Journal of Graphic Era University
Vol. 4, Issue 2, 72-83, 2016
ISSN: 0975-1416 (Print)

Advanced Digital Organic Vehicle Security System

Arun Pratap Singh Rathod[1], Poornima Mittal[1], Brijesh Kumar[2]

[1]Department of Electronics & Communication Engineering, School of Engineering and Technology
Graphic Era University, Dehradun 248002, Uttarakhand, India
[2]Departemnt of Electronics and Communication Engineering
M. M. M. University of Technology Gorakhpur-273010, Uttar Pradesh, India
Corresponding author: brijesh_ece@mmmut.ac.in

Abstract
This paper is about presenting an economical and simple vehicle security system by which a vehicle can identify its user and provide security against any unauthorized access to the vehicle. In this paper we have designed and implemented a simple digital interface (DI) at the front end which when placed between car battery and ignition system it makes the vehicle smart enough to identify its user with help of a security PIN. Further this vehicle system utilizes organic transistors which itself are quite innovative and widely used as alternative to conventional MOSFETs for cost efficient applications. Here too we have utilized them to make DI economical in cost and robust in nature to overcome much troubled issue of modern times i.e. stealing of vehicles with or without vehicle keys.

Keywords- Security system, Organic, OTFT, Digital interface, FPGA.

1. Introduction

Vehicles in contemporary world serve as the life-line of every society. The word ‘globalization’ has turned in to reality only because of fast moving automobiles. Vehicles not only connect us but also cut short the idol time between the destinations. Therefore, they have proved to be one of the precious belongings of their respective owner. Now when we declare something precious by default we have to its security. For that purpose, we use security systems to keep are vehicle safe.

Question which has to be considered now that if we are already utilizing different security system to secure our vehicle then how it is that vehicles are still being stolen so readily. Therefore, there is a need to look in to the working of an automobile generally car and find out where we lacking in providing security to our vehicle. So in this paper we have tried to present a new kind of security of system which provides security to the vehicle even if someone makes an unauthorized access by stealing the original keys. Moreover, this vehicle security system (VSS) implementation also emphasizes on importance of organic electronics in digital design. Therefore, a cylindrical organic thin film transistor (OTFT) is analytically modeled, simulated and analyzed so that it can be proposed as the transistor of choice for the DI implementation. (Voge, 1933; McMahon, 2013; Alrabady, 2005; Pedroni, 2004; Roth, 1998; Bakhshi, 2004; Klauk, 2006; Kumar, 2014; Kumar, 2013; Locci, 2007; Locci, 2009).

Journal of Graphic Era University
Vol. 4, Issue 2, 72-83, 2016
ISSN: 0975-1416 (Print)

2. Motivation

A security system is an integral of a car these days. Without them cars are vulnerable of burglary and thefts. So it is highly important these days that every car should have one. We observe from Figure 1 that the ignition system of a normal car is comprised of a battery, a contactor (i.e. key), an ignition coil, spark plugs, contact breaker and distributor. Battery is the source which provides power to the ignition coil. The circuit between the battery and ignition coil is completed by inserting a 'key'. As the circuit is completed the current moves from battery to ignition coil and from there it is directed to other parts of the ignition system where it is required to start the engine. It is clear from the Figure 1 that the 'KEY' is just acting as a switch between car battery and ignition coil. If the circuit is completed with or without 'KEY' (which mostly happens when thieves manually connect battery to ignition coil directly through wires bypassing the KEY), the car will start.

This is the loophole which is exploited time and again to steal the cars because car or more precisely its ignition system cannot differentiate between the users if the genuine or original keys are used after stealing. As there is no security measure other than the key that could prevent the starting of the engine. So to tackle this problem a digital interface is proposed in this paper, which will provide additional security to the cars and prevent the starting of the engine until a correct code is fed. Here is an attempt to design a unique security system which takes the car security to unexplored levels. This security system is basically a digital interface which isolates the battery current from ignition coil until the right password combination is fed into it and until current is not reaching the ignition coil the car won't start (Voge, 1933; McMahon, 2013). In this security system a password protected digital interface is placed between battery and lock so that the unauthorized access of car by stolen key can also be checked. Basic motive is to control the flow of current between ignition coil and battery so that the vehicle starts according to the will of actual user and not according to the will of key holder (Pedroni, 2004; Roth, 1998; Kumar, 2012; Mano, 2007).

Figure 3 is depicting a simple block diagram of the security system. Basically whole security system is divided in to combinational logic, control unit and password unit. Password unit store and compares password, control signal generates signals on basis of matching and mismatching of password. According to these control signals combinational logic opens or closes the circuit between battery and ignition coil.

