ASIC DESIGNER'S IC LIBRARY FOR IC CAMOUFLAGING

by

MD. ISMAIL HOSSAIN

MASTER OF ENGINEERING IN INFORMATION AND COMMUNICATION TECHNOLOGY

Institute of Information and Communication Technology

BANGLADESH UNIVERSITY OF ENGINEERING AND TECHNOLOGY

September 2020

The project titled "**ASIC Designer's Library for IC Camouflaging**" submitted by Md. Ismail Hossain, Roll No.: 1014312041, Session: October 2014, has been accepted as satisfactory in partial fulfillment of the requirement for the degree of Master of Engineering in Information and Communication Technology on September 27, 2020.

BOARD OF EXAMINERS

1. Dr. Md. Liakot Ali Professor IICT, BUET, Dhaka	Chairman (Supervisor)
2. Dr. Md. Rubaiyat Hossain Mondal Professor IICT, BUET, Dhaka.	Member
3. Dr. Hossen Asiful Mustafa Assistant Professor IICT, BUET, Dhaka.	Member

CANDIDATE’S DECLARATION

It is hereby declared that this project or any part of it has not been submitted elsewhere for the award of any degree or diploma.

Signature of the Candidate

MD. ISMAIL HOSSAIN

Table of Contents

List of Figures

Abstract

Reverse engineering is a burning issue in integrated circuit (IC) design and manufacturing. It results in revenue loss of billions of dollars every year. Through reverse engineering process, an attacker can easily find out the functionality of a chip using Scanning Electronic Microscopy (SEM) image processing techniques. Several researches have been done to combat this issue in the material level by changing the doping concentration and relevant techniques. In this work, a technique has been implemented in the physical design level to reduce the recognition of a circuit functionality through image processing methodology. Attacker will see similar layout structure or similar images for the universal logic gates. And, using these universal gates we can design any other logic gates and the whole standard cell library as well. For better output, besides physical design modifications, dummy/true contact based technique has been implemented. The library contains different camouflaged primitive gates developed by combination of using metal routing technique and true/dummy contact technique. In IC design industry, it is required to compromise additional area, power consumption, delay and relevant factor while implementing IC camouflaging techniques. This works results in increase of the total area by about 17.37% and 1.357ps delay. To implement and verify these things, firstly, universal gates NAND and NOR have been designed applying proposed techniques in Cadence Virtuoso platform. Then, a bigger logic gate, XOR has been designed using both convenient gates and camouflaged gates. Finally, a comparison has been shown what changes are found after implementing these techniques. The whole design has been implemented in 90nm process technology.

Acknowledgement

This project would have been impossible without the will and wish of the almighty Allah and I am grateful to Him.

This is my immense pleasure to express my sincere gratitude to my supervisor, Dr. Md. Liakot Ali, Professor, Institute of Information and Communication Technology (IICT), Bangladesh University of Engineering and Technology (BUET) for providing me the opportunity to conduct my M. Engg. Project on “ASIC Designer’s IC Library for IC Camouflaging”. I convey my heartfelt thanks to my supervisor Sir for continuous guidance, kind help and wholehearted encouragement during the course of the work, without which this work would never be possible.

I would like to convey my thanks to all other examiners of the board, the staff and the teachers of the IICT for the cordial and friendly support during this work. I would like to thank my institute IICT, BUET for giving me this opportunity.

I also express my deep gratefulness to so many people who have helped me during this work by their valuable lecture, time, hospitality and cooperation. Finally, I would like to thank my parents, wife and son for being the motivation behind finishing this project.

Chapter 1: Introduction

1.1 Introduction

In this chapter, a little bit background is discussed. What types of works are done so far and importance. Then the objective is explained with points. And, finally the organization of the whole report is explained.

1.2 Background

Continuous increasing of design complexity and high design cost have led to the globalization of integrated circuit (IC) design and fabrication [1]. However, several issues such as reverse engineering (RE), IC counterfeiting and overbuilding, hardware trojans, side channel attacks and others have caused serious security and economic concerns in semiconductor industry [2]. Specifically, it affects the total supply chain process which in turn has resulted in billions of dollars loss each year [3]. Different types of circuit camouflaging have been proved effective to combat the reverse engineering attacks which basically recovers the original netlist through scanning electron microscopy (SEM) images [4-5]. It is usually applied in combinational logic of an application specific integrated circuit (ASIC) and proactively hides the layout information of intellectual properties (IPs) with aim to make RE exponentially more difficult [6]. Specifically, it hides the design information of IC by replacing some conventional logic gates with specially designed camouflaged cells, in which different types of camouflaged gates have been configured to perform one of the multiple functionalities while maintaining an identical look to Reverse Engineering attackers [7]. Therefore, while the attacker performs top-down reverse engineering, he/she will not know the actual functionalities of the camouflaged gates or get an incomplete or deceived netlist and thus fail to reverse engineer the IC [8]. An open source library of different camouflaged gates of different combinational logic developed using true/dummy contact-based technique can help the ASIC designer to secure their design from RE and save huge revenue loss [9]. However, the ASIC designer need to know the performance matrix of each logic gate in terms of resource burden, power, and delay so that they can choose the best based on the need of their project. So, there are scopes of research in the said direction [10].

Different types of techniques have been implemented for years for camouflaging. True/Dummy contact based technique is the most popular way to make camouflaged cells as it works in alternate ways between two contacts based on the requirements. In this process, between two contacts, one acts like active while other as inactive. A clear instruction need to be provided to fabrication lab to apply special layer so that contact can decide whether it needs to be active or inactive.

Another way of making camouflaged cell is control the doping in the drain area of a MOS. This way, one NMOS acts like always ON device while PMOS acts like always OFF. Thus a NAND gate functions as an inverter. Similar works have been done before.

Few other methods are also popular like SRAM based camouflaging and filler cell based camouflaging. These methods make the overall performance slower than regular methods as it needs extra layers, sometimes extra cells, along with the logic gates.

Among them, layout design technique is the most effective method and better in terms of performance overhead. That’s why this project has been planned to apply camouflaging while designing layout of logic gates.

1.3 Objective with Specific Aims

The goal of this project is to design logic gates by implementing layout technique and develop an open source standard cell library so that ASIC designers can use to design chip. This objective would be fulfilled through the following aims:

I. To design universal logic gates with modified technique and dummy/true contact methodology.

II. To develop a full library that would be usable to design chip design and development.

III. To test and verify with design software and verification software so that all the conditions are fulfilled.

1.4 Organizations

There are 5 chapters in this report in total. In chapter 1, we discuss an overview and objectives of this project. In chapter 2, we discuss on IC camouflaging, their effects, benefits and applications in the IC design industry as well as the previous works. In chapter 3, we discuss in brief how the approach is done towards the objective and how the implementation has been done with the proposed design. In chapter 4, we show all the results and finally in chapter 5, there are few words about this project and suggestions on future possible works.

1.5 Motivation

The motivation is to design camouflaged gates those are industry acceptable and usable in the latest technology so that companies can also use these design for their chips as well as products.

Chapter 2: IC Camouflaging Overview

2.1 Introduction

This chapter contains the basics of IC camouflaging applications and importance. Different types of IC camouflaging are also elaborated with visual Figures.

2.2 IC Camouflaging Basics

Figure 2.1 shows the methodology and basic process of using IC camouflaging to thwart reverse engineering [6].

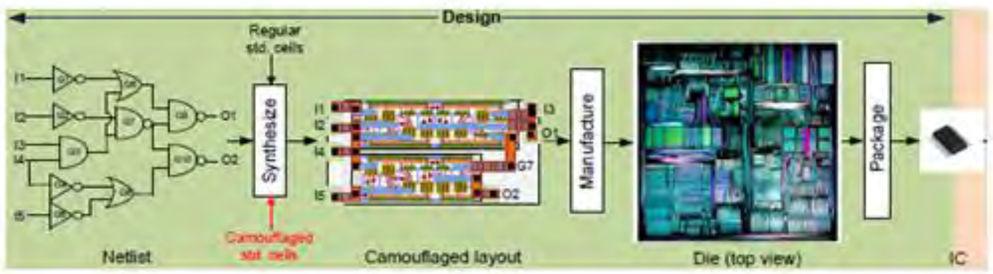


Figure 2.1: Camouflaged IC Designing

This process is divided into two main sub-processes. One is, Camouflaged IC Designing and another is Reverse Engineering.

A. Camouflaged IC Designing

The first step of the entire process starts with basic IC designing. The process of making an IC can be classified into two more sub-categories. First, it needs to be designed. Further, at second stage, it needs to be manufactured. The design process is again subdivided into front end and back end processes. They are again classified in different steps: Specification, RTL Design, Functional Verification, Synthesis, and Physical Design. Specification means writing the functionality of the IC and defining its microarchitecture. These specifications are further programmed in hardware description language like Verilog in RTL Design.

In the functional verification phase, the correctness of the RTL Design, and also the quality and completeness of the testing process is ensured. Back end processes include Synthesis and Physical Design. After being verified, the HDL code is converted into digital circuit using logic gates and flip-flops only. The digital circuit consists of list of logic gates that are connected appropriately to perform the designed functionality of the IC. This circuit diagram of the final IC comprising of logic gates is known as "Netlist".

Further when we go into synthesis, we not only use the standard cells, rather we also use the camouflaged cells. Then, we create a layout in physical design part, and the layout consists of patterns of both standard and camouflaged cells. This layout is then sent to fabrication. Thus, the chip is manufactured. From the designers or the defenders point of view, there are some decisions to be made like how many camouflaged cells we afford to use in a design, in what structure the camouflaged cells is to use in the design, in what part of the design we will use these camouflaged cells, and so on.

These decisions ensure the security that the design will obtain out of using camouflaged cells and also have implications in terms of the area, power, and delay overhead that the camouflaged cells incur. Usually a designer is not able to camouflage all the existing gates being present while designing due to the consideration of the aforementioned factors- area, power and delay overhead. After all the procedures of designing are completed, the manufactured IC is sold in the market.

B. Reverse Engineering of Camouflaged Process

From the attacker's point of view, reverse engineering procedures are explained in the Figure 2.2. The attacker takes the camouflaged chip and depackages it by using some corrosive chemicals. Here, the epoxy packaging of the chips is removed and thus, exposing the dies. Further, the delayering of each layer including diffusion, poly and metal is done. Delayering of the lower metal layers is tougher than the process of delayering the higher metal layers because of their relative higher thickness.

