Fingerprint Detection Technique Using FPGA

Avinash Kumar
2018PEV5137
VLSI Design, ECE
MNIT
Jaipur, India
2018pev5137@mnit.ac.in

Mohd. Arshad
2018PEV5144
VLSI Design, ECE
MNIT
Jaipur, India
2018pev5144@mnit.ac.in

Sachin Kumar Yadav
2018PEV5184
VLSI Design, ECE
MNIT
Jaipur, India
2018pev5184@mnit.ac.in

***Abstract*— Fingerprint recognition is one of the most common techniques used for biometric identification. Currently fingerprint technology is suitable to recognize users with high accuracy and low execution times using microprocessors able to solve algorithms with high-computational cost. This paper describes a new approach to fingerprint recognition problem, proposing a low cost system, implemented by Field Programmable Gate Array (FPGA).**

Keywords—Hardware, minutiae, recognition, process, fingerprint image

I. INTRODUCTION

Security is becoming an important challenge for usual activities that require high confidence levels such as access control, cash terminal or internet banking among others. The security of these systems is traditionally based on guarantying the user's identity by using identification cards or passwords, prior to give access to confidential information, relevant places or restricted resources. However, this identification method presents several disadvantages, basically due to its inherent risk of loss or robbery. Identification systems based on biometric features lack of these problems, since the user's identity is determined based on physiological or behavioural characteristics unique for each person. Fingerprint is one of the most widespread identification techniques allowing high-medium confidence rates. Additionally, the small-size and low-cost of sensors used in capture devices has contributed to increase its commercial use

A fingerprint can be seen as a set of interleaved ridges and valleys on the surface of the finger. The capture device returns an image, usually with 256 grey-levels, which consists of dark (ridges) and bright (valleys) lines. The most widespread fingerprint matching approach relies on the fact that the uniqueness of a fingerprint can be determined detecting prominent singular points known as minutiae, which are represented either by bifurcation or termination of ridges. Furthermore, these patterns can be seen as crossover, core, bifurcation, ridge ending, island, delta, pore.

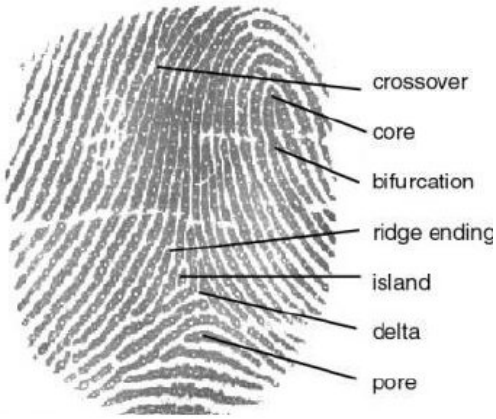

Fig. 1

II. FINGERPRINT EXTRACTION

The most critical step in a fingerprint recognition system is to extract minutiae from the input fingerprint image. Minutiae extraction relies on the quality of the input fingerprint image. In order to ensure the success of an automatic fingerprint recognition system, the quality of input fingerprint image must be good.

In our case the fingerprint data is being extracted and sent by the fingerprint module itself in the form of bits.

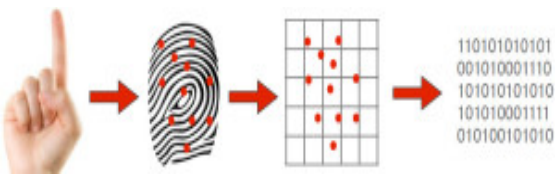

Fig. 2

We are using fingerprint module R305_v1.6 to read the fingerprint data.

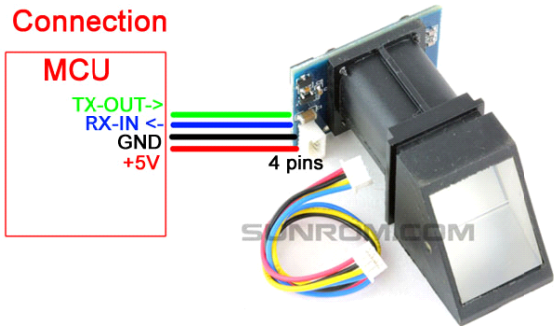

Fig. 3

It has 4 pins, first pin is for VDD, second is for ground, third for RX-IN of the FPGA, and fourth for TX-OUT of FPGA.

III. FPGA

A field-programmable gate array (FPGA) is an integrated circuit designed to be configured by a customer or a designer after manufacturing, hence the term "field-programmable". The FPGA configuration is generally specified using a hardware description language (HDL), similar to that used for an application-specific integrated circuit. Circuit diagrams were previously used to specify the configuration, but this is increasingly rare due to the advent of electronic design automation tools.

FPGAs contain an array of programmable logic blocks, and a hierarchy of reconfigurable interconnects that allow the blocks to be "wired together", like many logic gates that can be inter-wired in different configurations. Logic blocks can be configured to perform complex combinational functions, or merely simple logic gates like AND and XOR. In most FPGAs, logic blocks also include memory elements, which may be simple flip-flops or more complete blocks of memory.

FPGAs use LUTs to implement these logic functions.