Current from the battery will reach the ignition coil only when combinational logic provides a path to it. To complete the circuit right password combination has to be fed in to the security system. A password is saved in the memory unit by the user on the first go. Then the same password has to be fed again every time to start the engine. The password which is fed by the user is compared to the password saved in the memory. If both the password matches, then the control unit generates the required signals to the complete the circuit and current from

Journal of Graphic Era University
Vol. 4, Issue 2, 72-83, 2016
ISSN: 0975-1416 (Print)

battery reaches the ignition coil. Now key can be placed in the lock and vehicle can be started normally.

Once the Digital Interface is in ON state the password can be changed by generating a "RESET" signal and new password can be saved in the memory.

By placing a Digital Interface between battery and ignition coil, the flow of current has become dependent on the TRUE condition of digital logic. Until the logic is true no current will be passed. So even if someone manage to steal the keys or completes the circuit by joining the wires manually, he will not be able to start the car without the right password combination as the circuit remains open until digital logic is not true. Due to this key has become secondary and personal user password has become primary element required to start the car (Voge, 1933; McMahon, 2013; Alrabady, 2005; Pedroni, 2004; Roth, 1998).

3. Front End Implementation of DI of VSS

In this section we will discuss the gate level front end implementation of the DI as shown in Figure 2. Further we will also look at FPGA implementation of DI. Hardware implementation of DI is essential for logical feasibility of the DI. Before designing its backend part, it is very important that its logical output is tested and altered if necessary. Further it also ensures the correctness of our idea on logical level.

Digital Interface (DI) of Vehicle Security System which is indicated in Figure 4 and 5 at block level and RTL level respectively has 8 input and 4 output pin (pins can be varied according to the requirement as they just represent the input and outputs to the DI) device. In this particular prototype we have:

(i) One decimal input is applied at input pin 'a [9:0]'. This input serves as the input password for the device. In this prototype only single digit is taken as input. But it does not mean that input digits can't be increased. They can be increased by increasing the input lines.
(ii) CLK is the system clock input which is required to synchronize the different sequential circuits utilized in the device. So that all devices work synchronously.
(iii) MS is the main switch which acts as main disable for the device.
(iv) RESET is required to set reset the device when the device is in on state and password has matched correctly.
(v) Engine, light, acc1, acc2 are different input control signals applied to DI by user to operate different components and accessories attached to the vehicle by applying the current obtained from the battery.
(vi) Ac1, ac2, e, l represents the output control signal obtained from DI which is applied to the different component of vehicle and operate them by providing current from the battery.

Journal of Graphic Era University
Vol. 4, Issue 2, 72-83, 2016
ISSN: 0975-1416 (Print)

Password module X1 deals with the password, which includes features like intake of password and its storage. It also takes care of the comparison of input password and password stored in the memory. In short this unit is responsible for taking input by the end user and its comparison with the password stored in the memory of the system. Once the password is correctly matched it generates a high signal as the output otherwise not, this can be easily understood from Figure 6 which represents the complete working of DI. It includes decimal to bcd decoder, memory, comparator and shift registers. Password module is further divided into x1 and x2. Here x1 is decimal to BCD decoder and x2 is memory and comparison unit as depicted in Figure 7. Figure 8 and 9 are depicting different output stages of password module. It is clear from the above figures that how the DI will retain and match the password. Table 1, 2 and 3 show the resource utilized by the DI during FPGA implementation of the circuit. Further it also indicates the successful hardware implementation the circuit which was designed using VHDL at gate level.

4. Incorporation of Organic Transistor

Organic electronics is field of enormous possibilities as it is still less explored in comparison to silicon based devices. Moreover, organic electronics provides numerous advantages like flexibility of the substrate, low cost raw material, low cost fabrication, simple fabrication steps and flexible devices. Properties like low cost of material and fabrication and independence of substrate are quite useful in our security system. It will not only make the security system economical but also provide us with an option of embedding the system in the polymer interior of the vehicle itself. Making is more secure and inaccessible during any unauthorized access.

Some of the advantages of Organic transistors over silicon based transistors are mentioned in Table 4. Analytical modeling of Circular OTFT is also done in the paper along with the simulation of circular OTFT on state of art industry grade Silvaco ATLAS software. Utilization of Organic transistors will definitely facilitate the reduction in cost and make the device more affordable and commercially viable. It will also make the security system more robust and easily replaceable in contrast with other conventional technologies (Bakhshi, 2004; Klauk, 2006; Kumar, 2014; Kumar, 2013; Locci, 2007; Locci, 2009).

Analytical Modeling of Cylindrical OTFT (*Locci, 2007; Locci, 2009*):
Capacitance, C_i:

$$C_i = \frac{\varepsilon_i}{r_i \times \ln\left(\frac{r_i}{r_g}\right)} \quad (1)$$

Journal of Graphic Era University
Vol. 4, Issue 2, 72-83, 2016
ISSN: 0975-1416 (Print)

Here, r_i = insulator radius, r_g = gate radius, ε_i = dielectric permittivity ($3\varepsilon_0$), ε_0=8.85 x 10^{-12}F/m.