Then, by using an optical microscope, the imaging of the top view of the chip's each layer is conducted. All the metal routing, pins and conducts present in each layer may be displayed in this image. This imaging process can also be carried out by using a single electron microscope as well.

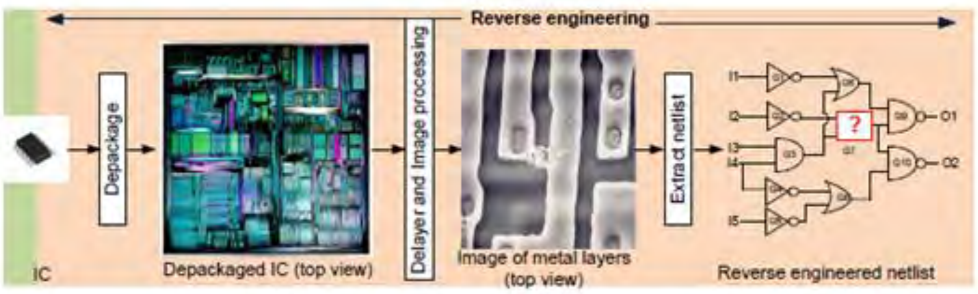

Reverse engineering
IC
Depackage
Depackaged IC (top view)
Delayer and Image processing
Image of metal layers (top view)
Extract netlist
I1
I2
I3
I4
I5
?
O1
O2
Reverse engineered netlist

Figure 2.2: Reverse Engineering of Camouflaged IC.

The last stage of a reverse engineering technique is the extraction of Netlist. For completing this stage successfully, the attacker may use the tools Degate or Chipworks. But, after extracting the Netlist, the attacker will find some ambiguity due to the presence of the Camouflaged Cells.

The attacker won't be able to distinguish whether the gate used is a NAND gate or a NOR gate under the microscope because the contacts might be True contact or Dummy contact. Thus, the attackers won't be able to know all the functionalities of the camouflaged cells. That's the reason an attacker can't reverse engineer any camouflaged cell, though they can do so the same to any standard cells.

2.2 Types of IC Camouflaging

2.2.1 True/Dummy Contact Based Camouflaging

In the Figure 2.3, if we consider the formation of a multiplexer based camouflaged cell [6], it will be seen that each input line termed as Xi is connected to both Drain to Drain Voltage, Vdd and Ground, Gnd. In between the connection the true/dummy contacts are placed. If one contact is the connection (True), the other one will be isolation (Dummy), and vice versa. If Xi configured to "1" refers to the Vdd being the true, whereas the Gnd connector being the dummy contact.

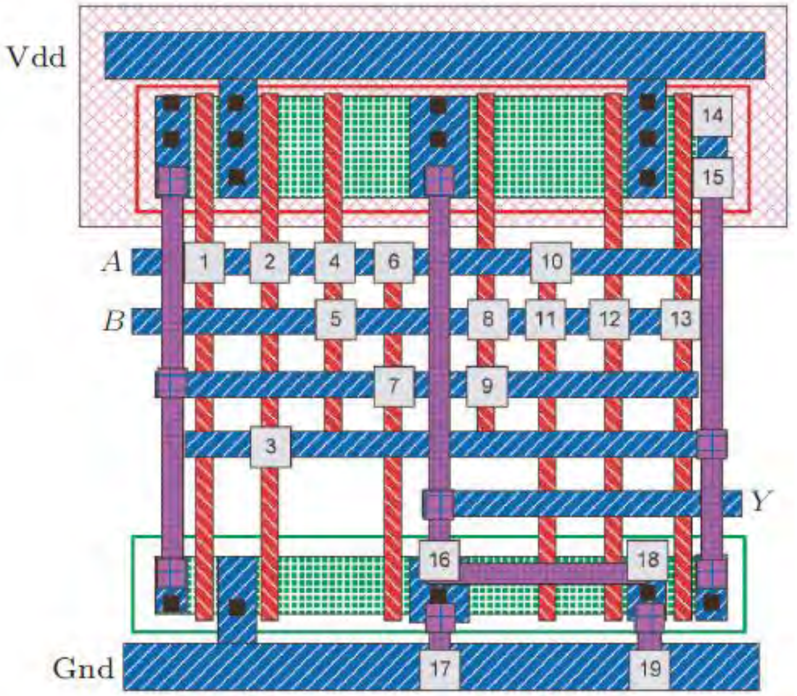


Figure 2.3: True/Dummy Contact Based Camouflaging

Again, if the Vdd connector is the dummy and Gnd is true, then it'll refer that Xi is configured to the state "0". If it's considered that the selection lines be the inputs, again the output lines be the output; then the equation of the functionality of a camouflaged cell can be written as,

$$Y = (A \text{ x } B) \text{ x } X1 + (A \text{ x } B) \text{ x } X2 + (A \text{ x } B) \text{ x } X3 + (A \text{ x } B) \text{ x } X4. \qquad (1)$$

So, there can be 16 possible combinations of 2-input and 1-output Boolean functions. Thus, for X1, X2, X3 and X4, there are 16 different possible configurations. If the input values of X1, X2, X3 and X4 be 1110, then the functionality function of Camouflaged Cell becomes Y= A x B + A x B + A x B = A x B. So, the camouflaged cell will perform as a NAND gate.

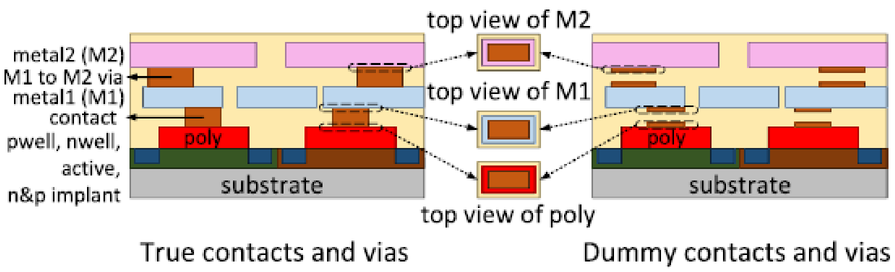


Figure 2.4: How True/Dummy Contacts Technique Works

As per Figure 2.4, True/Dummy contact concept is based on a layer that is pushed while doing Fabrication. It's a thin layer; after implementation it, physical connection get disconnected. From top view it seems it's connected, but in reality it's disconnected.

2.2.2 SRAM Based Camouflaging

The configuration information of SRAM based camouflaged cells is stored in a SRAM, which is better known as tamper proof memories. Thus, the real functionality of SRAM based camouflaged cells is concealed. For example, in case of the SRAM based camouflaged cell, it stores its configuration bits in memory cells instead of configuring them into any true/dummy contacts. If the 4 by 1 multiplexer, shown in Figure 2.5, is configured to perform 16 possible 2 to 1 (2 input to 1 output) Boolean functions, a similar sort of effect will be achieved [10].

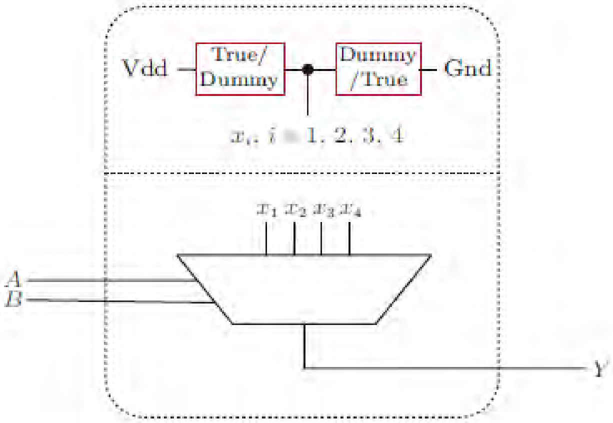


Figure 2.5: Multiplexer configuration with True/Dummy contacts.

2.2.3 Doping Based Camouflaging

In case of doping based camouflaged cells, there is an integration of certain always on/ off MOS transistors [10].

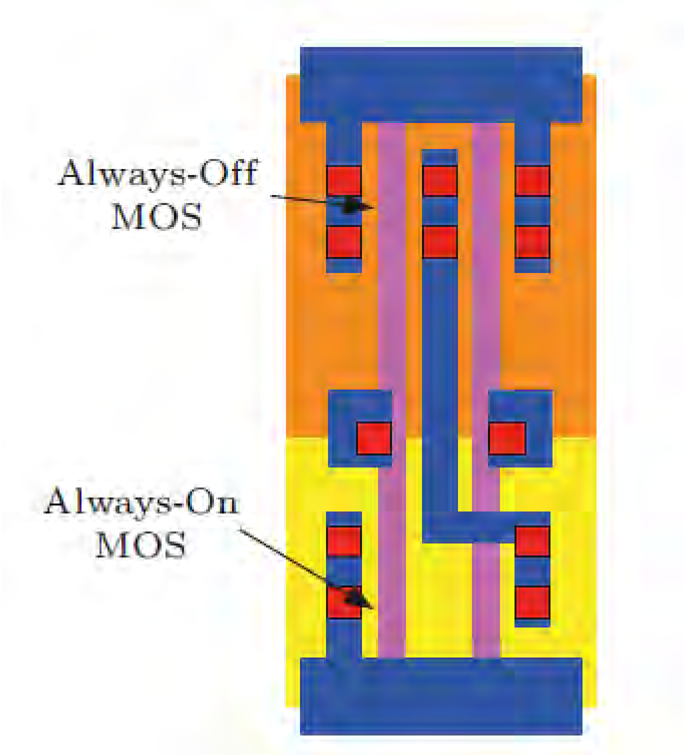


Figure 2.6: Doping based IC Camouflaging

In the Figure 2.6, MOS refers to Metal Oxide Semiconductors. These certain characterized MOS transistors are designed by altering the nature and shape of typical Light Doped Drain (LDDs). This can be achieved in different ways, either by changing the polarity of the dopant used in the MOS transistors' source and drain, or by changing the LDD implants' length and type. Thus, these sorts of doping based cells will obtain the same amount of polysilicon and metal layers with standard ones in the library.

For example, in case of the conventional 2-input NAND cell showing in Figure 2.6, if the always on doping scheme can be used for NMOS transistor, and inverse one, i.e. the always off scheme can be implemented for PMOS transistor, then the camouflaged cell will turn into an inverter.

