Security of Integrated Circuits Physical Design in 45 NM Technology

M.VINOD KUMAR[1], G.VENKATA RAO[2]

[1]Student Department of Electronics and Communication Engineering Lakireddy Balireddy College of Engineering, Mylavaram

[2]Associate professor Department of Electronics and Communication Engineering Lakireddy Bali reddy College of Engineering, Mylavaram

Abstract: Camouflaging is a configuration level frame works that hampers an aggressor from reverse engineering by showing, in one exemplification, dummy contacts into the design. By utilizing a blend of genuine and dummy contacts, one can cover a standard cell whose usefulness can be one of numerous. On the off chance that an assailant can't resolve the usefulness of a disguised entryway, he/she will extricate a wrong netlist. In this paper, we break down the possibility of recognizing the usefulness of covered entryways. We moreover propose system to achieve based IC camouflaging procedure strong to reverse engineering. Moreover, we prudently select doors to cover by utilizing procedures which guarantee that the yields of the extricated netlist are controllably undermined utilizing 45 um Cadence technology**.** We moreover propose system to achieve area, power and delay.

Keywords: *IC Camouflaging, IC Reverse engineering, Dummy contacts, Security*

I. INTRODUCTION

1.1 Reverse engineering of Integrated Circuits (IC$_s$)

The present development identifies with frameworks and techniques for shielding printed circuits from reverse engineering and specifically to a framework and strategy for camouflaging a standard cell based integrated circuit. Reverse engineering of an IC is a procedure of recognizing its structure, outline and usefulness. Generally, reverse engineering of IC's has been performed to gather focused insight, to confirm an outline, and to check for business robbery and patent encroachments.

Reverse engineering, likewise got back to engineering, is the procedures of extricating learning or plan data from anything man-made and imitating it or recreating anything in light of the separated data. The procedure frequently includes dismantling something (a mechanical gadget, electronic part, PC program, or natural, synthetic, or natural issue) and dissecting its segments and workings in detail.

The reasons and objectives for getting such data shift generally from ordinary or socially useful activities, to criminal activities, contingent on the circumstance. Regularly no licensed innovation rights are broken, for example, when a man or business can't recall how something was done, or what something does, and needs to reverse architect it to work it out for themselves. Reverse Engineering is additionally helpful in wrongdoing anticipation, where malware speculated is reverse designed to comprehend what it does, and how to identify and evacuate it, and to enable PCs and gadgets to cooperate ("interoperate") and to enable spared records on out of date frameworks to be utilized as a part of more up to date frameworks. By differentiate, reverse engineering can likewise be utilized to "break" programming and media to expel their duplicate assurance or to make a (potentially enhanced) duplicate or even a knockoff; this is generally the objective of a component.

• **Identify the device technology**: It is used to identify the technology of integrated circuits(IC)

•**Extract**: The integrated circuits are in gate level netlist

•**infer the functionality**: Reverse engineering on Apple's processor revealed the type of graphic processing units used in iPhone 5.

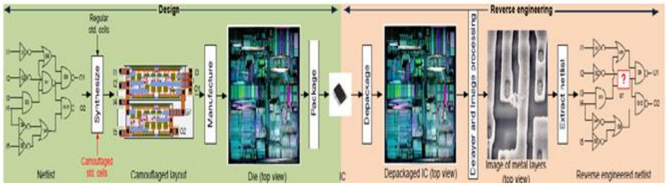


Fig.1: Reverse engineering process of integrated circuits

1.2. IC camouflaging to reverse engineering:

Camouflaging is a layout level technique to mix real and dummy contacts to the layout.

In one exemplification of IC camouflaging, the formats of logic gates are intended to appear to be indistinguishable, bringing about an off base ex-footing. For instance, the format of normal NAND cell (Figure2 (a) NAND and NOR Figure2 (b)) cell appear to be unique and are thus simple to reverse architect. Be that as it may, the design of covered NAND cell (Figure 2(c)) and NOR cell (Figure 2(d)) appear to be indistinguishable and are hard to separate. At the point when misdirected into mistakenly deciphering the usefulness of the disguised gate, the assailant may get a reverse designed netlist that is unique in relation to the first. The netlist got by an aggressor is the deluding netlist where the usefulness of the disguised gates are discretionarily as-marked.