Channel width, *z*:

$$z = (2 \times \pi \times r_i) \tag{2}$$

Channel length, *l*:
For circular OTFTs

$$z = l \tag{3}$$

Drain current linear:

$$I_{d1} = \left(\frac{z\mu C_i}{l}\right)\left((V_g - V_t)V_d - \frac{V_d^2}{2}\right) \tag{4}$$

$$I_d = \left(\frac{z\mu C_i}{l}\right)\left((V_g - V_t)\left(V_d - (R_s I_{d1}) - \left(V_d - \frac{(R_s I_{d1})^2}{2}\right)\right)\right)$$

Drain current saturation:

$$I_d = \left(\frac{z\mu C_i}{2l}\right)(V_g - V_t)^2 \tag{5}$$

Here, V_g = gate voltage, V_d = drain voltage, z = channel width, C_i = parasitic capacitance, l = channel length, μ = mobility, V_t = threshold voltage, R_s = contact resistance.

Figure 11 throws light on the successful device implementation of Cylindrical OTFT and its functioning and its structure. It also depicts different material regions and doping profiles. The current concentration in the device on application of supply voltage is also shown clearly. Similarly Figure 10 represents output characteristics of cylindrical OTFT calculated by analytical modeling and verifying the mathematical model of the organic transistor.

5. Conclusion

Digital interface proposed in this paper is a step towards making vehicles more secure towards theft at affordable price. Efforts have been made in this paper to incorporate the OTFTs in the device fabrication in order to achieve the goal of cost efficiency. Therefore, by placing this economical and robust DI between the battery and the ignition coil we control the functionality of the vehicle. This DI not only controls the ignition of ignition coils but also controls the initialization and termination of all other accessories attached to the battery and

Journal of Graphic Era University
Vol. 4, Issue 2, 72-83, 2016
ISSN: 0975-1416 (Print)

requires battery current to operate. In conclusion we can say that this DI offers an efficient and secure way to operate any vehicle which requires battery current to initialize its engine.

Component Name	Number
Shift Registers	8
3-bit shift register	8
Multiplexers	4
1-bit 4-to-1 multiplexer	4
Logic shifters	4
4-bit shifter logical left	4
Comparators	3
4-bit comparator equal	1
4-bit comparator greater	1
4-bit comparator less	1

Table 1. Number of different components used by the device during FPGA implementation

Cells	Numbers
BELS	38
GND	1
LUT2	9
LUT3	7
LUT4	20
VCC	1
FLIP FLOPS/LATCHES	16
FDE	8
LD	8
SHIFTERS	8
SRL16E	8
Clock Buffers	2
BUFGP	2
IO Buffers	20
IBUF	16
OBUF	4

Table 2. Cell usage by the device during FPGA implementation

	Used	Total	Percentage
Number of Slices	29	192	15%
Number of Slice Flip Flops	16	384	4%
Number of Slice Flip Flops	44	384	11%
Number of bonded IOBs	20	90	22%
Number of GCLKs	2	4	50%

Table 3. Complete device utilization summary for SPARTAN 2 Xc2s15

Journal of Graphic Era University
Vol. 4, Issue 2, 72-83, 2016
ISSN: 0975-1416 (Print)

	Organic electronics	Silicon
Cost (raw material)	$5/ ft^2	$100/ft^2
Fabrication cost(setup)	Low Capital	$1-$10 billion
Device size	10 feet x Roll to Roll	<1m^2
Material	Flexible Plastic Substrate	Rigid Glass or Metal
Fabrication condition	Ambient Processing	Ultra clean room
Process	Continuous Direct Printing	Multi-step photolithography

Table 4. A comparison of organic and silicon technology [Klauk, 2006; Kumar; 2014; Kumar, 2013; Locci, 2007)]