2.2.4 Emerging Device based Camouflaging

Considering the alternatives of CMOS technology, emerging devices have already been researched for meeting the scaling challenges. Examples of such emerging devices are FinFETs, Carbon Nanotube FETs (CNTFETs), tunnelFETS (TFETs), Memristors, Graphene based Symmetric Tunneling FETs (SymFETs), and Spin Transfer Torque Devices (STT). Recently, it has come to light that these emerging devices have some exclusive features which can be used to implement some safety related applications.

Emerging technology has been implemented in circuit camouflaging techniques to build camouflaged circuits. For example, using the exclusive feature of controlling the polarity of SiNW FETs, it is possible to build the desired Camouflaged Cells avoiding redundancy of using extra FETs.

STT based LUT has some distinct features like high density assimilation density, higher retention time period, thermal strength, and high withstanding almost zero leakage. Thus, as an alternative model of SRAM based LUT, this STT based LUT is highly efficient to design.

Recently, the idea of employing emerging devices as means of building camouflaged cells is a promising trend and it has also gained immense attention by specialists and researchers. Emerging devices have multiple advantages over basic CMOS logic and show more promises. But, still most emerging devices are on the stage of simulation and yet to go a long way to make them implemented in real life circuitry designing. On the other hand, SRAM based camouflaged cells have re-configurable properties. These properties have made these cells capable of utilizing detection of Trojan in online hardware appliances. It can be done by loading a mistaken configuration first after the Trojan being identified. There is a single drawback though in such applications. The memory cells count may be higher and thus there might be non-volatile memory requirements. Doping based Camouflaged Cells use latest and high technology and require precise control over the type of LDD being used, and also the shape of their body. Apart from all other Camouflaged Cells, the study related to the true/dummy contact based Camouflaged Cell has been a bit extensive, and they are also widely spread in academic research purposes. Designers are expecting to increase the functionalities of camouflaged cells; also they are hoping that their sustained performance overheads can be reduced. There exists a tradeoff between two different camouflaged cells. The 16 function multiplexer based one shows better performance overhead than the 3 function {NAND, NOR, XOR} camouflaged cell. However, the challenge of increasing the possible number of each camouflaged cell's functionalities while reducing their performance overheads still has remained as a challenge that needs to be overcome as soon as possible.

Chapter 3: Library Development Technique

3.1 Introduction

This chapter contains the library development flow. We discuss the design and development process and the tools used. Steps are also described.

3.2 Components in the Library

Research has been done in hardware obfuscation changing the doping level and concentration [11]. In this report, only metal routing-based camouflaging has been applied. An attempt to design similar structured universal gates has been done in this work. As other logic gates are possible to design with only universal gates NAND and NOR, that's why those gates have been implemented with camouflaging technique. And, later on, an XOR gate has been designed with proposed technique to compare with the conventional design. So, initially, NMOS, PMOS, NAND, NOR and XOR, these 5 designs are available in this library. As training version of EDA tool has been used, there could be a deviations from the practical accuracy. On the other hand, professional library is expensive. Full library including all the other logic gates can be developed gradually. Each design has schematic design to check functionality and its corresponding layout design to check physical functionality.

3.3 Description of Each Elements

We have 5 designs in this proposed library: PMOS, NMOS, NAND, NOR and XOR. PMOS and NMOS. These have the normal structure and the size has been kept similar to avoid any complexity. Normally, the size of the PMOS is kept 1.2 – 2 times of the NMOS in the higher node technologies specifically in 180nm. But, here the size has been kept similar as it didn't affect the final result. Sizing could be optimized for better result in the profession library setup that is called Process Design Kit (PDK). NAND and NOR has been designed with these PMOS and NMOS devices. Then using these NAND and NOR gates, an

XOR gate has been implemented to check the effects of these proposed gates compared to the conventional gates.

3.4 Description of Design Steps

From scratch all the gates, PMOS, NMOS, NAND, NOR, XOR, are designed. The steps of XOR design are explained step by step in the following, as shown in Figure 3.1.

First of all, schematic is designed, then, a simulation run is done. From simulation result, proper functionality is found. After this confirmation, physical design is done with proper physical verification and RC extraction.

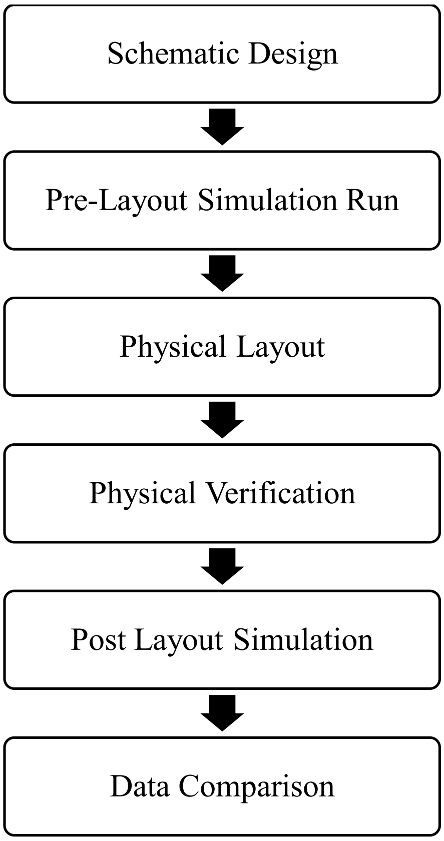


Figure 7: Design Steps Flowchart

Figure 3.1 shows the design steps that are followed while designing PMOS, NMOS, NAND, NOR and XOR gates.

3.4.1 Designing Schematics

In 1st step, schematic design of the gates or cells are done. Node connections and Pin Placements are done properly. In Figure 3.2, XOR schematic is shown.

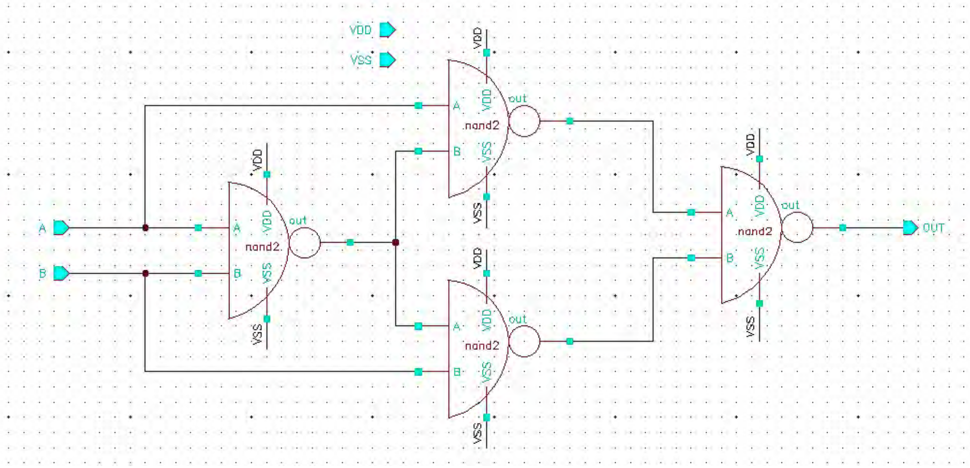


Figure 8: XOR Schematic Circuit

3.4.2 Simulation Run

In the 2nd step, proper simulation is run to check the functionality and design errors. No error is found and result comes as expected. This simulation run is also called Pre-Layout Simulation. When layout is involved in the whole design, simulation is called Pre-layout simulation. In Figure 3.3, the pre-layout simulation result is shown for XOR gate.

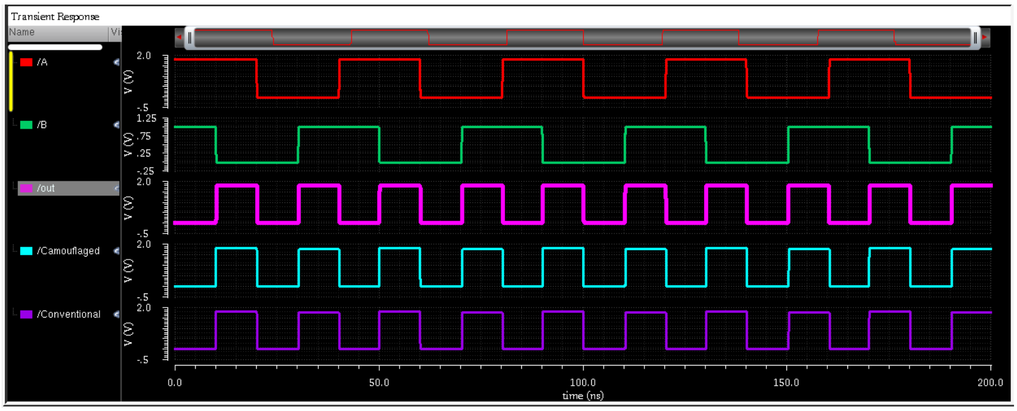


Figure 9: Pre-layout Simulation of XOR Gate.

3.4.3 Physical Layout Design

In this step, necessary setup is done to start the layout design like pins naming and placement. Layout design of each cell is completed. In this step, proper Floorplanning, device placement has been assured to make sure the maximum possible optimization. We can see from the schematic in Figure 3.2 that there are 4 NAND gates to form the XOR logic. In Figure 3.4, a single NAND is marked with RED Colored Box. 4 NAND gates are placed one by one and XOR is designed.

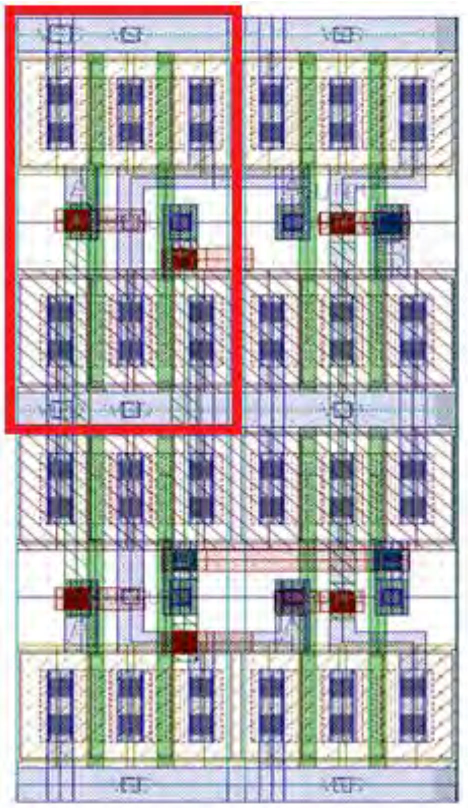
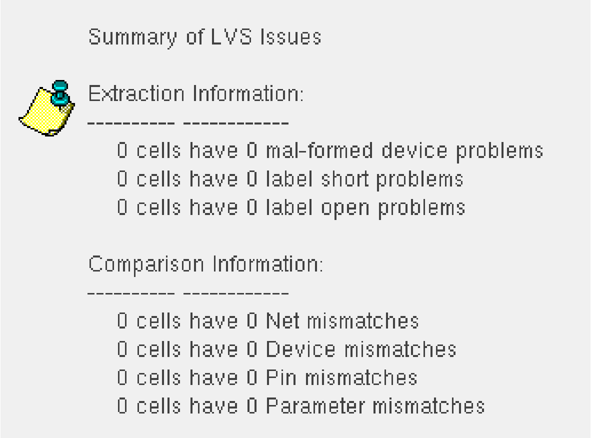


Figure 10: XOR Layout Design

3.4.4 Physical Verification

After the completion of the layout design, physical verification has been done: LVS and DRC. LVS stands for Layout vs. Schematic whereas, DRC means Design Rule Checking. LVS is a comparison between the schematic and layout.