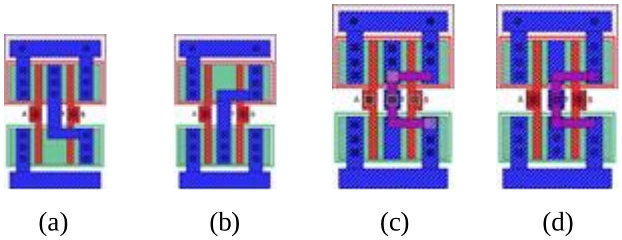


Fig.2: (a) NAND gate layout (b) NOR gate layout (c) camouflaged NAND layout (d) camouflaged nor layout

Figure 2 demonstrates how camouflaging ensures an IC plan against reverse engineering. A creator covers certain gates in the design 2. For instance, the NAND gate, in Figure 2 is camouflaged. This plan with covered gates is then fabricated at a foundry. The fabricated IC is sold in the market. An assailant reverse architects an IC by depackaging, delayering, imaging the layers, and extricating the netlist. Notwithstanding, in the removed netlist, the usefulness of the disguised gates are obscure. For example, in Figure 2, the usefulness of is obscure. An assailant doles out a discretionary two-input capacity to it. Thusly, he may get an off base netlist.

To upset reverse engineering of an IC, any camouflaging technique needs to give the accompanying assurances.

(1) Flexibility to reverse engineering: An aggressor ought not to have the capacity to distinguish the usefulness of a covered gate.

(2) Undermined outputs: The outputs of the first and the deceiving netlists ought to be controllably extraordinary.

In this paper, we examine the achievability of distinguishing the functionality of the covered gates. We propose an IC camouflaging strategy that is strong to reverse engineering. Besides, we sensibly select gates to cover by utilizing strategies which guarantee that the outputs of the deluding netlist are controllably corrupted.

II. EXISTING SYSTEM

Standard cells play out a rationale work and are utilized as building hinders in planning ICs. By utilizing a blend of genuine and dummy reaches, one can plan a standard cell whose usefulness can be one of numerous. The genuine contacts direct the usefulness of a camouflaged gates. The utilization of optical and electrical microscopy will neglect to recognize the concealed usefulness as they can't separate amongst genuine and dummy contacts, muddling figuring out. The more functionalities a camouflaged standard cell could actualize, the more troublesome the figuring out progresses toward becoming. It is basic for a camouflaged standard cell to have an extensive number of transistors that can be associated in various approaches to acknowledge diverse rationale capacities. Of the considerable number of cells in the standard cell library, XOR and XNOR doors have the most elevated number of transistors. Henceforth, we alter the format of XOR and XNOR gates for camouflaging.

In this existing technique camouflaging circuit, in the place of camouflaging circuits c1, c2 used XOR, NAND and NOR circuits. But designing of NAND, NOR and XOR using 12 transistors in schematic level. So, the circuit requires more power, area and delay.

- Reverse engineering that can resolve the functionality of the camouflaged gates,
- A metric to measure the hardness of reverse engineering,
- First technique to select the gates in a design to camouflage so that the functionality of the camouflaged gates can only be resolved by brute force,
- A second technique to select the gates to camouflage such that the deceiving netlist produces outputs which are controllably different from those of the original netlist, and
- Evaluation of the proposed attack and defense techniques on.

A reverse engineer may face the following difficulties.

Difficulty 1: Delayering the lower metal layers (M1 and M2) is difficult as compared to delayering higher metal layers (M3 and above) because lower metal layers are only a few tens of nanometers thick. Hence, a reverse engineer has to precisely control the strength of the chemicals used for delayering. Notwithstanding this difficulty, reverse engineers have successfully extracted information from the lower metal layers

Difficulty 2: A reverse engineer can try to differentiate between a true and a dummy contact by slicing the die and imaging the side view. However, there are hundreds of millions of contacts in an IC and an attacker has to slice the IC into million pieces to classify all of them. Hence, such reverse engineering will not be feasible.