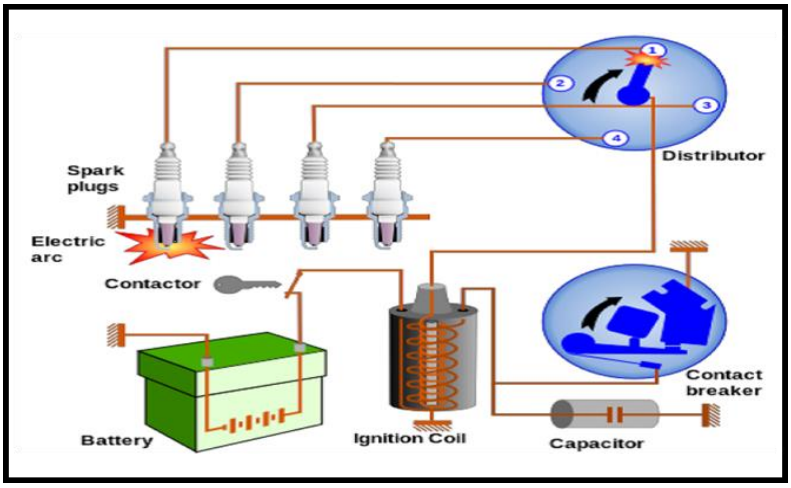

Figure 1. Cartoon representation of battery ignition system

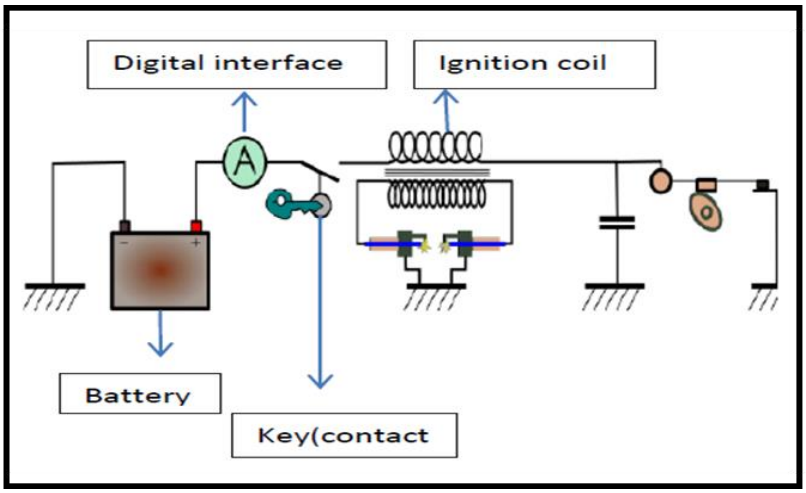

Figure 2. Innovative car security system with digital interface (DI)

Journal of Graphic Era University
Vol. 4, Issue 2, 72-83, 2016
ISSN: 0975-1416 (Print)

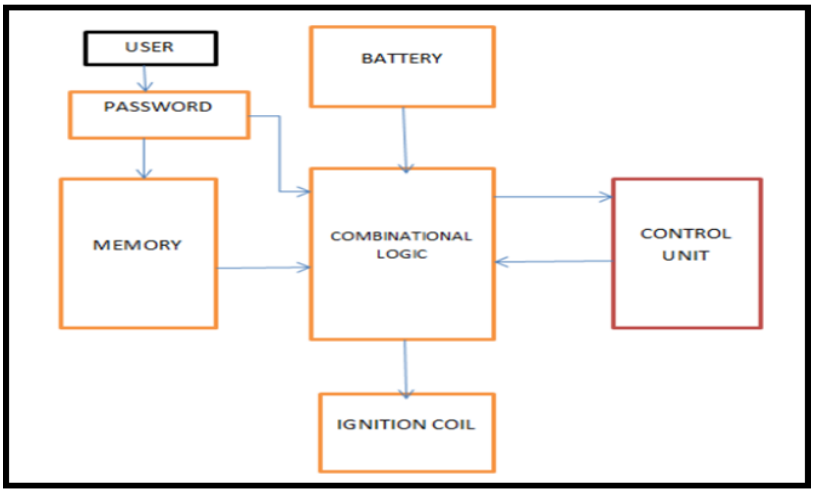

Figure 3. Block diagram of car security system

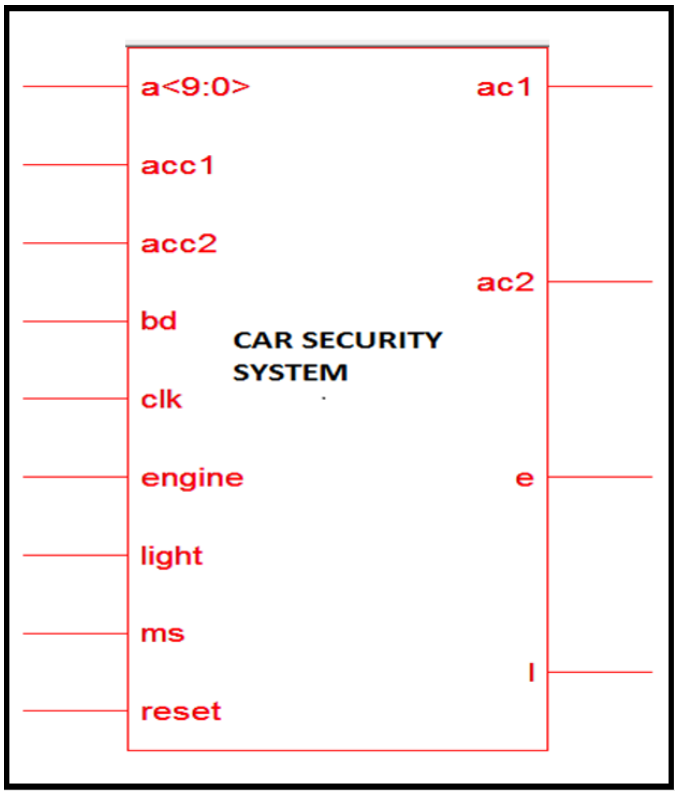

Figure 4. Basic RTL view of car security system

Journal of Graphic Era University
Vol. 4, Issue 2, 72-83, 2016
ISSN: 0975-1416 (Print)