Schematic of any gate should be matched with Layout of that gate. It ensures that design is okay to move further like post-layout simulation. In Figure 3.5, we see the numbers are zero. Zero means no error or warning found from the design. LVS goes right.



```
Summary of LVS Issues

Extraction Information:
---------- ------------
    0 cells have 0 mal-formed device problems
    0 cells have 0 label short problems
    0 cells have 0 label open problems

Comparison Information:
---------- ------------
    0 cells have 0 Net mismatches
    0 cells have 0 Device mismatches
    0 cells have 0 Pin mismatches
    0 cells have 0 Parameter mismatches
```

Figure 11: Physical Verification of XOR Gate Design

3.4.5 RC Extraction

In the final step, RC calculation has been done to check delay and other performance. When layout is designed, each and every layer has individual parasitics values that affects the performance considering practical things. So, delay is added due to these parasitics values. We can see delay in the output signals in Figure 3.6 for different configurations of XOR gate.

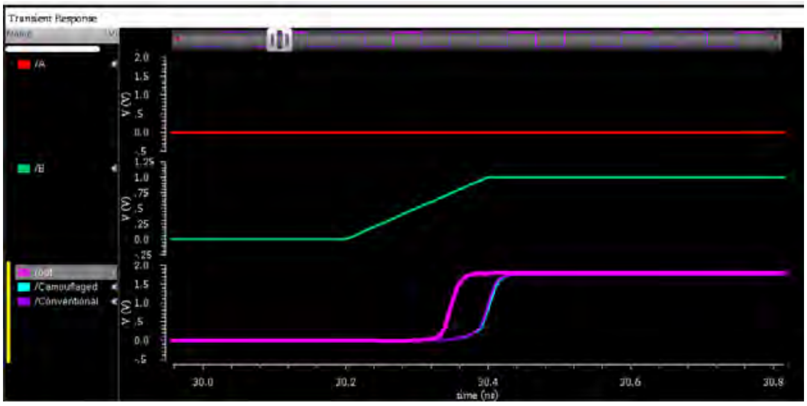


Figure 3.6: Delay due to RC Extraction.

3.5 Brief Description of Each Tool

The tools used for this project has been enlisted in Table 3.1. A little bit description is written after the table in different section.

Table 3.1: Tools Used for Implementation of Camouflaged XOR Gate.

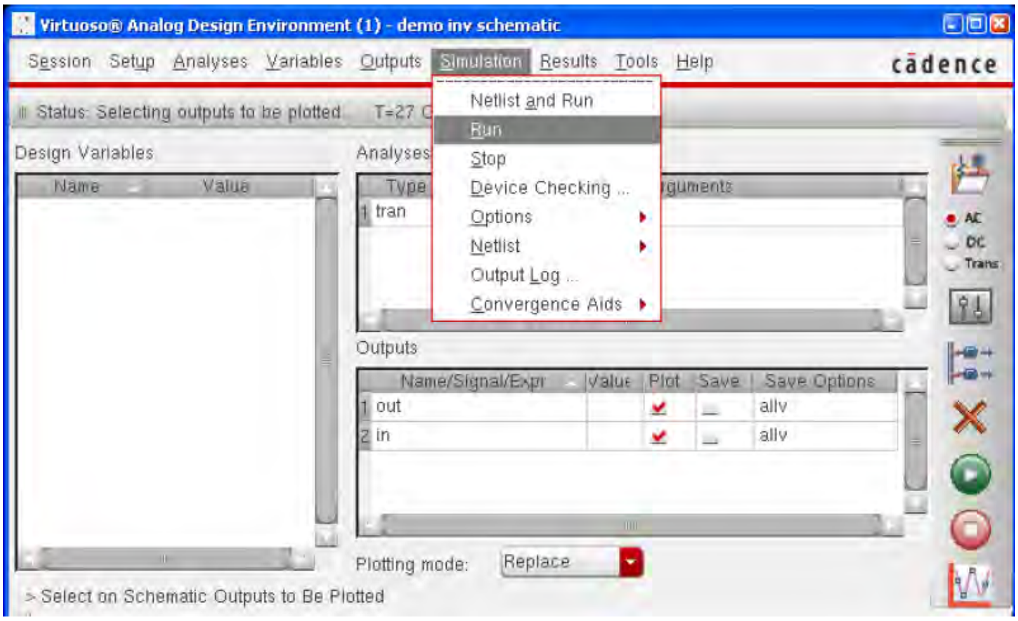
SN	Task	Tool Name	Vendor
1	Schematic Design	Virtuoso Schematic Editor	Cadence
2	Symbol Creation	Virtuoso Schematic Editor	Cadence
3	Simulation	Virtuoso ADE	Cadence
3	Layout Design	Virtuoso Layout Editor	Cadence
4	Physical Verification	PVS / Assura	Cadence
5	RC Extraction Post Layout Simulation	PVS / Asssura	Cadence

3.1.1 Cadence Virtuoso Schematic Editor

This tool provides many options and faster ways to import any component and design any complex circuit with proper and accurate annotations. The more options are there the more accuracy would be possible to get as outcomes from any circuit. A huge number of libraries are available there to start any design at instant. Cadence Virtuoso allows a number of tabs to open at the same time. In addition, it allows hierarchical design opportunity. And, the important thing is, there is no limitation of the level of hierarchy of a design.

3.1.2 Virtuoso ADE

This is a design environment by Cadence that enables all the settings to simulate any design. Any kind of simulation with any kind of setup is possible to run and check data generated from a specific design. ADE interface is shown in Figure 3.7.


Virtuoso® Analog Design Environment (1) - demo inv schematic
Session Setup Analyses Variables Outputs Simulation Results Tools Help
cādence
Netlist and Run
Run
Stop
Device Checking ...
Options
Netlist
Output Log ...
Convergence Aids
AC
DC
Trans

Status: Selecting outputs to be plotted T=27 C

Design Variables

Name	Value

Analyses

	Type	Arguments
1	tran	

Outputs

	Name/Signal/Expr	Value	Plot	Save	Save Options
1	out		✓	□	allv
2	in		✓	□	allv

Plotting mode: Replace

> Select on Schematic Outputs to Be Plotted

Figure 12: Cadence Virtuoso Analog Design Environment (ADE)

3.1.3 Cadence Virtuoso Layout Editor

This tool allows fabrication quality physical design of any design. Normally it generates physical components from schematic and designer can design any complex chip using this tool. GDSII file generating from the layout view design is forwarded to the FAB for manufacturing the design on wafer. So, the practical application of any design that has been designed using this software is very much impactful. Both flat and hierarchical design options are available in this software. Figure 3.8 shows a sample design in Virtuoso Layout Editor [13].

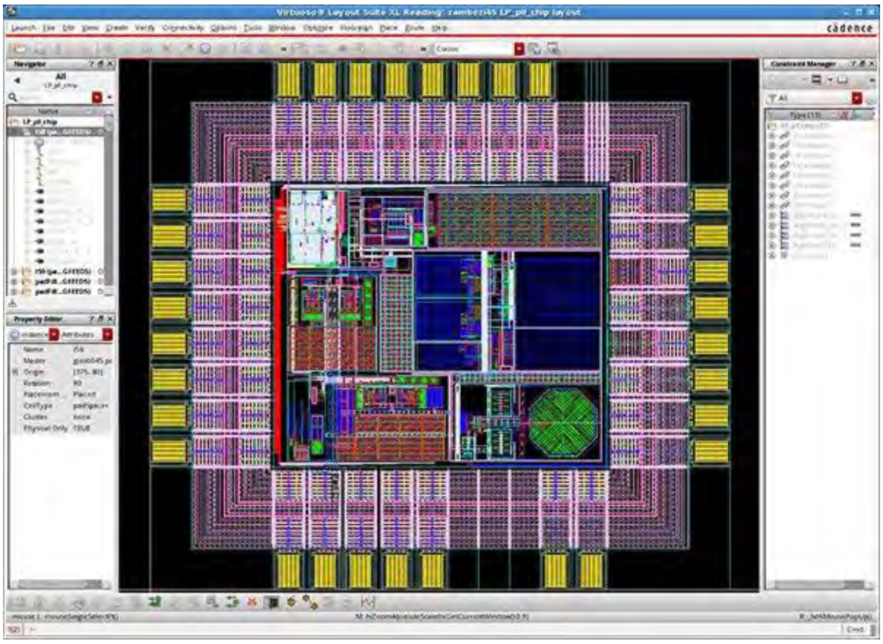

Virtuoso® Layout Suite XL Reading: zambezi45 LP_pll_chip layout
Launch File Edit View Create Verify Connectivity Options Tools Window Optimize Floorplan Place Route Help
cādence
Navigator
All
LP_pll_chip
Property Editor
Constraint Manager

Figure 13: Complex Chips are designed in Virtuoso Layout Editor XL.

3.1.4 Cadence Assura or PVS

After completing the schematic and its corresponding layout design of any logic gates or complex circuit, it's important to check both design whether they are functioning well, maintaining the quality, etc. To verify those designs, Assura (Cadence older version) or PVS (Cadence newer version) tool is used in the industry. They compare the functionality of any design, find out error regarding design rules, and calculate total power consumption, total delay and overall performance.

3.6 Execution Flow

So far, the design steps and tool descriptions are done one by one. Now, the execution flow is shown in Figure 3.9 shows the concept is implemented practically. The flow shows the full process.