Difficulty 3: A reverse engineer can use anisotropic techniques like reactive-ion etching to partially etch the layers. However, on using such techniques for top-down reverse engineering

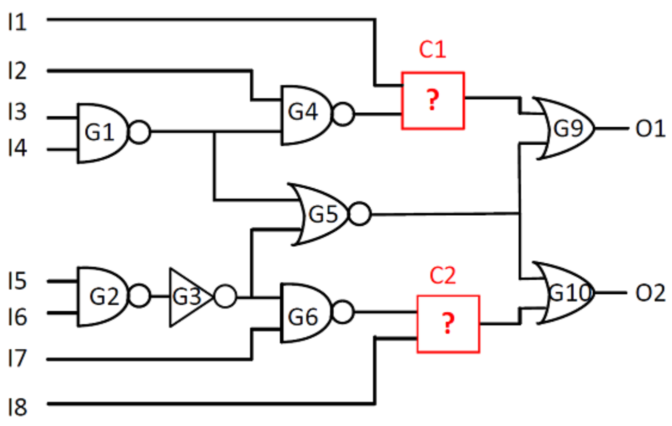


Figure 3: block diagram of the circuit, c1 c2 are camouflaging gates

III. PROPOSED SYSTEM AND IMPLEMENTATION

The proposed technique, An Integrated Circuit (IC) can be reverse built by imaging its configuration and reproducing the netlist. IC camouflaging is a format level procedure that hampers imaging-based reverse engineering by utilizing, in one epitome, practically extraordinary standard cells that carbon copy. Reverse engineering will fizzle if the usefulness of a camouflaged gate can't be effectively settled. We adjust VLSI testing standards (justification and refinement) to evaluate the capacity of a reverse engineer to unambiguously resolve the usefulness of carbon copy camouflaged gates.

In the proposed technique is camouflaging technique in the block diagram of camouflaging circuit has c1, c2 .this are replaced with NAND, NOR, XOR and NOR are normally gates using four transistors. In XOR gate using 12 transistors. So using this technique reduced power, area and delay. We are proposing hope tool for fault simulation for input patterns of schematic level.

We are design camouflaging circuits of block diagram and after complete layouts (LVS) layout verses schematic and my proposed paper is to reduce the area, power and delay.

3.1 IC camouflaging circuit replacing with XOR, NAND and NOR gates.

In the proposed system fig 3 we are replacing c1, c2 blocks with few logic gates like XOR, NAND and NOR as shown in fig 4.1, 4.2, 4.3. With the help of this gate we are modifying the existing camouflaging circuit. Camouflaging is a layout based technique and adding of dummy contacts to the layouts for the high security reasons. In device level input patterns are applying by using fault simulation process for high security purpose.

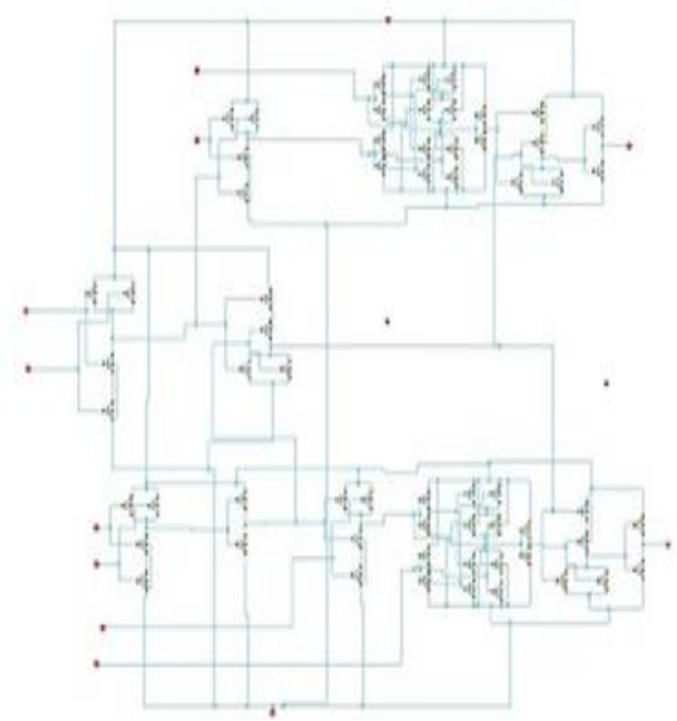


Fig.4.1 camouflaging c1, c2 replaced with XOR gate

At well as c1, c2 replaced with NAND and NOR gate also.

