Enhancing Security with Binary Bit Password Protection Techniques

Darshana Pandya[1*], Abhijeetsinh Jadeja[2], Sheshang Degadwala[3], Pooja Borate[4]

Associate Professor, Shri C. J Patel College of Computer Studies (BCA), Sankalchand Patel University, Visnagar[1]
Professor, Department of Engineering, Darshan University, Rajkot, Gujarat[2]
Professor & Head of Department, Department of Computer Engineering, Sigma University, Vadodara, Gujarat, India[3]
Research Scholar, Madhav University, Pindwara, Sirohi, Rajasthan, India[4]

ddpandya.fcs@spu.ac.in[*1], abhijit.highereducation@gmail.com[2], sheshang13@gmail.com[3], pborate790@gmail.com[4]

Abstract: The Objective of this Paper is to Develop a Password Security System Utilizing BinaryBit Technology logic gates AND, XOR, and NOT. A separate color light will glow to signify incorrect password entry (as opposed to the value previously stored). A colorful light will glow if the password you entered matches the password you previously stored. I'll try to put this approach into practice using the Multisim and Verilog programs. This password security system is an approachable one that may be used in homes, workplaces, and other institutions. Passwords are used throughout the system to restrict access. This simple circuit can be installed in residential areas to increase safety. It can be used in businesses to ensure authorized access to places with high security requirements. I'll be attempting to use a counter in the real-time circuit to lower the number of password entry tries as a result, the security system will be significantly safer and less error-prone.

Keywords: Security, Password, Counter, Simulation

I. INTRODUCTION

In the Password Security System, one input comes from the data entry switches, while the other comes from the key code switches. The XOR gate generates a low output when both inputs are high or low, and a high output when one input is high and the other is low. Due to this characteristic, XOR functions as a bit comparator, comparing the entered code to the hidden code. If both codes are the same, the output will be low, but if they are different, the output will be high. OR gates are diodes whose anodes are connected to the outputs of XOR gates and cathodes are connected to the negative terminal of the battery via a resistor. In both cases i.e. the password match and wrong password case, different colored LEDs are accordingly glown.

In the 2-bit Asynchronous Down Counter, the clock pulses are counted using counters. The clock pulses are spaced out in a regular pattern. They're utilized to track the passage of time and frequency. Counters can also be described as sequential circuits that modify their pre-defined states in response to clock pulses. An external clock pulse is provided for only the first flip flop in the asynchronous counter; after that, the output of the first FF functions as a clock pulse for the second FF, and so on. It has two flip flops in it. A ripple counter with two bits can count up to four states. It's called a down counter since it counts down from three to zero. We can connect the clock frequency to the U21 / the and gate that leads to the password incorrect LED. By doing the above, we can ensure that the third consecutive wrong attempt leads to an LED alert. Due to the software's inability to connect the clock frequency on both sides , the complete circuit cannot be made . We expect the red led of the down counter to glow when the password is not matched for 3 consecutive times. When the first wrong attempt is made, the output is the 2-bit combination 11 (decimal - 3). In the 2-bit Asynchronous Down Counter, the clock pulses are counted using counters. The clock pulses are spaced out in a regular pattern. They're utilized to track the passage of time and frequency. Counters can also be described as sequential circuits that modify their pre-defined states in response to clock pulses. An external clock pulse is provided for only the first flip flop in the asynchronous counter; after that, the output of the first FF functions as a clock pulse for the second FF, and so on. It has two flip flops in it. A ripple counter with two bits can count up to four states. It's called a down counter since it counts down from three to zero. We can connect the clock frequency to the U21 / the and gate that leads to the password incorrect LED. By doing the above, we can ensure that the third consecutive wrong attempt leads to an LED alert. Due to the software's inability to connect the clock frequency on both sides, the complete circuit cannot be made. We expect the red led of the down counter to glow when the password is not matched for 3 consecutive times. When the first wrong attempt is made, the output is the 2-bit combination 11 (decimal - 3). When the second wrong attempt is made the output is the bit combination 10 (decimal 2). Finally, when the third wrong attempt is made; the output is the bit combination 01 (decimal 1). This is when the red LED of the down counter glows, giving an alert

which leads to the user to not be able to enter the password anymore after 3 wrong attempts. Create a password (preset password). Then, as an input provided by the user, a password is used (password input). They are then compared. Access is provided if they match. If they don't match, access is refused, and the count goes up by one. If the count is less than three, the system starts over [a password match causes the count to be zero]. If the count reaches three, an alert is triggered and the condition of "Access Denied" is maintained.