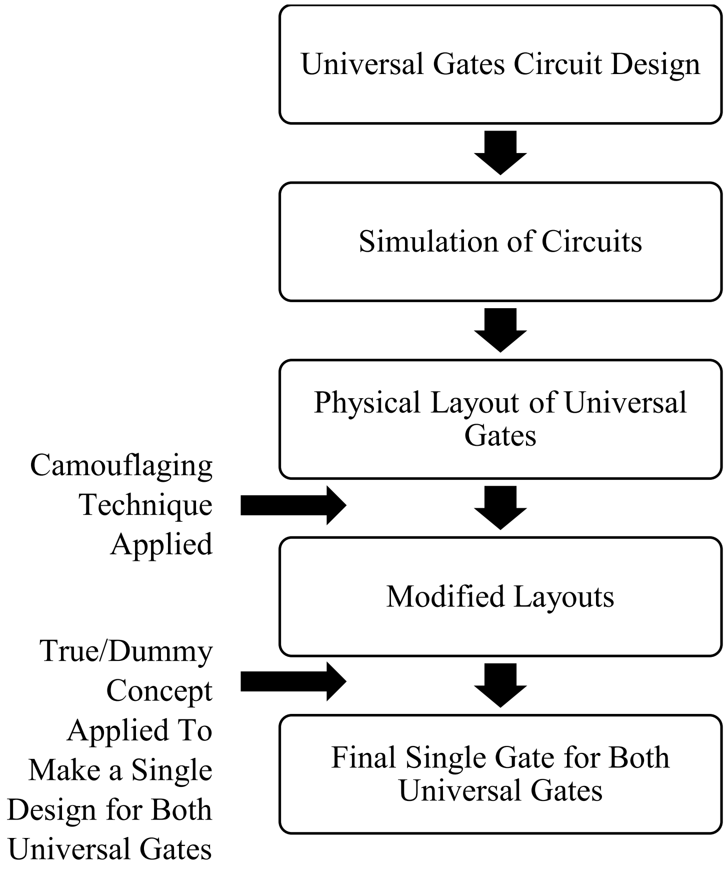

Universal Gates Circuit Design
Simulation of Circuits
Physical Layout of Universal Gates
Camouflaging Technique Applied
Modified Layouts
True/Dummy Concept Applied To Make a Single Design for Both Universal Gates
Final Single Gate for Both Universal Gates

Figure 14: Execution Flow.

Chapter 4: Results and Discussion

4.1 Introduction

This chapter contains the result and relevant discussions. Also the difference and comparison between the conventional design and proposed design is depicted through a tabular form.

4.2 Proposed Universal Gates Design

The idea was implemented on the universal gates NAND and NOR. First of all, metal routing was designed in such way that only VIA contacts position remains different. Except VIAs, all the other layer position and design are same in both gates. So, if we use the True/Dummy contact technique while fabricating the design then we can say that our designs are almost same for both NAND and NOR and it would become so tough to identify which is NAND gate and which is NOR.

The layout of the proposed logic gates is drawn in a camouflaged way by applying different metal routing technique. In semiconductor design industry, it is suggested to use the lowest allowable metal layers while designing standard cells to overcome the extra delay issue and slow performance. In our design, we used both metal 1 and metal 2 for routing.

4.2.1 Camouflaged NAND Gate

Figure 4.1 is the proposed camouflaged NAND gate. This design is done with some modifications in the metal level routing. The blue color layers are Metal 1 routing and the red color layers are Metal 2. In the conventional design, it’s possible to connect this nodes with only Metal 1. In this proposed design, there are two Metal 2 of same width and length. Then, Metal 1 connects these 2 layers.

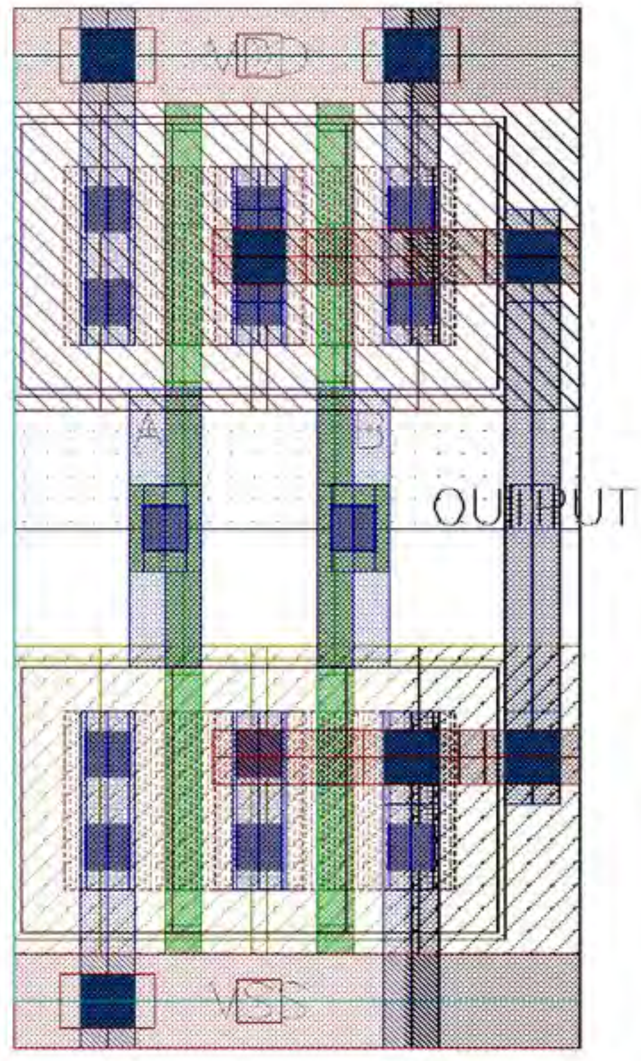


Figure 15: Proposed camouflaged NAND Gate

4.2.2 Camouflaged NOR Gate

Almost same design is done while designing NOR gate in Figure 4.2 to keep the similar patterns while routing with Metals. If we compare with the NAND gate shown in Figure 4.1, we can see only the VIA connections (deep blue color layer) are different here.

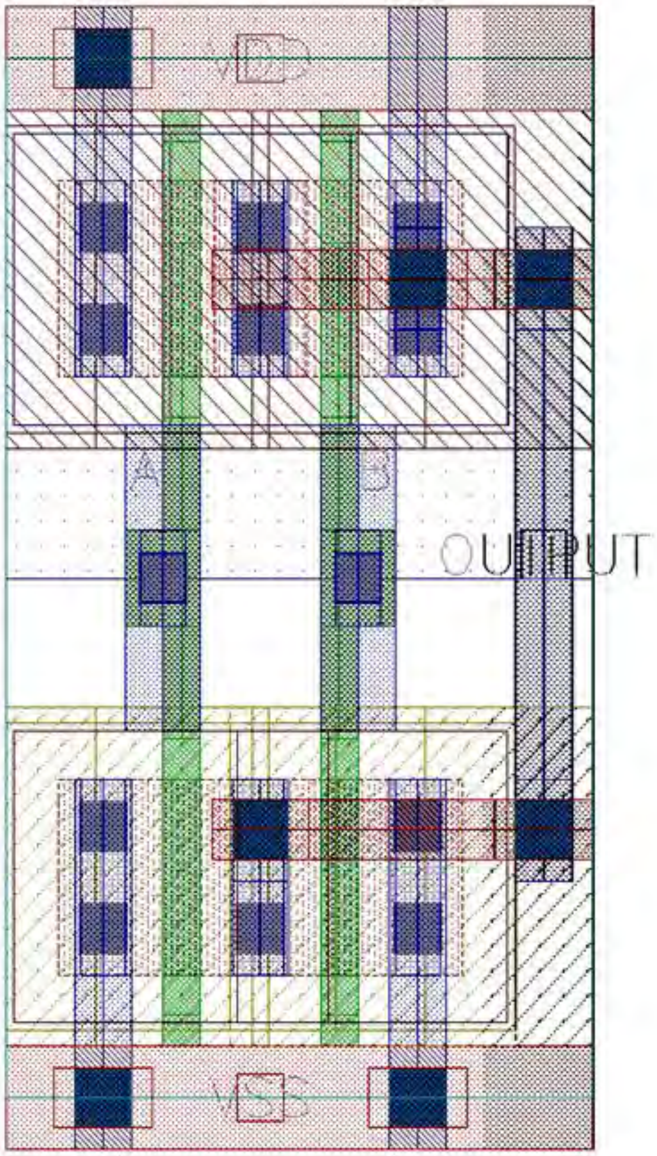
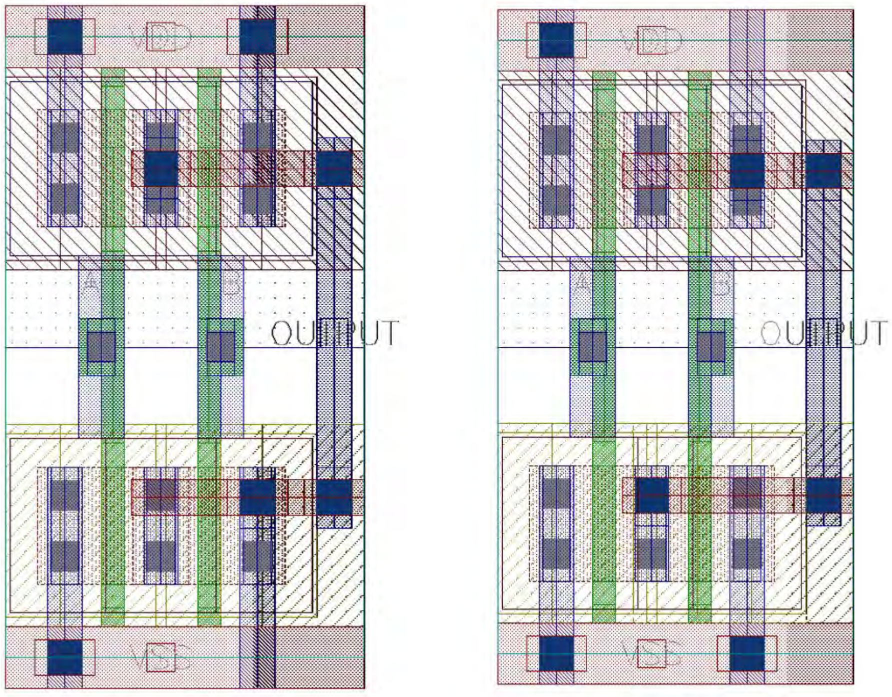


Figure 162: Proposed Camouflaged NOR Gate

4.3 Comparison of Conventional Design & Proposed Design

To differentiate the proposed gates, we need to compare them with conventional designs. In Figure 4.3, we can see the similarity between NAND and NOR gate. Only the VIA connections positions are different here. Others layers are same.