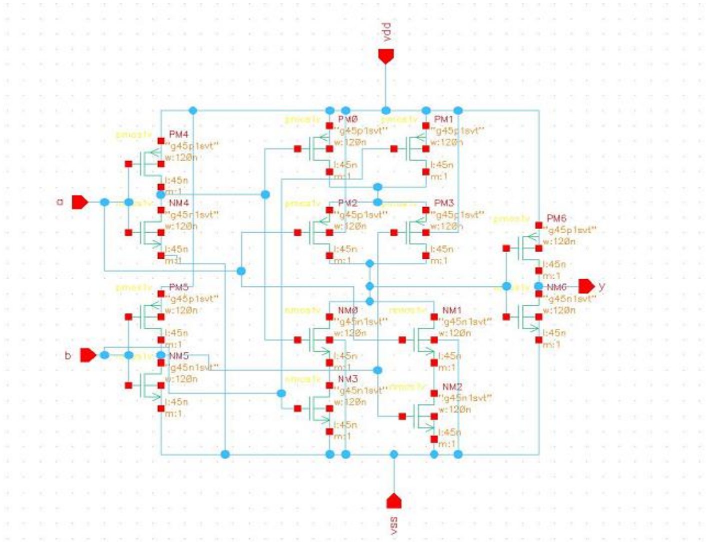


Fig.4.2 normal XOR gate schematic

Conventional XOR gate designs with 12 transistors.

As well as we design with NAND, NOR gates let's see in this below figures.

Normal NAND and NOR gates used in this paper.

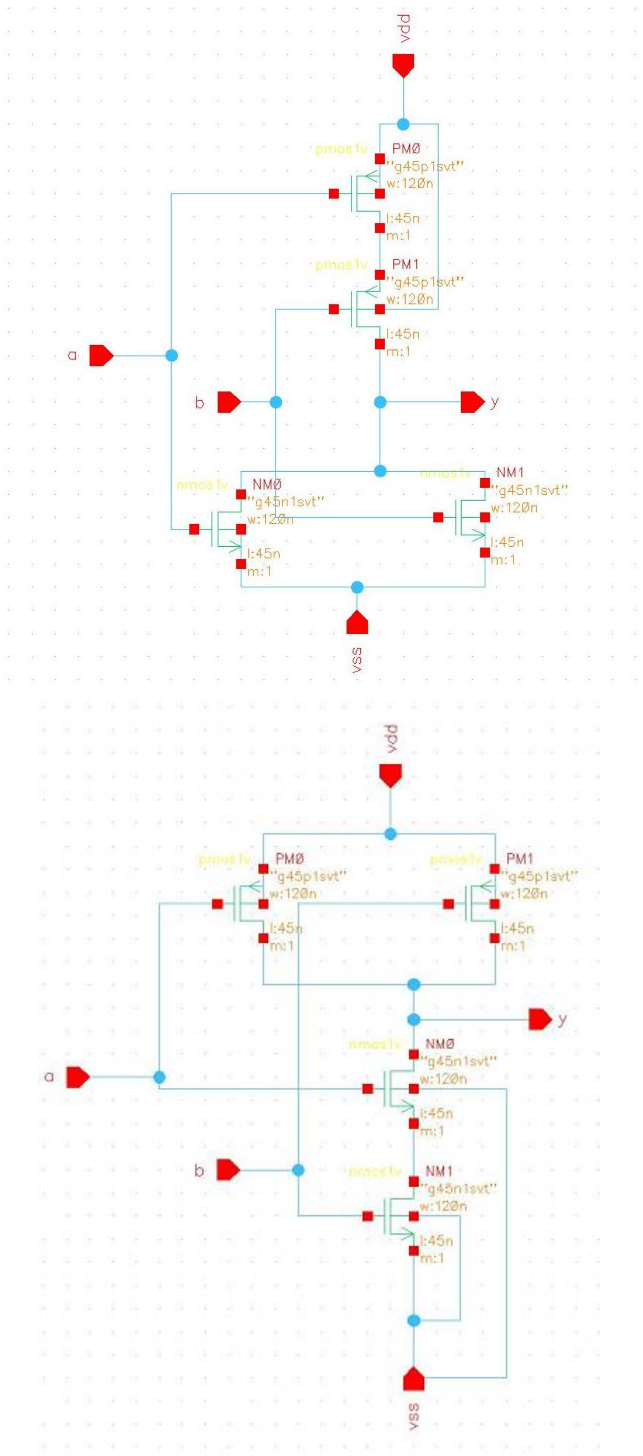


Fig.4.3 NAND and NOR, gate design

3.2. Working operation of IC camouflaging circuit.

Consider the disguised gate C1 in Figure 3.