II. IMPORTANT FIGURES & PARTS

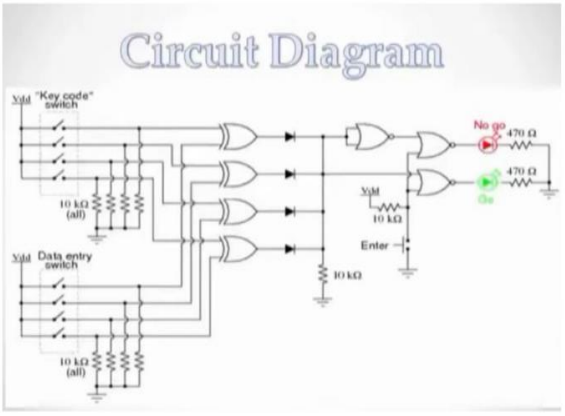


Figure 1: 2-bit Asynchronous counter

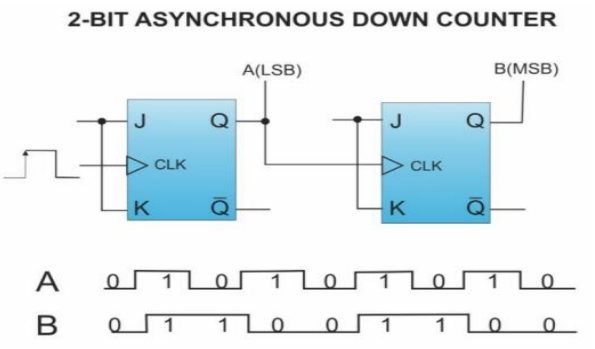


Figure 2: 2-bit Asynchronous down counter

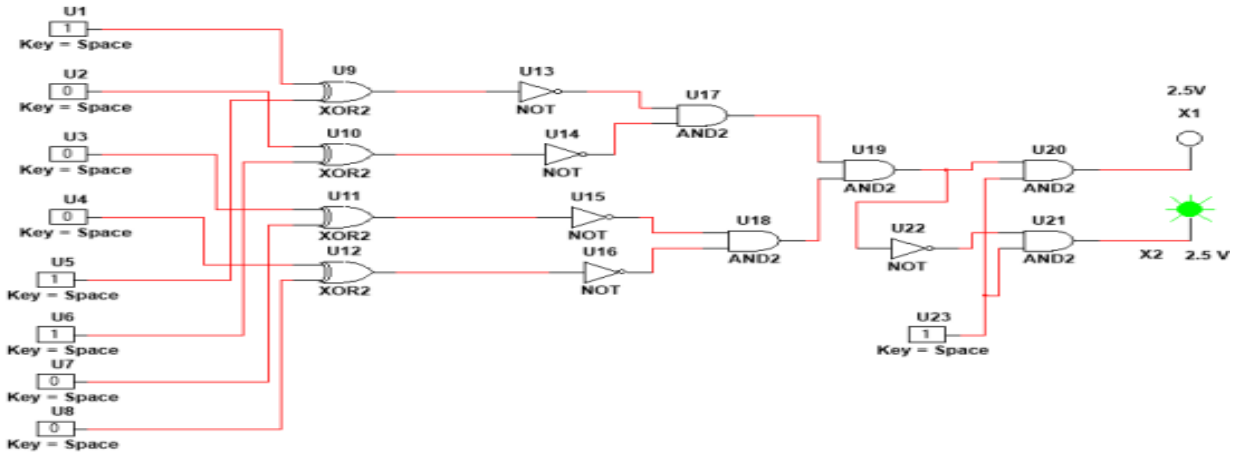


Figure 3: Asynchronous down counter

The hardware aspect of this project requires the following components:

For the General Password Security System:

1) Four XOR gates, 2) Five Not gates, 3) Five And gates, Each of the IC can have 4 gates.