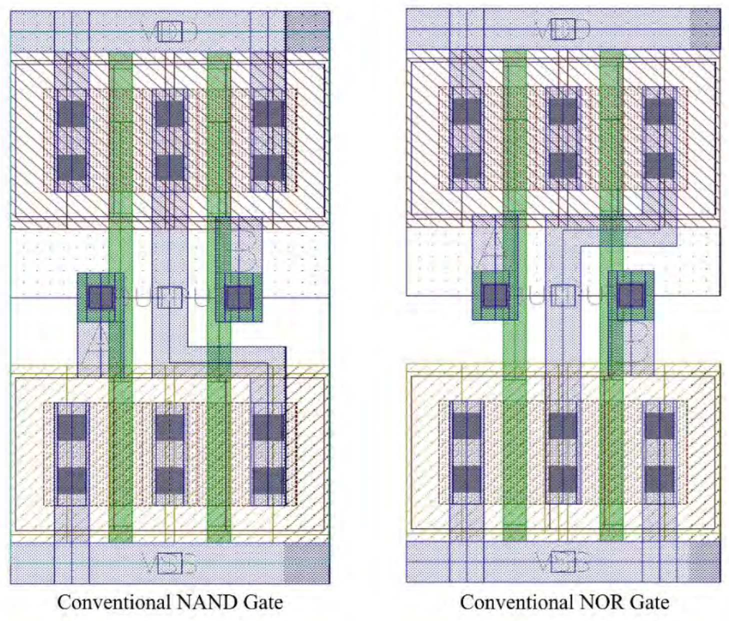


Camouflaged NAND Gate

Camouflaged NOR Gate

Figure 17: Camouflaged NAND and NOR Comparison

In Figure 4.4, we can see the conventional designs of NAND and NOR gates. Here only Metal 1 routing is used; no Metal 2 is there. For this type of design, it's possible to identify which is NAND and which is NOR gate. Due to Metal 1 bending, it's recognizable the series connection and parallel connections of the MOS. In the proposed design in Figure 4.3, there is no such confusion as the routings are almost similar. So, if someone tries to identify the gates with image processing approach, it would be very difficult to track it is NAND or NOR gate. If intruder tries to detect VIAs with precision, only then would be possible. That's why, True/Dummy contact approach is incorporated with this Metal routing techniques. The idea is discussed in section 4.5 with visualization.


Conventional NAND Gate

Conventional NOR Gate

Figure 18: Conventional NAND and NOR Gates

In Figure 4.5, it’s clear as we can see only the Metal that connects all nodes. For the PMOS, it’s visible that PMOS are in parallel and NMOS are in series connections. Then, it’s possible to get the idea which NAND and which NOR. Metal 1 bending connection depicts the connection clearly. That bending is removed the proposed design.

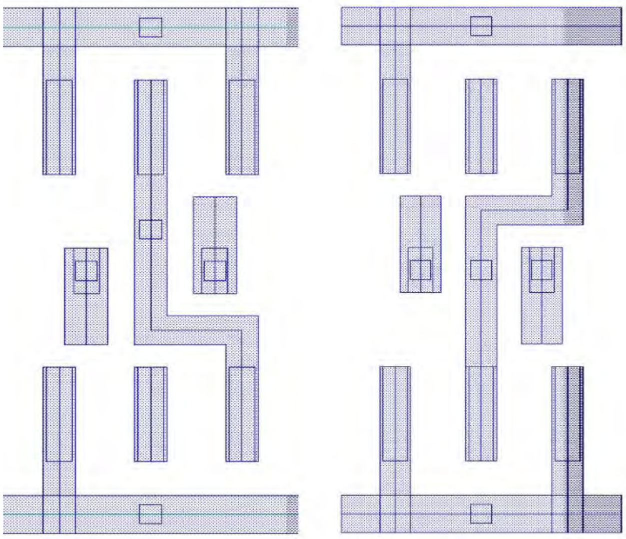


Figure 19: Conventional Gates Metal Routing

In Figure 4.6 and Figure 4.7, it is visible that the Metal 1 bending is removed. It is now straight connection. Internal connection is done with Metal 2. That's why, we don't see any kind of bending metal and it is possible to keep safe the design from the intruders.

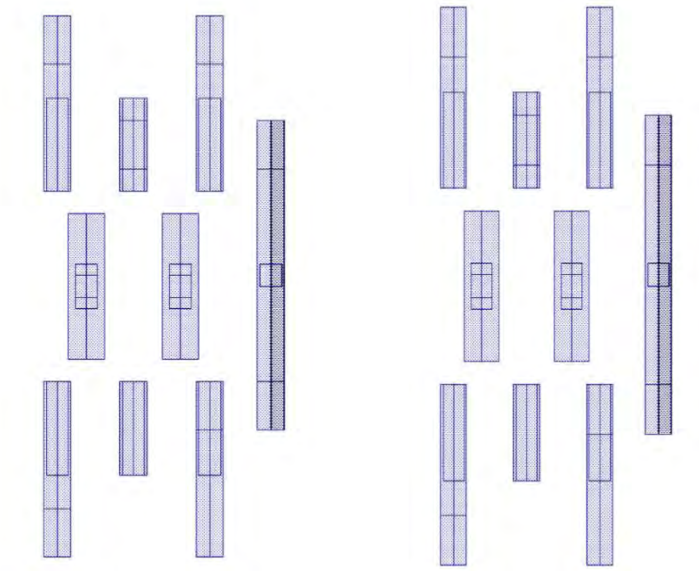


Figure 20: Proposed Camouflaged Gates Metal 1 Routing

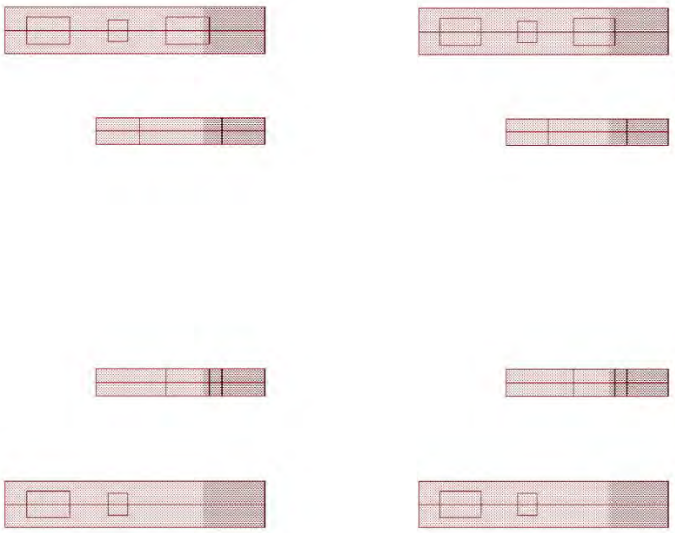


Figure 217: Proposed Camouflaged Gates Metal 2 Routing

In Figure 4.8, we can see only the VIA connections are different.

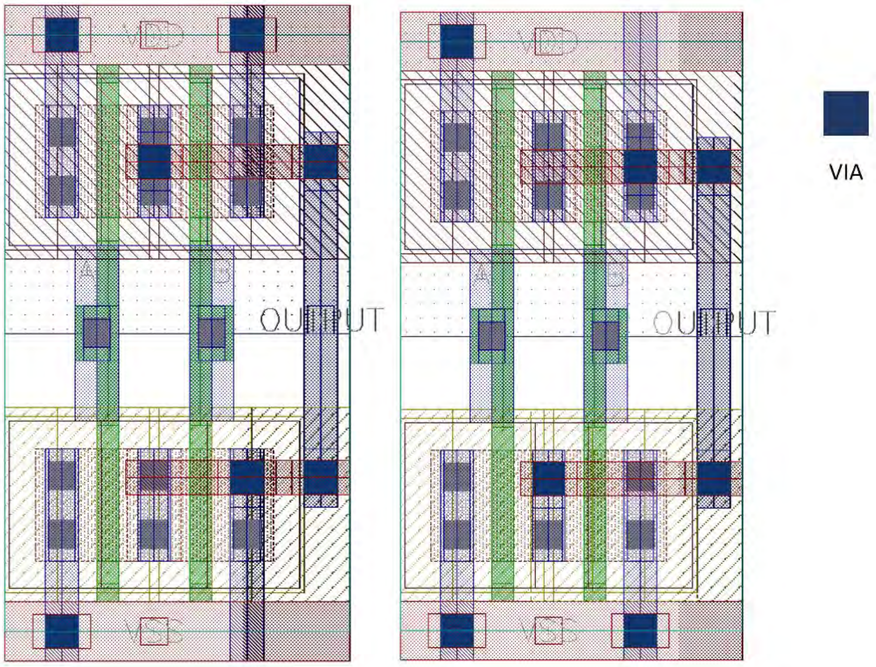


Figure 22: Proposed camouflaged gates difference is VIA positions.

As per our previous discussion, the only differences are visible in the Figure 4.8. The deep blue colored VIA placements are the only differences here.

4.4 XOR Design using both Conventional Design and Camouflaged Design

Figure 4.9 shows the schematic of the XOR gate. This gate is selected to see the effects of the circuit designed with the proposed camouflaged concept. Figure 4.10 shows the simulation result and Figure 4.13 shows the post layout simulation results.