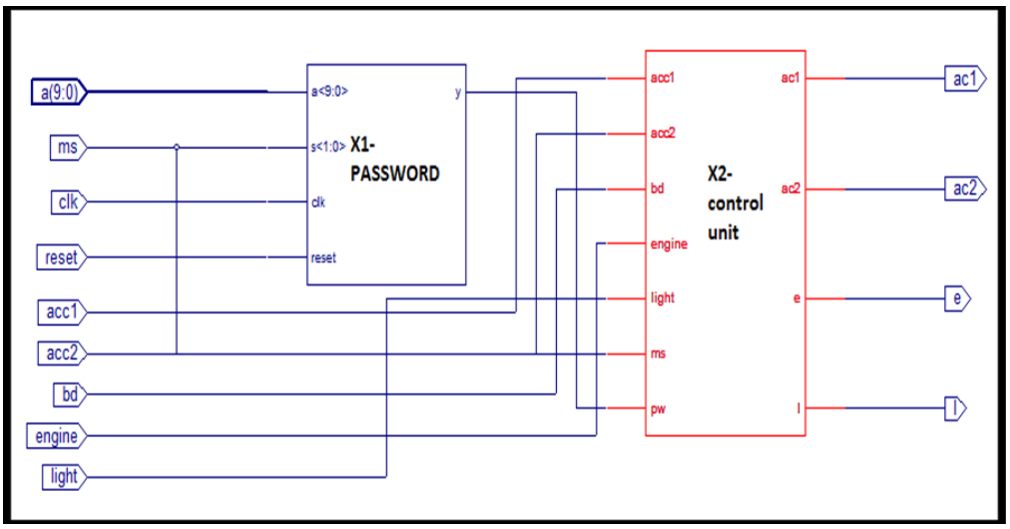

Figure 5. Detailed RTL view of car security system

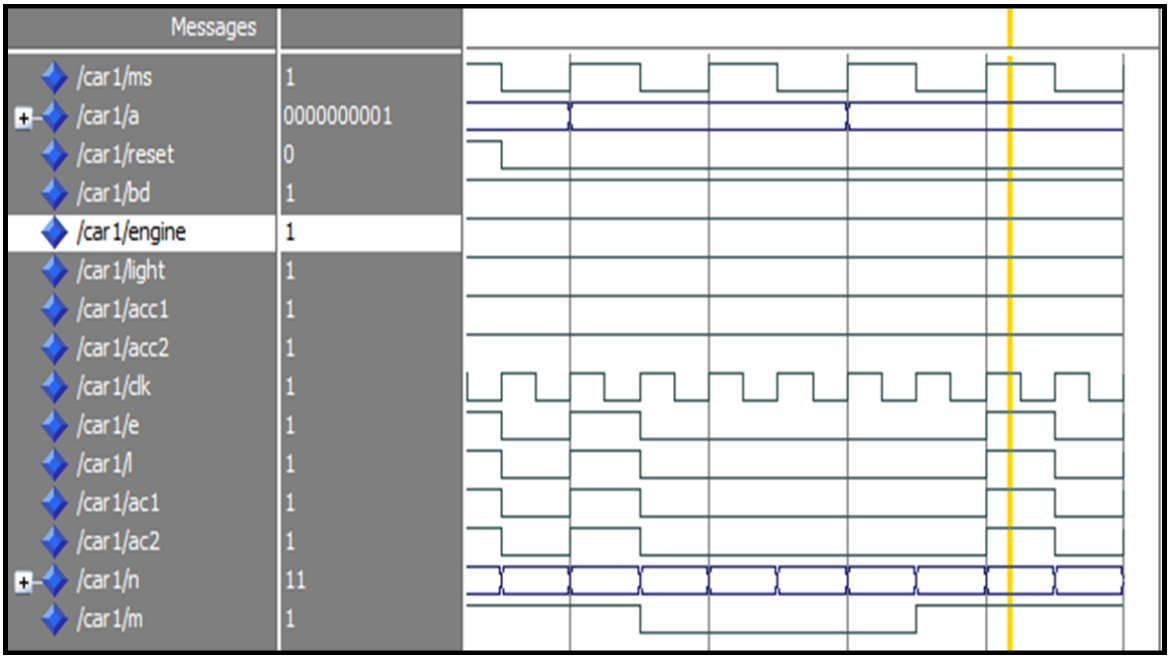

Figure 6. Simulated output of car security system. It is shown in the figure when 'ms' is '1' and password applied as input matches the password stored in the memory the system is in 'on' state and if input is applied at components like 'engine' and 'light' a positive output is generated

Journal of Graphic Era University
Vol. 4, Issue 2, 72-83, 2016
ISSN: 0975-1416 (Print)