For the 2-bit Asynchronous Down Counter:

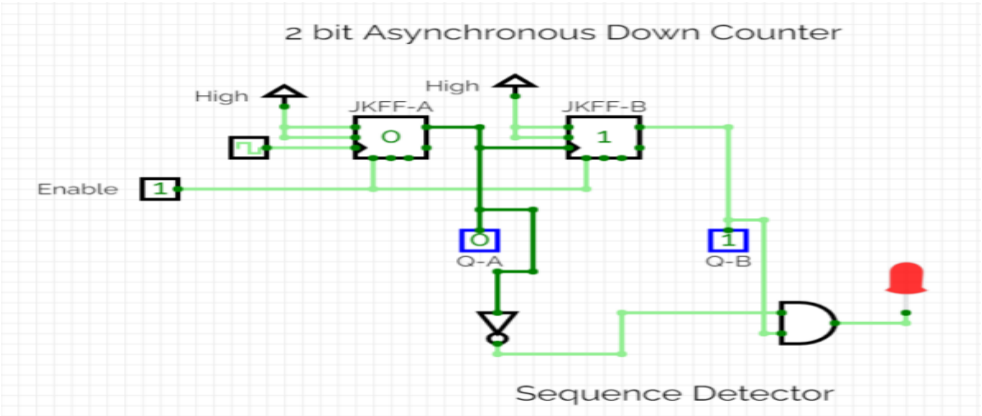


Figure 4: Two Asynchronous down counter

III. VERILOG CODES, SIMULATIONS & OUTPUT

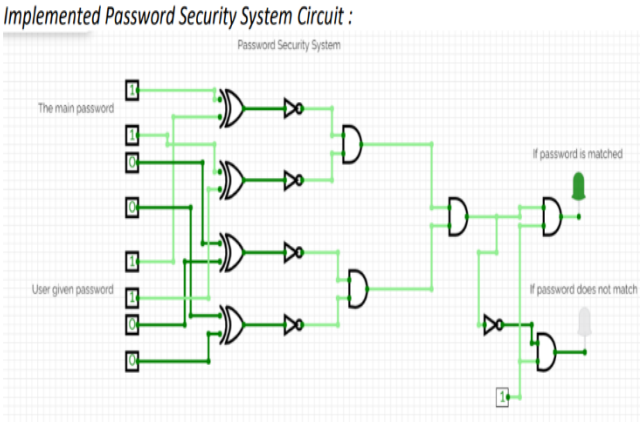


Figure 5: Password security system circuit

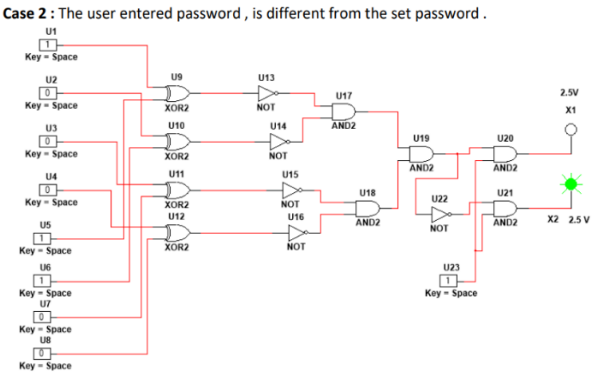


Figure 6: Password security system circuit

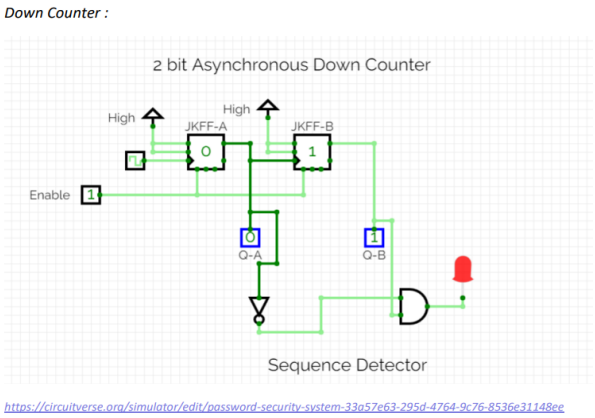


Figure 7: Two-bit Asynchronous counter

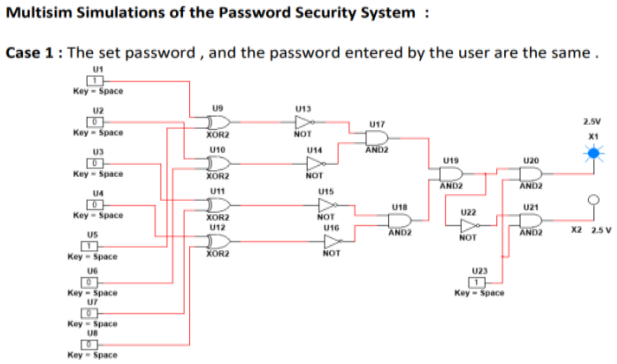


Figure 8: Simulation of the password security system

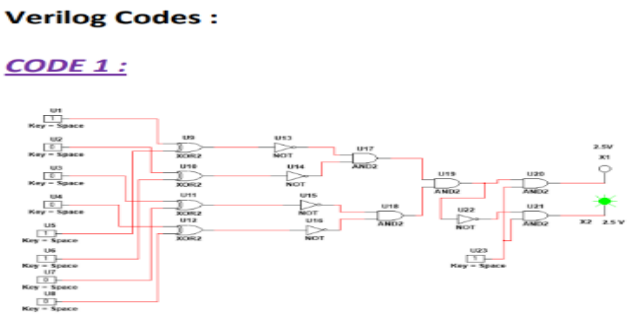


Figure 9: Verilog codes

Code I is written exactly how the gates are connected in the circuit. 'Assign' keyword is used to give the input and get the intermediate and final outputs. We expect a high output in the U20 gate, if the password matches. U21's output is low this time. We expect a low output in the U20 gate, if the password doesn't match. U21's output is high in this case. U20 - has a high output, when password is matched (U21's output is low here). U21 - has a high output, when password is not matched (U20's output is low here)