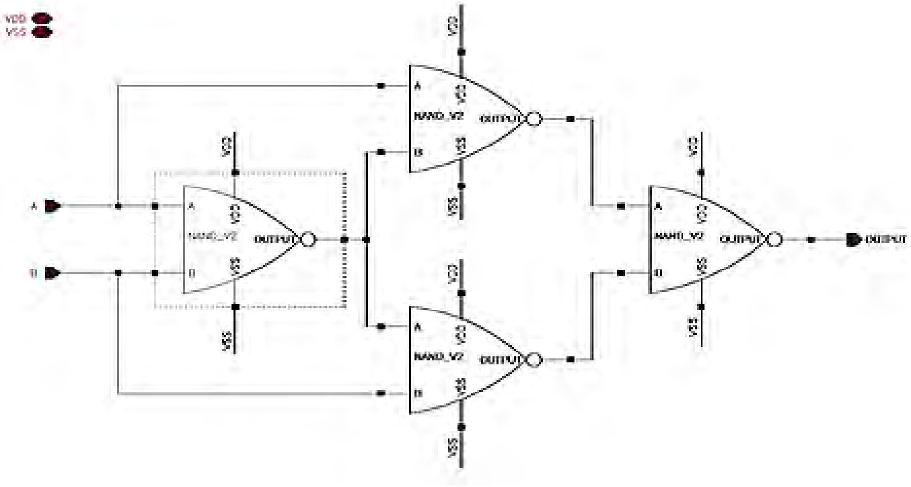


Figure 23: XOR Schematic Design

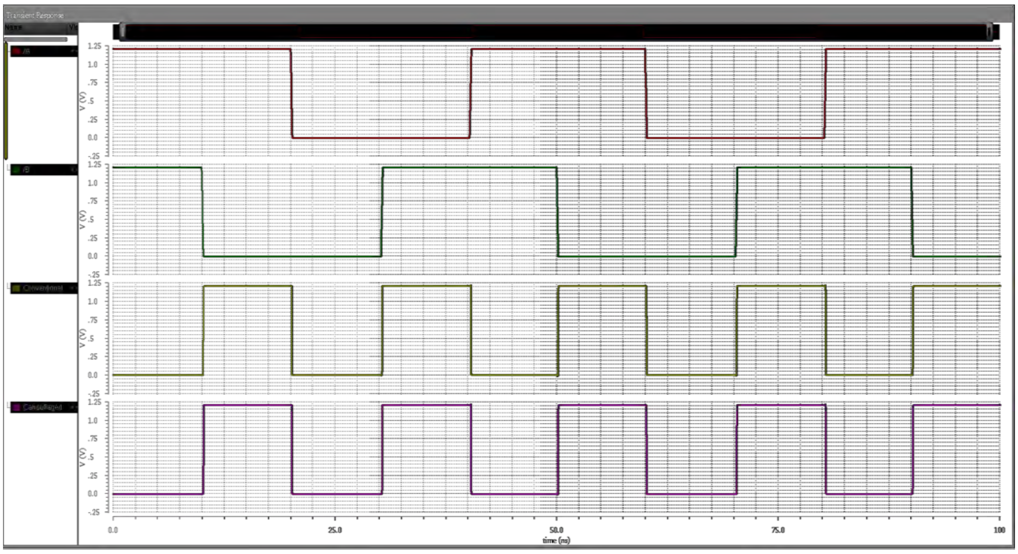


Figure 24: XOR Circuit Simulation Result

Figure 4.11 is the complete XOR design using camouflaged universal gates. On the other hand, Figure 4.12 is the XOR gate physical layout design using conventional gates. Table 4.1 depicts the post layout simulation result comparison where we 17.37% area increase and 1.357ps delay increase.

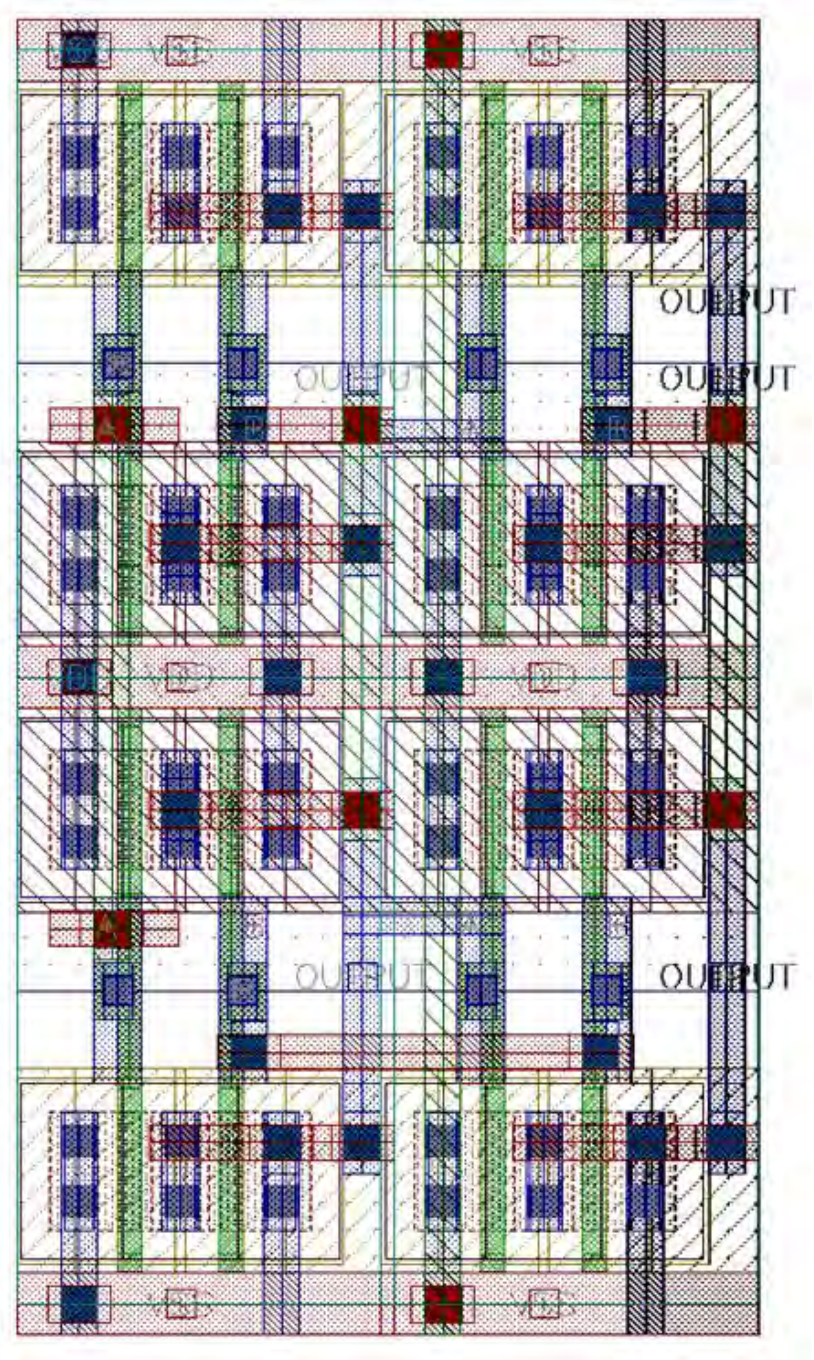


Figure 25: XOR Gate Using Camouflaged Gates

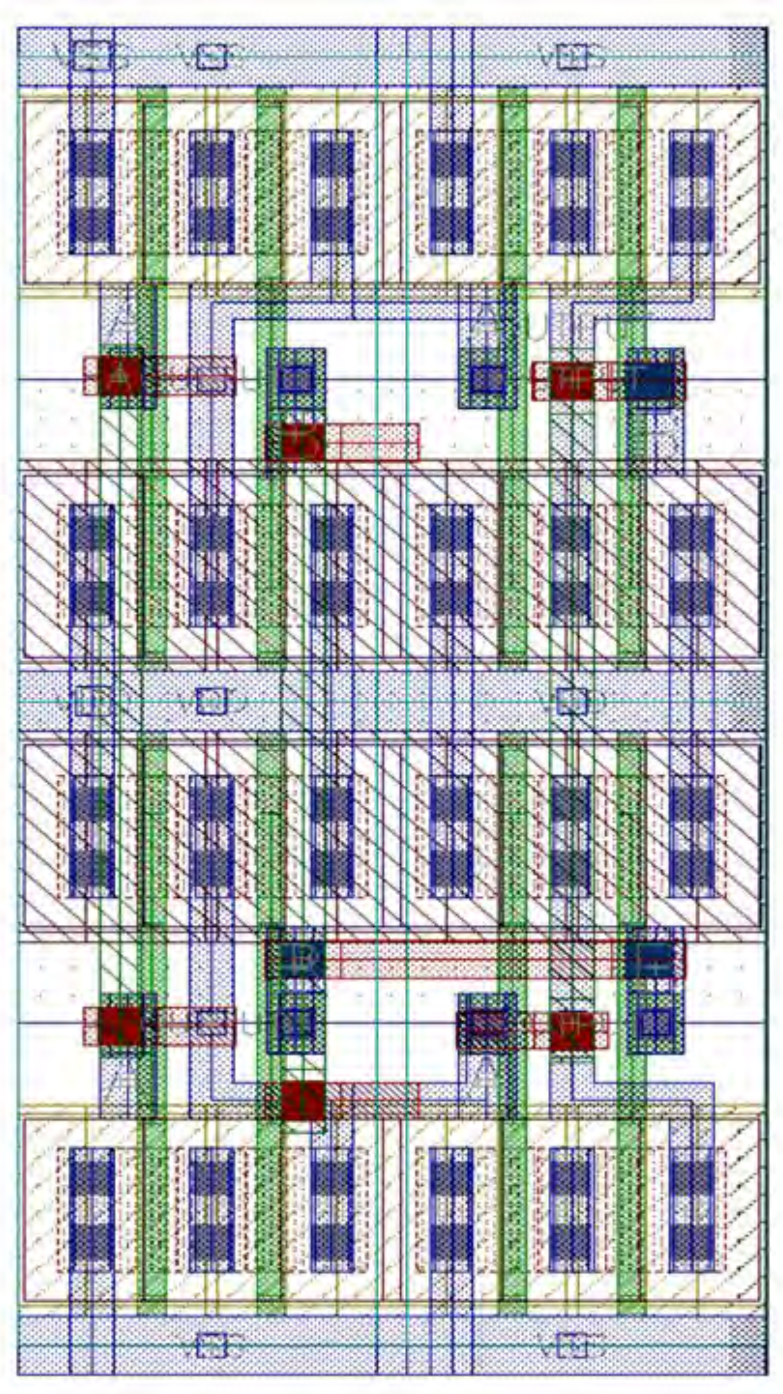


Figure 26: XOR Gate Using Conventional Gates

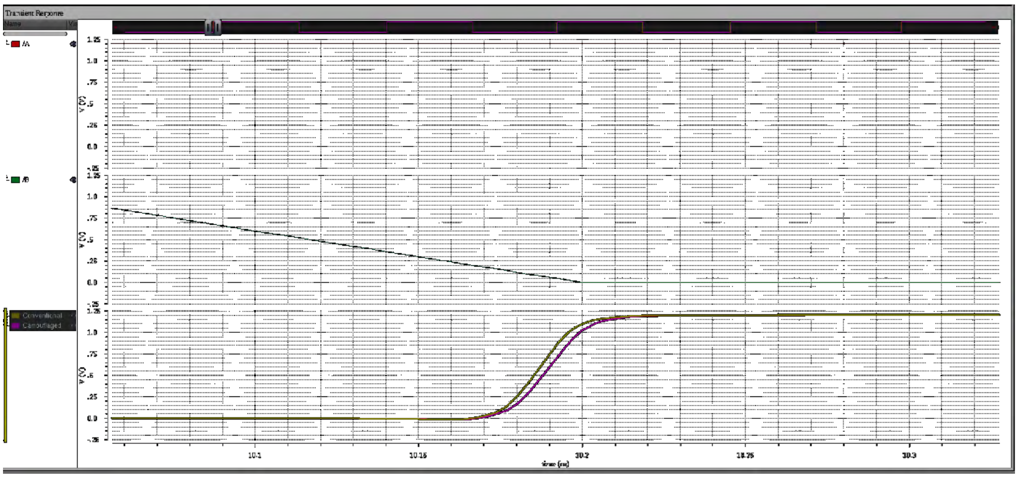


Figure 27: XOR Post Layout Simulation Result

Table 4.1: Comparison Analysis between XOR Conventional Design & XOR Camouflaged Design