IV. UART PROTOCOL

In UART communication, two UARTs communicate directly with each other. The transmitting UART converts parallel data from a controlling device like a CPU into serial form, transmits it in serial to the receiving UART, which then converts the serial data back into parallel data for the receiving device. Only two wires are needed to transmit data between two UARTs. UARTs transmit data asynchronously, which means there is no clock signal to synchronize the output of bits from the transmitting UART to the sampling of bits by the receiving UART. Instead of a clock signal, the transmitting UART adds start and stop bits to the data packet being transferred. These bits define the beginning and end of the data packet so the receiving UART knows when to start reading the bits.

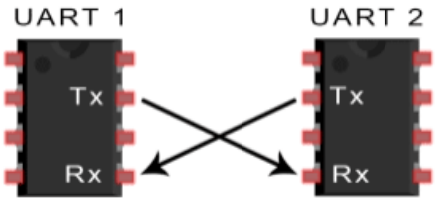

Fig. 4

When the receiving UART detects a start bit, it starts to read the incoming bits at a specific frequency known as the baud rate. Baud rate is a measure of the speed of data transfer, expressed in bits per second (bps). Both UARTs must operate at about the same baud rate.

V. BITS TRANSMISSION TO FPGA

The fingerprint data given out by the fingerprint module is to be sent to the FPGA for saving or matching. We use UART Protocol to send data bits from sensor to FPGA. UART Protocol helps the FPGA to communicate with the fingerprint sensor by sending and receiving data bits serially. We can send 8 bits (i.e. 1 byte) of data at a time serially, in addition it has 1 bit as start bit and 1 bit as end bit, so the total data sent at a time serially is 10 bits.

Fig .5

In this sensor, one fingerprint data consists of 256 bytes, so we need to repeat this process 256 times in order to get one fingerprint data.

VI. SAVING BITS IN RAM

Now, we have to save these bits of data which we are receiving in order to compare it for future authentications. So we are using BRAM for storing these bits. BRAM is a dedicated FPGA resource designed to implement large memories. We can manually instantiate the BRAM memory or can use the use the BRAM generator. We at first make one module for storing data and then call it wherever required.

For our application we have generated a simple single port BRAM module which has four input ports Clock (clk), Write enable (we), Data in (din) and Address in(addr) and it has one output port Data out (dout). Thus clearly it defined that how the data is saved and read from this module.

VII. USER AUTHENTICATION

For Authentication of user we first take the fingerprint from user, which will be extracted by the same procedure using minutiae extraction technique and the data bits will be transferred to the FPGA for matching with previously stored fingerprint bits. For authentication this new data will be compared with each row of the block ram. If the fingerprint data is already stored in the RAM then it will match and provide the user authentication successfully if it does not matches any of the stored data then the authentication will fail. The matching of the data is done sequentially, i.e. the data is matched bit by bit and if at any point the bit is found to be mismatching, user authentication fails.

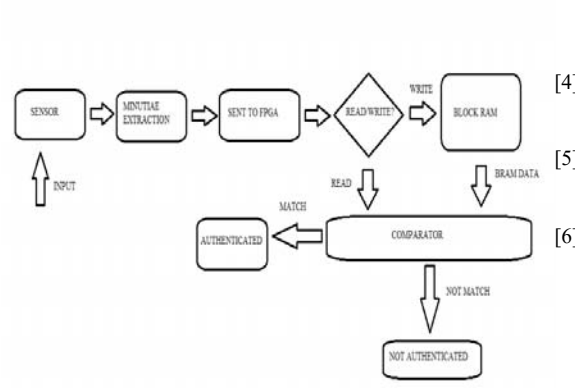

Fig. 6

VIII. CONCLUSION

There is a huge requirement of a secure authentication process in order to validate an authorised person at various organizations, for example at a banking environment we require a secured and reliable way of identifying that the person is who he says he is. The Traditional way of identification i.e. password based authentication system is good but can be compromised as the secret code needs to be memorised and is easy to be broken. We can use a fingerprint authentication method to authenticate a person as an effective and reliable method. As for this the person needs to be available himself and so this cannot be compromised.

Fingerprint detection process is implemented on FPGA board using fingerprint sensor. The sensor provides the information in form of data bits using minutiae extraction technique. The result shows the particular user is a authenticated person or not. The fingerprint detection technique can be used as a secure way of person authentication at different organisations.

IX. REFERENCES

[1]. Mariano Lopez and Enrique Canto, "FPGA implementation of a minutiae extraction fingerprint algorithm" https://ieeexplore.ieee.org/document/4676920

[2]. A. Alilla, M. Faccio, T. Vali, G. Marotta and L. DeSantis, "A new low cost fingerprint recognition system on FPGA" https://ieeexplore.ieee.org/document/6505806/authors#authors

[3]. Prof S Gayathri and Dr V Sridhar, "Implementation of Fingerprint Recognition System on FPGA", Implementation of Fingerprint Recognition System on FPGA[4].

[4]. Xilinx forums https://forums.xilinx.com/

[5]. Fingerprint sensor (R305) manual https://www.sunrom.com/p/finger-print-sensor-r305

[6]. UART Protocol https://web.stanford.edu/class/cs140e/notes/lec4/uart-basics.pdf