In Code II, Reset is an input which is kept high if the user wants to refresh the values of SetPass and PassIn. We don't want to do that; hence we keep Reset as 0. Enter is an input which is kept at 1, because it's the input that registers the input if provided; and prevents any stray input from getting registered. The SetPass is the password set by the user. The PassIn is the password entered by the person trying to get access into the system. The assignment statement causes, the

bit-by-bit comparison from LSB to MSB (faster than LSB to MSB). The below code, can take the password values, of up to 12 bits [11:0]; but works for an n bit system too. The code for Down Counter is also written. Backward counting happens in Code II.

CODE 1 Output :

Output Figure 1 : Code output , when both the entered passwords are the same.

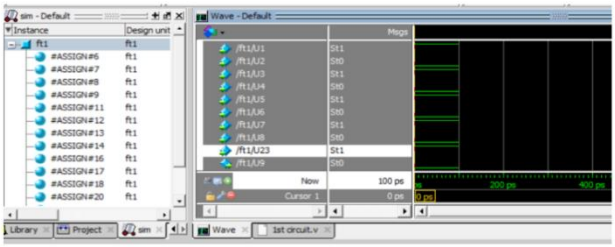
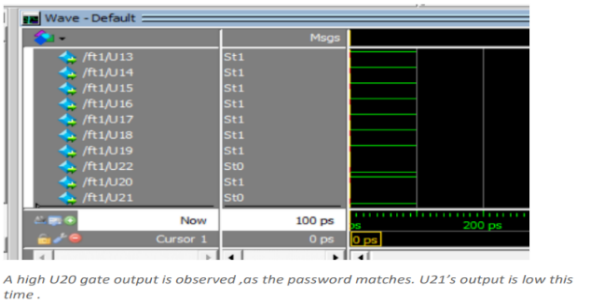


Figure 10: Code Output



A high U20 gate output is observed ,as the password matches. U21's output is low this time .

Figure 11: Code Output

Output Figure 2 : Code output , when the entered password doesn't match the set one.