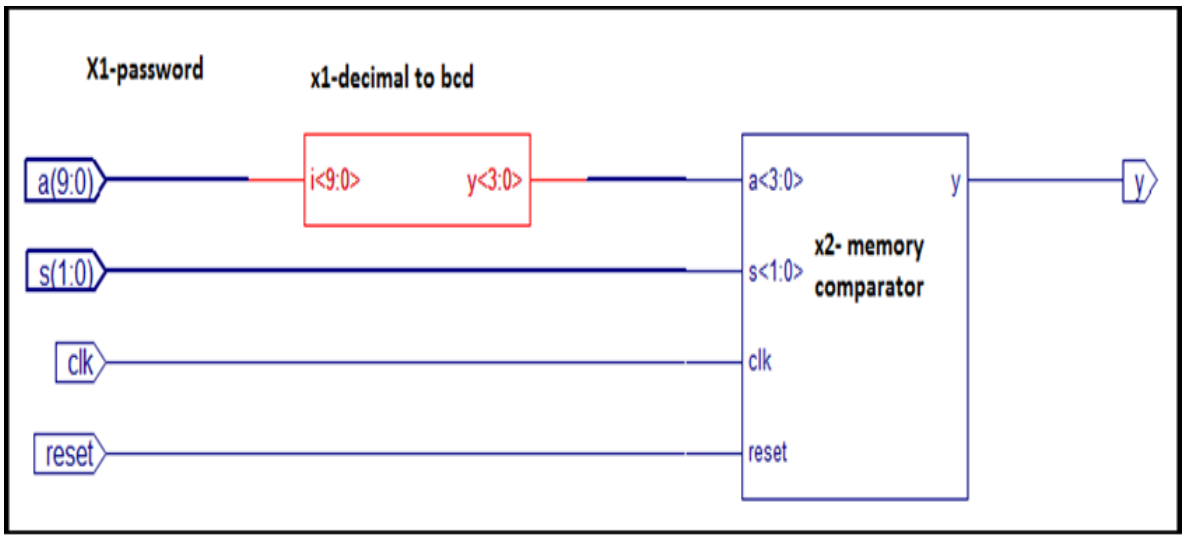

Figure 7. RTL of password module (X1)

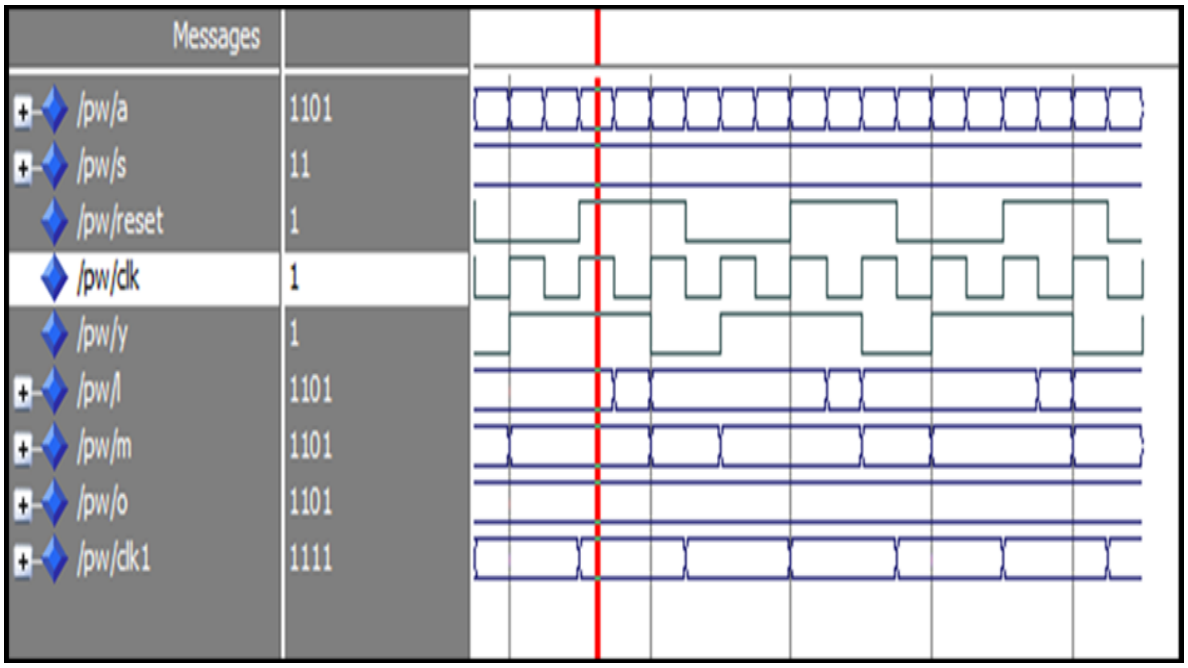

Figure 8. Analyzed output of password module. Here it is shown that when reset is '1' password is being stored in the memory. Output 'y' indicating password is stored and matched correctly

