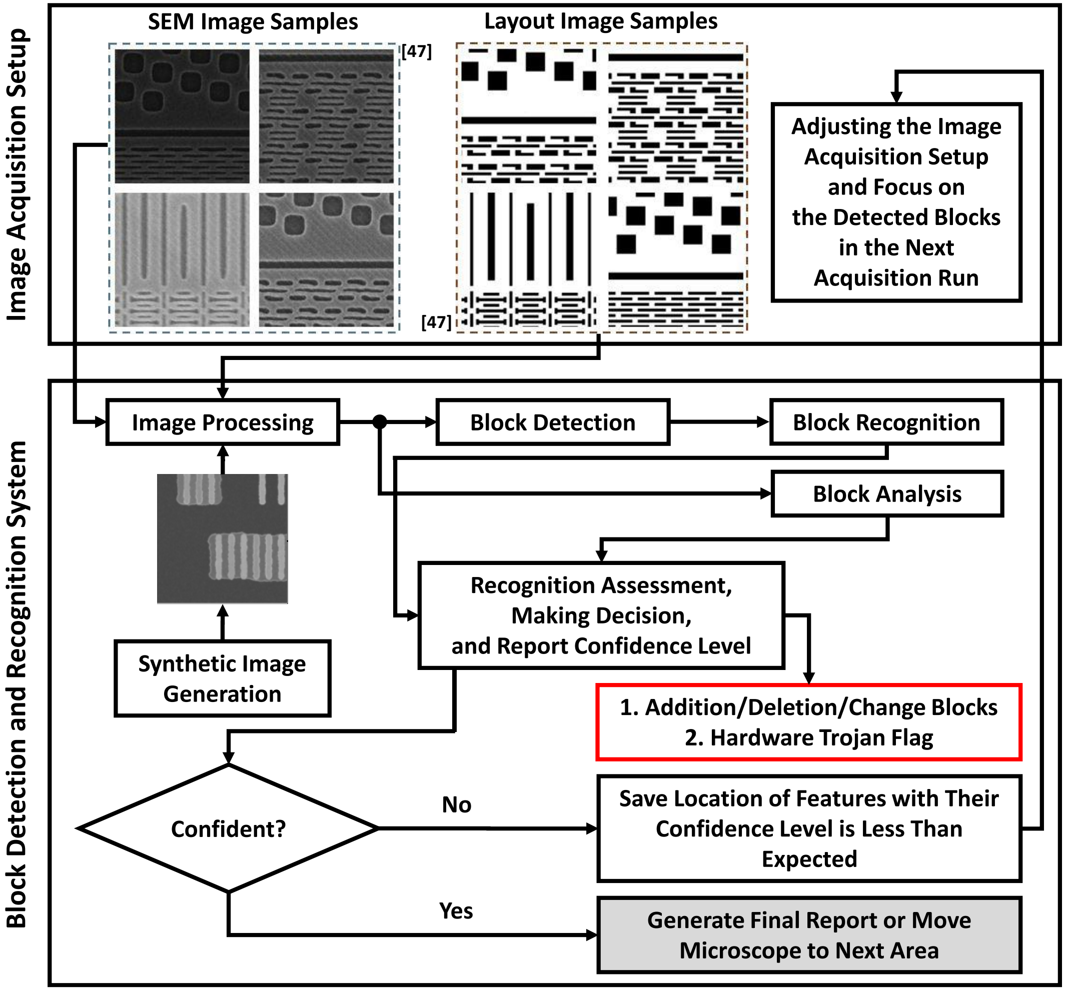


Image Acquisition Setup
SEM Image Samples
Layout Image Samples
[47]
[47]
Adjusting the Image Acquisition Setup and Focus on the Detected Blocks in the Next Acquisition Run
Block Detection and Recognition System
Image Processing
Block Detection
Block Recognition
Block Analysis
Synthetic Image Generation
Recognition Assessment, Making Decision, and Report Confidence Level
1. Addition/Deletion/Change Blocks
2. Hardware Trojan Flag
Confident?
No
Yes
Save Location of Features with Their Confidence Level is Less Than Expected
Generate Final Report or Move Microscope to Next Area

**The general system architecture for block detection and recognition of the ICs and their physical assurance.**

# Wrap-up

- **Application of AI in Cybersecurity** includes having security-based methods developed for both software and hardware platforms.
- **AI** can help both **attackers and defenders** in Cybersecurity by increasing their **strength** and making them **smart**.
- **AI** is applicable into different parts of the **security of hardware**, from the system-level, through logic-level design, physical design, and test and validation.
- Using **AI** in physical inspection of electronic devices provides intelligent examination of IC package.
- **AI-based PIE** can engage various technologies (including in-memory computing, **computer vision**, **deep learning**, transfer learning, and **reinforcement learning**) in order to improve the assessment of hardware status.
- We studied an AI-based hardware assurance system that operates based on stack of information and attributes extracted from IC layout.
- We reviewed a deep learning-based pre-simulation tool for predicting and correcting distortions in the fabricated ICs.
- We discussed the design of a synthetic IC SEM image generation system with having conditional GAN as the baseline.
- We talked about an IC inspection system that performs hardware-based object detection and recognition on IC SEM image.

# References

**[1]** Lin, T, Shi, Y, Shu, N, Cheng, D, Hong, X, Song, J, and Gwee, B.H., 2020. Deep Learning-Based Image Analysis Framework for Hardware Assurance of Digital Integrated Circuits.

**[2]** Shao, H.C., Peng, C.Y., Wu, J.R., Lin, C.W., Fang, S.Y., Tsai, P.Y. and Liu, Y.H., 2020. From IC Layout to Die Photo: A CNN-Based Data-Driven Approach. *arXiv preprint arXiv:2002.04967*.

**[3]** Du, H. and Shi, Z., 2020, April. Wafer SEM Image Generation with Conditional Generative Adversarial Network. In *Journal of Physics: Conference Series* (Vol. 1486, p. 022041).