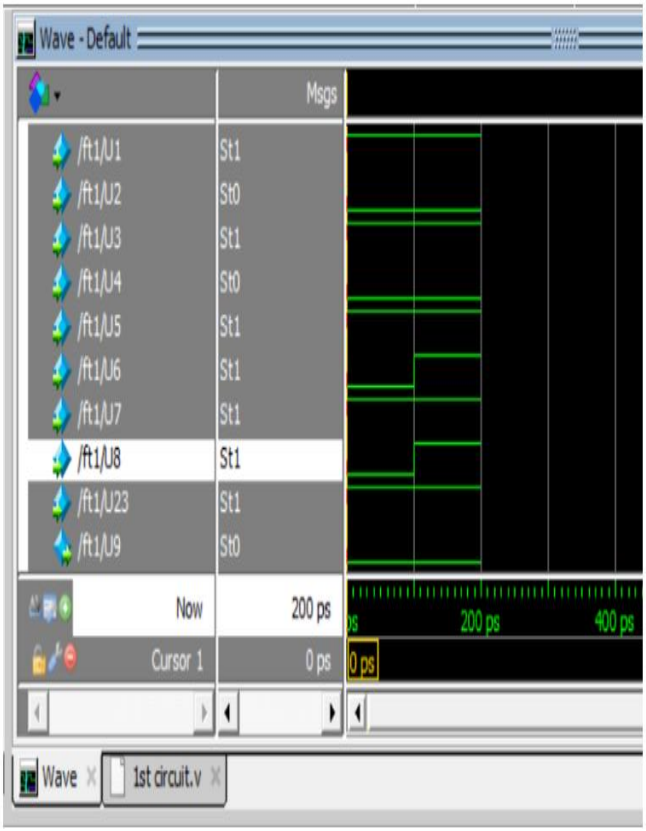
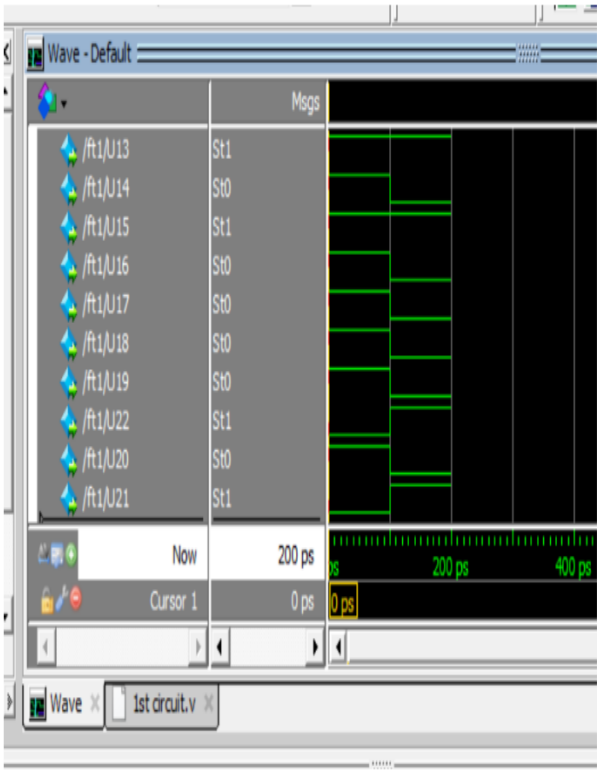


Figure 12: Code Output



A high U21 gate output is observed , as the password doesn't match. U21's output is high this time .

Figure 13: Code Output

CODE 2 Output :

- The SetPass is the password set by the user. The PassIn is the password entered by the person trying to get access into the system .
- If both these are same , then the 'Check' waveform is expected to be high . This can be seen in Figure A.
- The Check waveform , is expected to be low , when the passwords do not match . This can be seen in Figure B.

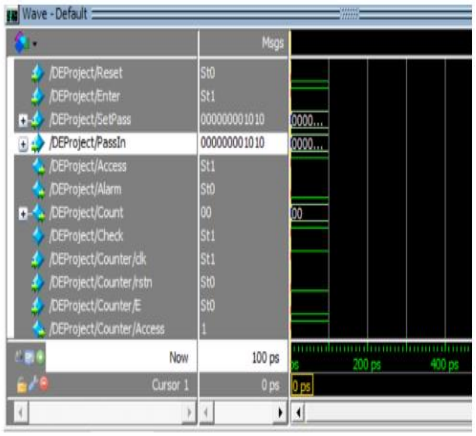


Figure A : Code output , when both the entered passwords are the same. The Check waveform is in high state .