Journal of Graphic Era University
Vol. 4, Issue 2, 72-83, 2016
ISSN: 0975-1416 (Print)

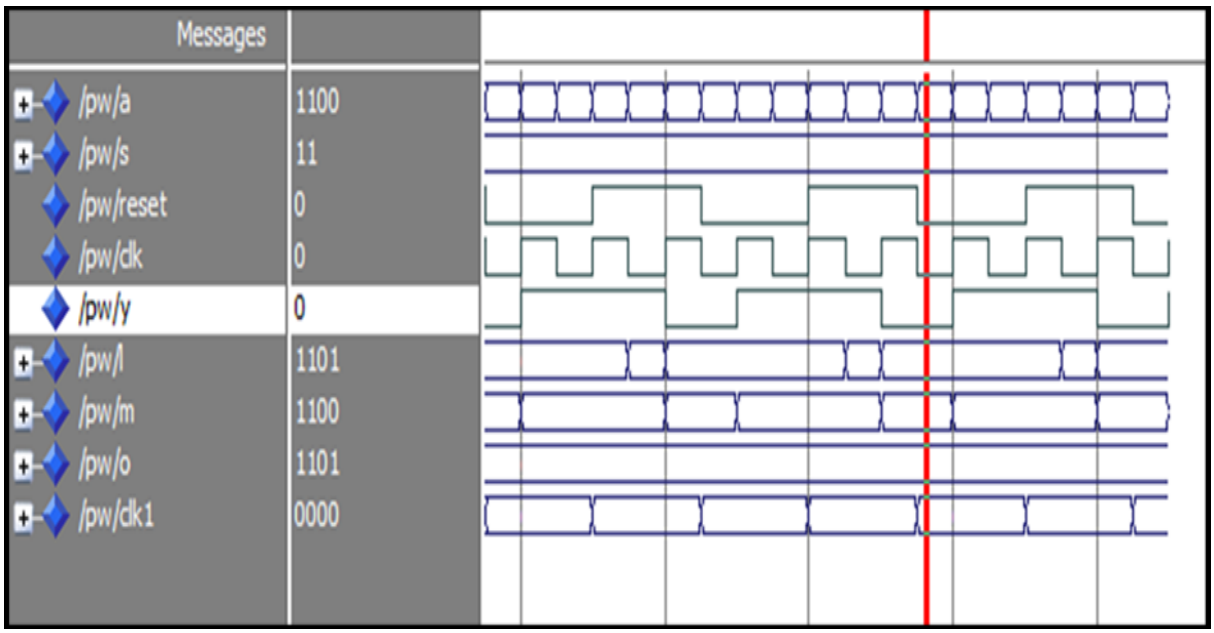

Figure 9. Analyzed output of part X1 in off state. Here 'reset' is set to '0' and new input password has been applied. Since the input password has not matched to the stored password output 'y' is '0'

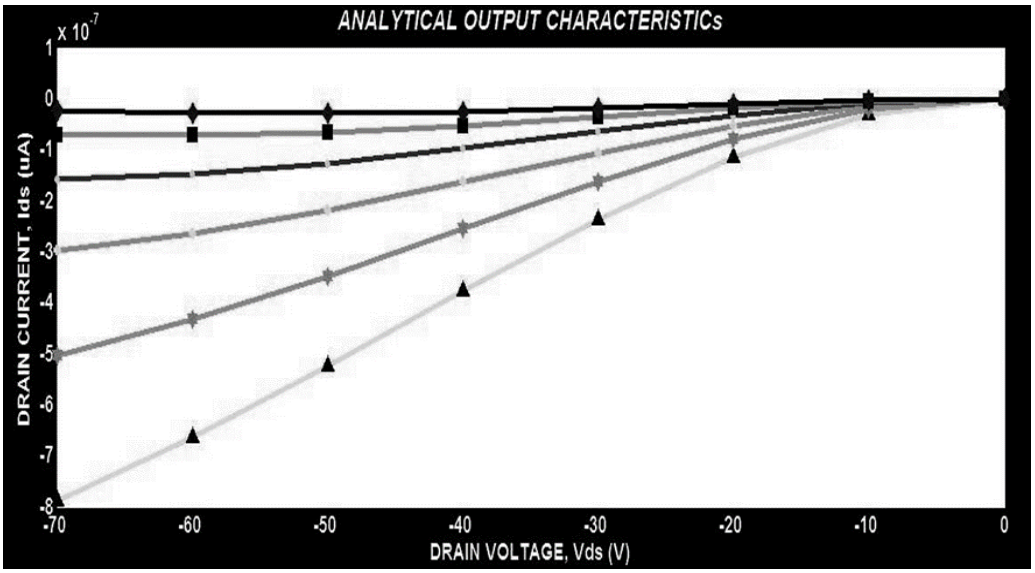

Figure 10. Output characteristics of cylindrical OTFT calculated by analytical modeling in Matlab