Designs	**Schematic**	**Conventional Layout**	**Camouflaged Layout**	**Difference**
Metal Hierarchy Used	N/A	M1, M2, M3	M1, M2, M3	
Area	N/A	2.62 X 5.54	3.075 X 5.54	17.37% Increase
Pre Layout Simulation delay	26.47435ps	N/A	N/A	
RC Extraction delay	N/A	32.7456ps	34.10262ps	1.357ps Increase

4.5 Discussion

True/Dummy contact based camouflaging is very popular strategy. In this project, this concept is incorporated with a small modifications in the layout design. In Figure 4.14, the red colored boxes are the differences between two gates. We can implement True/Dummy concept to make similar VIA locations.

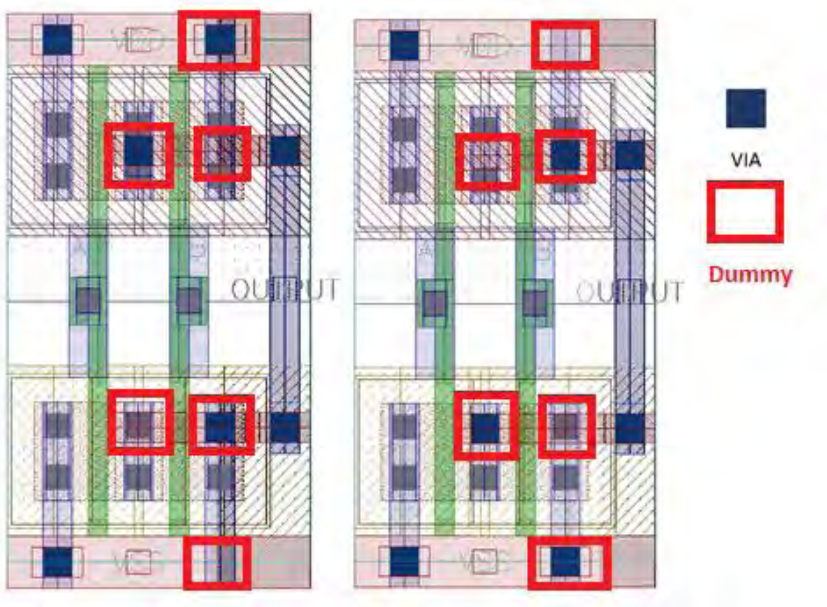


Figure 28: Incorporating with True/Dummy Concept

So, using the both approach 1) modifications in the layout design and 2) Incorporating with True/Dummy contact technique, we're getting more compact design. This is much better than only True/Dummy contact approach as we can see in Figure 2.3 only True/Dummy approach takes a wider area to implement. In the proposed design, area is taking less, and if it's incorporated with True/Dummy concept as illustrated in Figure 2.4, it's not possible to figure out the exact design by the attackers through Scanning Electron Microscopy (SEM) Images.

Considering the True/Dummy contact technique, both NAND gate and NOR gate can be designed with a single gate. If we need NAND or NOR gate, we can put the thin layer to disconnect physical connections of VIA where we don't need.

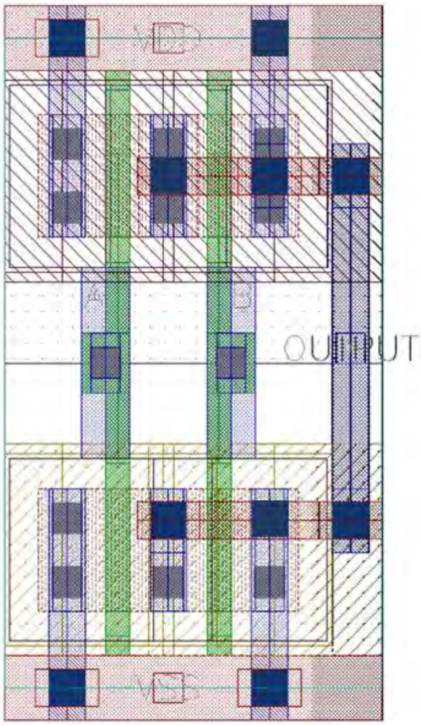


Figure 29: Final Common Gate for both NAND gate and NOR gate.

Figure 4.15 depicts the single gate that we can use both as NAND and NOR gate. With the camouflaging technique modifications are done in layout. And with the application of True/Dummy contact concept the whole design gets a unified shape.

Chapter 5: Conclusion

It’s not possible to stop the attacker from hacking the chip and excluding logic and data. But, it might be possible to reduce the damages of the chip design and manufacturer companies through applying camouflaging techniques. The whole idea was to improve the way of designing circuit in physical level with minimum effort considering the cost of manufacturing. The whole plan was to complete a full standard cell library so that all the logic gates remain there to design any kind of complex chip using the IC camouflaging concept. Initially, universal gates are selected to implement the proposed techniques and see the differences between proposed design and conventional design. Then, a larger logic gate is designed using these proposed designs to see how the concept works in practical implementation. First of all, an attempt is taken to change in the conventional design whether it’s possible to make both gates almost similar. That is possible as per the result and discussion. After implementing that, VIA looks different for the both gates. Then, an attempt is taken to implement True/Dummy concept. After incorporating it with the design modifications it is possible to make both universal gates 100% similar.

5.1 Limitations

In many cases camouflaging techniques increases the area, reduces the performance but it’s a matter of trading of for the companies. If they can allow reduced performance and save their design from being pirated then it could be good option for them. Where higher performance is first priority, camouflaging might not be a good option for the companies.

Due to unavailability of industry grade library and technology files, it’s not possible claim real time data. And, due to shortage of time, only universal gates are done. Using those gates a bigger logic gate is implemented to check the effects of using camouflaged gates instead of conventional ones.

As we know camouflaging technique demand less performance as it takes extra area, additional power consumptions and delay. Considering those effects design is done and we can see in Table 4.1, the overall performance degrades. Despite having lower performance company is sometimes willing to implement camouflaging technique to minimize the circuit and IP. For the protection of these IPs when intruder tries to leak circuit information through image processing will work better.

5.2 Future Works

Only NAND, NOR and XOR gates are included in the library at this moment and in future the library will be enriched with rest of the gates. All the implementation part has been done using an open source PDK with process technology 90nm. To make it more feasible for industry grade application, professional PDK would help to make it more professional considering the parasitic extraction, delay calculation and related data. So, this concept could be applied in any other professional PDK and lower process technology and could be possible to get more accurate data for practical applications. Dynamic camouflaging has been introduced already [12]. So, there would be a possibility to implement these design techniques on that concept.

References

1. Y. Feng, J. Wu, and P. He, "*Global M&A and the Development of the IC Industry Ecosystem in China: What Can We Learn from the Case of Tsinghua Unigroup?"* Journal of Sustainability, 2018.

2. J. Rajendrany, O. Sinanogluz, and R. Karriy, "*VLSI Testing based Security Metric for IC Camouflaging*," INTERNATIONAL TEST CONFERENCE, 2013.

3. B. Liu, and B. Wang, *"Embedded Reconfigurable Logic for ASIC Design Obfuscation Against Supply Chain Attacks,"* Conference of Design, Automation and Test in Europe, 2014.

4. M. Li, K. Shamsi, T. Meade, Z. Zhao, B. Yu, Y. Jin, and D. Z. Pan, "*Provably Secure Camouflaging Strategy for IC Protection*," IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, 2017.

5. B. Liu, and B. Wang, *"Reconfiguration-Based VLSI Design for Security,"* IEEE JOURNAL ON EMERGING AND SELECTED TOPICS IN CIRCUITS AND SYSTEMS, 2014.

6. J. Rajendran, and M. Sam, *"Security Analysis of Integrated Circuit Camouflaging,"* in Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security, Berlin, Germany, 2013.

7. X. Wang, M. Gao, Q. Zhou, Y. Cai, and G. Qu, *"Gate Camouflaging-Based Obfuscation,"* Springer International Publishing, 2017

8. E. Oriero, and S. R. Hasan, *"Survey on recent counterfeit IC detection techniques and future research directions,"* Elsevier Integration, vol. 66, 2019.

9. C. Yan, J. Dofe, S. Kontak, Q. Yu, and E. Salman, *"Hardware-Efficient Logic Camouflaging for Monolithic 3-D ICs,"* IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS, vol. 65, 2018.

10. X. Y. Wang, Q. Zhou, Y. C. Cai, and G. Qu, *"Spear and Shield: Evolution of Integrated Circuit Camouflaging,"* JOURNAL OF COMPUTER SCIENCE AND TECHNOLOGY, 2018.

11. S. Malik, G. T. Becker, C. Paar, and W. P. Burleson, *"Development of a Layout-Level Hardware Obfuscation Tool,".*

12. N. Rangarajan, S. Patnaik, J. Knechtel, R. Karri, O. Sinanoglu and S. Rakheja, *"Opening the Doors to Dynamic Camouflaging: Harnessing the Poer of Polymorphic Devices"* IEEE TRANSACTIONS ON EMERGING TOPICS IN COMPUTING, 2020.

13. *Virtuoso Layout Suit.* Cadence. https://www.cadence.com/en_US/home/tools/custom-ic-analog-rf-design/layout-design/virtuoso-layout-suite.html