The usefulness of C1 can be made arrangements to be XOR by applying '010XXXX' at the inputs. This information example will legitimize the inputs of C1 to '00' and hones the yield of C1 to O1. If O1 is '0', by then the usefulness of C1 is settled as XOR. Something unique, the usefulness of C1 can be embarked to be NOR by applying '110XXXX' at the inputs. This info example will legitimize the inputs of C1 to '10' and hone the yield of C1 to O1. In case O1 is '0', by then the usefulness of C1 is settled as NOR. Something unique, the usefulness of C1 is settled as NAND.

Applying c1 and c2 same gates and different gate also but we get same outputs .this is for verification process.

After design the schematic diagram of all camouflaging circuits , like XOR camouflaging, NAND camouflaging and NOR camouflaging circuits

By applying '010XXXX' to the circuit of figure 4.1 and by applying '110XXXX' to the circuit of figure 4.1 we get some outputs like this waveforms.

IV. RESULTS

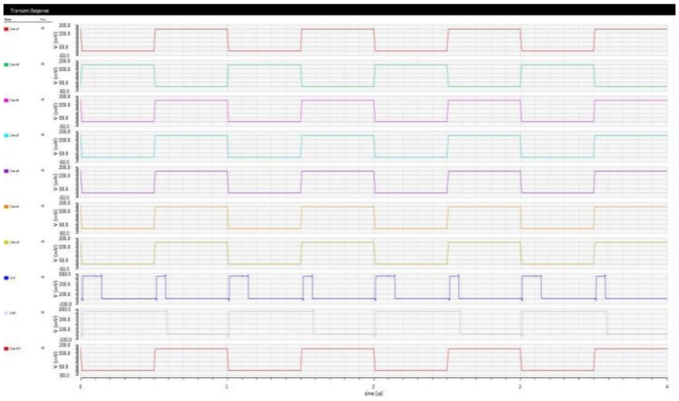