Figure 14: Code Output

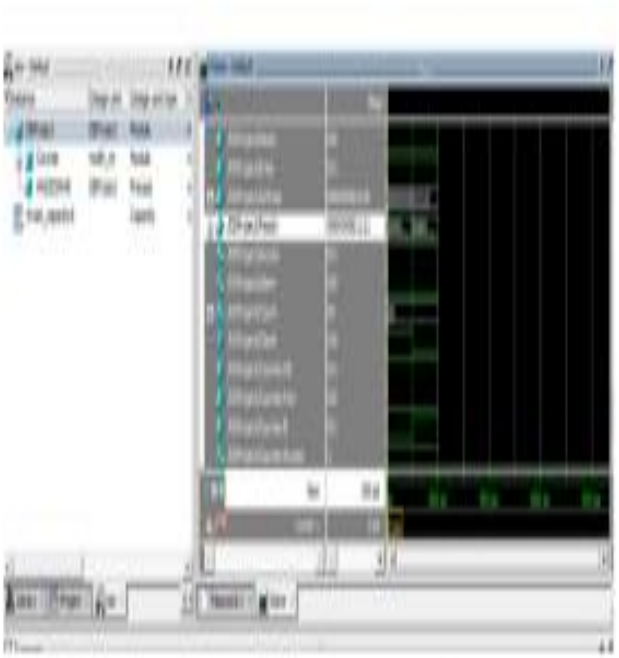


Figure B : Code output , when both the entered passwords are different . The Check waveform is in a low state .

Figure 15: Code Output

IV. CONCLUSION

A straightforward circuit that may be created with the aid of fundamental logic gates is the Password Security System. The 2 Bit Asynchronous Down Counter, which can cap the amount of password entry tries at 3, is an additional feature added to this project. Security concerns are the primary use of the Password Security System. It is convenient and easy to use. It requires less management but still offers enough protection. It is easy to keep an eye on. Occasionally, circuits can be bypassed using grounding or electrical breakdown. It needs a power source to run, if it runs at all.

REFERENCES

[1] Taj, Md. Nasim & Sultan Mahmud, Md & Hasan, Samit. (2020). Hex-Password Based Lock Security System. 10.13140/RG.2.2.26007.91047.

[2] A Arefín, Utsho & Rashu, Md & Islam, Md. Rashedul. (2014). Electronic Password Protected Security System. 10.13140/2.1.1782.

[3] Wahyudi, Hasimah Ali, and M. J. E. Salami (2009). Combining ANN and ANFIS-based classifiers, we can create a typing biometrics authentication system based on keystroke pressure. The 5th International Colloquium on Signal Processing and Its Applications was held in 2009. (pp. 198–203).

[4] Tsai, C.-J., Chang, T.-Y., and Lin, J.-H. (2012). a touch screen dynamic authentication system with graphical input for handheld mobile devices. 85(5), 1157-1165, Journal of Systems and Software.

[5] Sanjay Gaur, Darshanaben Dipakkumar Pandya (2019), Closest Fit Approach for Pattern Designing to Recovered Anomalous Values in Data Mining, 2018 Second World Conference on Smart Trends in Systems, Security and Sustainability (WorldS4), 308-312 IEEE Xplore, DOI: 10.1109/WorldS4.2018.8611610

[6] Sanjay Gaur, Darshanaben D Pandya, Manish Kumar Sharma (2020), Applied NF interpolation method for recover randomly missing values in data mining, Fourth International Congress on Information and Communication Technology: ICICT 2019, London, Springer Singapore, Volume 2, 475-485.

[7] Sanjay Gaur, MS Dulawat (2011), Improved Closest fit Techniques to handle missing Attribute values, Journal of Computer and Mathematical Sciences Vol-2, no-2, 170-398.

[8] Smith, J. A. (2021). Significance of Sentiment Analysis with Text-based Mining Approach. Journal of Text Mining and Sentiment Analysis, 8(2), 112-128.

[9] Alonso, M. A., Vilares, D., Gómez-Rodríguez, C., and Vilares, J. (2021). Sentiment analysis for fake news detection. Electronics 10:1348.