Journal of Graphic Era University
Vol. 4, Issue 2, 72-83, 2016
ISSN: 0975-1416 (Print)

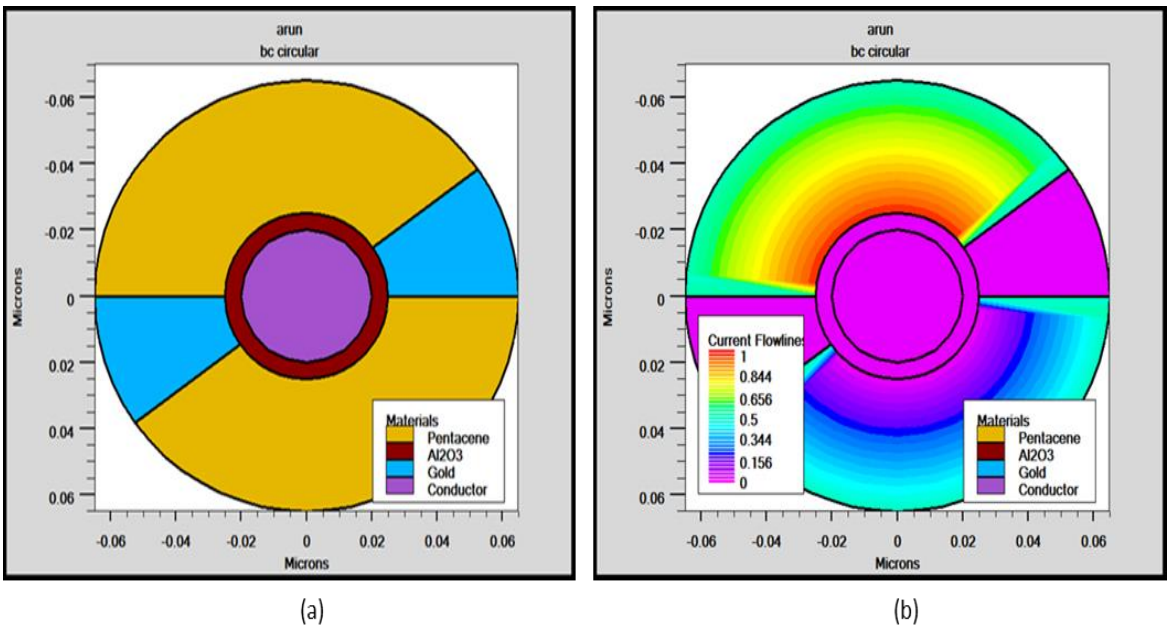

Figure 11. (a) Structure of simulated cylindrical OTFT along with (b) Current flow lines and current density of cylindrical OTFT

References

Alrabady, A. I., & Mahmud, S. M. (2005). Analysis of attacks against the security of keyless-entry systems for vehicles and suggestions for improved designs. IEEE Transactions on Vehicular Technology, 54(1), 41-50.

Bakhshi, A. K., & Bhalla, G. (2004). Electrically conducting polymers: Materials of the twenty first century. Journal of Scientific and Industrial Research, 63, 715-728.

Ciletti, Michael D., Mano, M. Morris, (2007). Digital Design (1st Ed.). Pearson India.

Klauk, H. (Ed.). (2006). Organic electronics: materials, manufacturing, and applications. John Wiley & Sons.

Kumar, B., Kaushik, B. K., & Negi, Y. S. (2012, December). Analysis of Contact Resistance Effect on Performance of Organic Thin Film Transistors. In Electronic System Design (ISED), 2012 International Symposium on (pp. 198-202). IEEE.

Kumar, B., Kaushik, B. K., & Negi, Y. S. (2013). Modeling of top and bottom contact structure organic field effect transistors. Journal of Vacuum Science & Technology B, 31(1), 012401.

Kumar, B., Kaushik, B. K., & Negi, Y. S. (2014). Organic thin film transistors: structures, models, materials, fabrication, and applications: a review. Polymer Reviews, 54(1), 33-111.

Locci, S. (2009). Modeling of physical and electrical characteristics of organic thin film transistors.

Locci, S., Maccioni, M., Orgiu, E., & Bonfiglio, A. (2007). An analytical model for cylindrical thin-film transistors. IEEE Transactions on Electron Devices, 54(9), 2362.

McMahon, M. (2013). Trade of Motor Mechanic: Basic Ignition Systems (2nd Ed). SOLAS.

Pedroni, V. A. (2004). Circuit Design with VHDL, (1st Ed.). MIT Press London.

Roth, C. H. (1998). Digital systems design using VHDL (Vol. 20). PWS publishing company.

Voge, C. J. (1933). U.S. Patent No. 1,928,744. Washington, DC: U.S. Patent and Trademark Office.