Fig.5.1 XOR Camouflaging wave forms

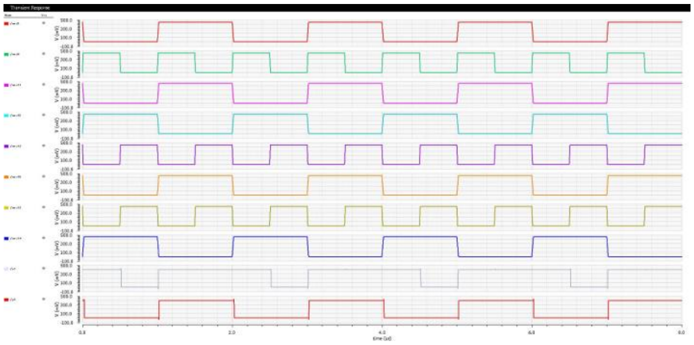


Fig.5.2 NAND Camouflaging wave forms

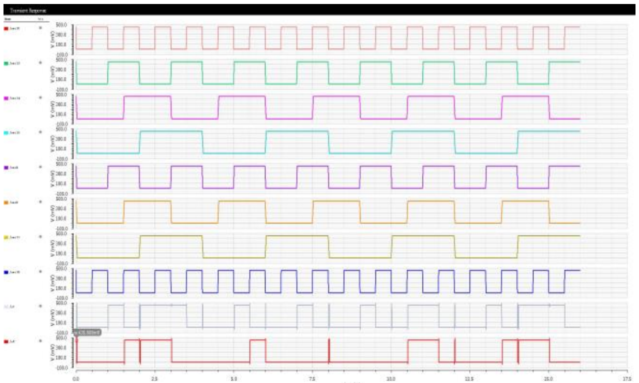


Fig.5.3 NOR camouflaging wave forms

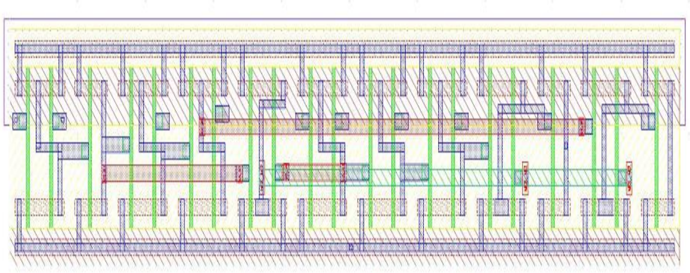


Fig.5.4 NAND camouflaging Layout

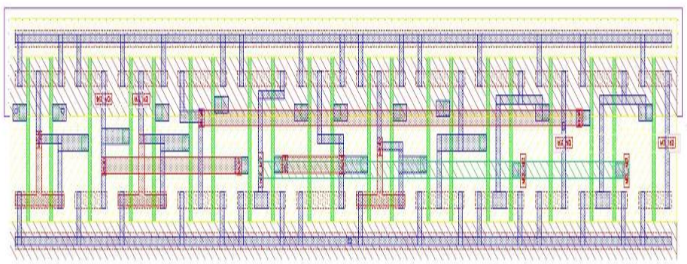


Fig.5.5 NOR camouflaging Layout.

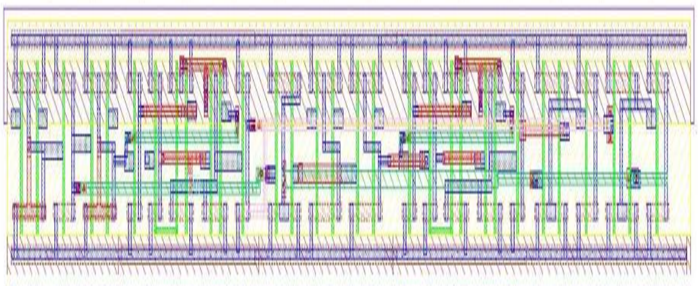


Fig.5.6 XOR Camouflaging layout.

Figures 5.4, 5.5 and 5.6 are layouts of camouflaging circuits and in side layouts added dummy contacts. It means these are acting like no connection between the two layers but these are stretching with
Dummy contacts

V. PERFORMANCE & DIFFERENCE BETWEEN EXISTING AND PROPOSED SYSTEM

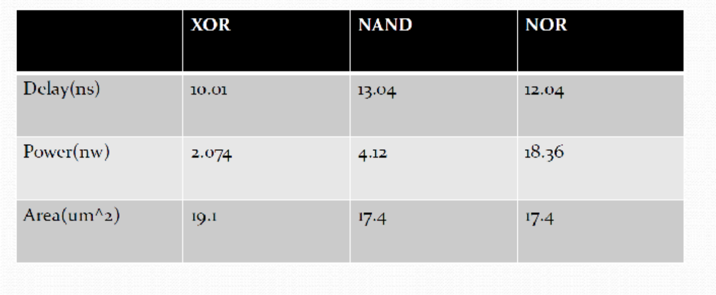
6.1 Performance of exiting technique

The performance of exiting technique has taking high power, more delay and area in Nano meters.

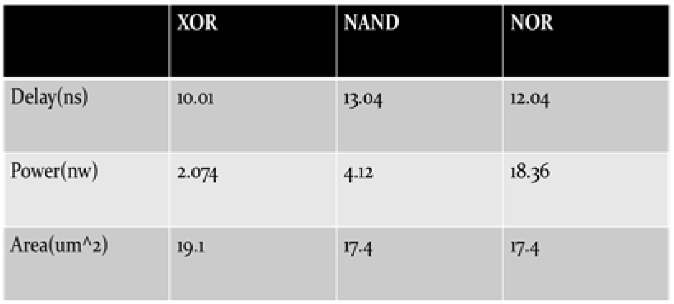
Table 1 shows that performance of camouflaging technique.

Function	Camouflaged gate					
	XOR+NAND+NOR			XNOR+NAND+NOR		
	Power	Delay	Area	Power	Delay	Area
NAND	5.5X	1.6X	4X	5.1X	1.8X	4X
NOR	5.1X	1.1X	4X	4.8X	1.4X	4X
XOR	0.8X	0	1.2X	N/A		
XNOR	N/A			0.7X	0	1.2X

6.2 Performance of proposed camouflaging technique



	XOR	NAND	NOR
Delay(ns)	10.01	13.04	12.04
Power(nw)	2.074	4.12	18.36
Area(um^2)	19.1	17.4	17.4



	XOR	NAND	NOR
Delay(ns)	10.01	13.04	12.04
Power(nw)	2.074	4.12	18.36
Area(um^2)	19.1	17.4	17.4

Table 2 shows that performance of proposed camouflaging technique results.

The proposed technique of camouflaging show low power, decreased delay and area decreased to Nano meter to micro meters as per the existing technique

VI. CONCLUSION AND FUTURE SCOPE

Although dummy contact-based IC camouflaging is a successful format level strategy against reverse engineering, it is powerless when the camouflaged gates are detached and are completely resolvable. While a creator can disguise every one of the gates, it brings about power, delay and power overheads. We demonstrate that camouflaging can be reinforced by sensibly choosing the gates in the plan to cover, without acquiring much overhead. The proposed systems depend on resolvability and corruptibility measurements that convey camouflaging arrangements which are flexible to reverse engineering. Along these lines the aggressor is compelled to do brute force. While we defined these security Prerequisites as imperatives for automatic test pattern generation (ATPG) tools, one reason additionally utilize SAT based ATPG and identicalness checking apparatuses exist to manage choice of gates for IC camouflaging. Reverse engineering ends up noticeably confused when other camouflaging procedures. For example, programmable cells what's more, dummy filler cells are utilized as a piece of conjunction with dummy contacts. The proposed security metric can be utilized to assess the quality of these camouflaging procedures either separately or, on the other hand when consolidated.

VII. REFERENCES

[1]. Chip works documentation of transformed chip works Intel 22 nm

[2]. R.Torrance and D.james, “the best state of fig in semiconductors reverse engineering “. In the process.

[3]. Extrame tech, “iPhone 5 A6 SoC Reverse engineering figure out, uncovers uncommon handmade custom cpu and tri gate gpu “.

[4]. Silicon Zoo,”the layman’s layout manual for ic figuring out”.

[5]. Chip work,”figuring out programing “, specialized focused eximination /assets/reveres engineering process.

[6]. Degate documentation in online

[7]. 7.”Sequrity analysis of integrated circuits in camouflaging technique” in the process of reverse engineering

[8]. Semi Ädvanced is in danger as semiconductors gear and material industry loses up to $4 bilion every year because of IP encroachments”

[9]. SypherMedia,”Syphermedia library circuit over innovation”, solutions.hm.

[10]. J.P.Baukus, L.W.Chow, R.P.Cocchi, and B.J.Wang,”technique and contraption for covering a standed cell based incorporated circuit with miniaturized scale circuits and posts preparing “.

[11]. J.P. Baukus, L.W.Chow, R.P.Cocchi, and “building obstruct for a safe cmos rational cell library “.

[12]. J.P. Baukus, L.W.Chow, R.P.Cocchi, and incorporated circuits ensured against figuring out and strategy for creating a similar utilizing a clear metal contact line ending on field oxide “.

[13]. 13.”Sun Microsystems, opensparc T1 process”

[14]. 14. J.P. Baukus, L.W.Chow, R.P.Cocchi, p.ouyang and B.J.wang,’disguising a standard cells based coordinated circuits”.

[15]. 15. M.L.Bushnell and V.D.Agrawal,” Basic of electronic testing for digital memory , mixed signal VLSI circuit testing”.

M.VINOD KUMAR
Student Department of Electronics and Communication Engineering Lakireddy Balireddy College of engineering, Autonomous (Approved by AICTE, New Delhi, Affiliated to JNTUK), Mylavaram, pin 521230

G.VENKATA RAO
Associate professor Department of Electronics and Communication Engineering Lakireddy Balireddy College of engineering, Autonomous (Approved by AICTE, New Delhi, Affiliated to JNTUK), Mylavaram, pin 521230