ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Online Signature Verification by Using FPGA

D.Sandeep
Assistant Professor,
Department of ECE,
Vignan Institute of Technology & Science,
Telangana, India.

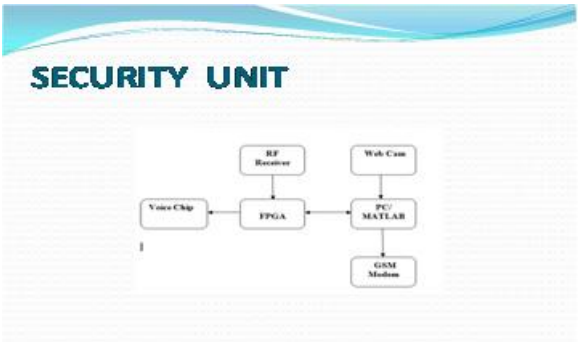
Ch.Chandrakanth
PG M.Tech, (VLSI-System Design),
Vignan Institute of Technology & Science,
Telangana, India.

ABSTRACT:
The main aim of this project is used for system verifying the signature of particular person with mobile devices.

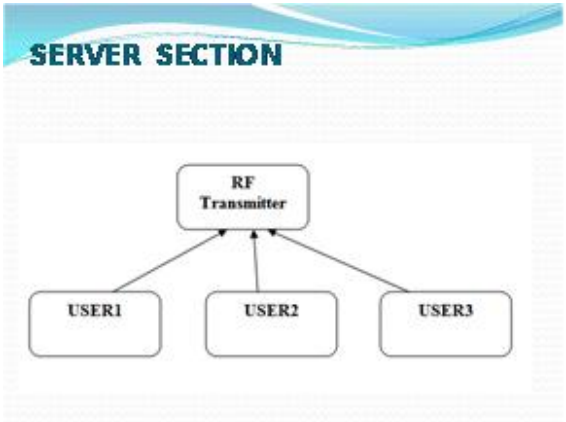
i) Introduction:
The project mainly studies online signature verification on PC interface-based mobile devices. A simple and effective method for signature verification is developed. An online signature is represented with a discriminative feature vector derived from attributes of several histograms that can be computed in linear time. The resulting signature template is compact and requires constant space. The algorithm used in this project is SVM (support vector machine). The results show that the performance of the proposed technique is comparable and often superior to state-of-the-art algorithms despite its simplicity and efficiency. In order to test the proposed method on we are using camera devices, a data set was collected from an uncontrolled environment and over multiple images.

ii) Description:
The online verification system mainly consists of 2 modules of security system and server section. For the FPGA part we interface the Rf receiver when ever authorized person enters then FPGA send the signal to PC with Matlab in the matlab it asks for opening of signature if signature was selected then with database matching will be start then if it is authorized ATM app form will open then corresponding voice will be played in the speaker module that was connected to the FPGA. In the existing system we mainly used Manual verification for signature verification Which does not have accurate checking of the signature to overcome the problem in the existing system we mainly use this system for signature verification which automatically verify signature by using GSM technique which has high accuracy and GUI representation is used .Online signature verification is mainly used for currency note checking applications, online monitoring ,home monitoring, security applications. In this project we divide the user using the RF transmitter which will allocate the different frequencies to the different persons. For the FPGA part we interface the RF receiver when ever authorized person enters then FPGA send the signal to PC with Matlab, whenever it was matched with the database then WEBCAM will be opened then it asks for the signature Image. The current signature Image was correlated with the database signature for verification. If the signature matches then with database then ATM app form will open then corresponding voice will be played in the speaker module that was connected to the FPGA If the signature doesn't match then an Alarm indication was given which was connected to FPGA and an SMS will be sent to the owner number.

2. BLOCK DIAGRAM:
INTRODUCTION:
In this project we mainly propose the Signature verification by using Spartan 3A FPGA that is supposed to replace the existing software and proposed method is in advanced.

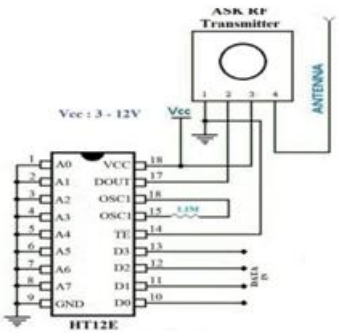


ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal



2.1 RF TRANSMITTER:

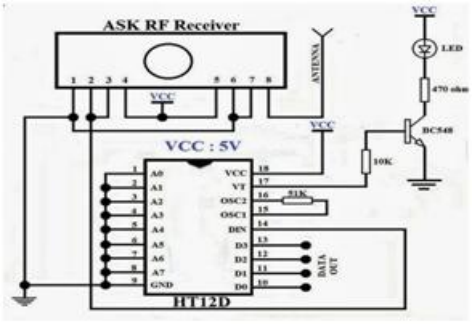
This simple RF transmitter, consisting of a 434MHz license-exempt Transmitter module and an encoder IC , was designed to remotely switch simple appliances on and off. The RF part consists of a standard 434MHz transmitter module, which works at a frequency of 433.92 MHz and has a range of about 400m according to the manufacture. The transmitter module has four pins. Apart from "Data" and the "VCC" pin, there is a common ground (GND) for data and supply. Last is the RF output (ANT) pin. Note that, for the transmission of a unique signal, an encoder is crucial. For this, I have used the renowned encoder IC HT12E from Holtek. HT12E is capable of encoding information which consists of N address bits and 12N data bits. Each address/ data input can be set to one of the two logic states. The programmed addresses/data are transmitted together with the header bits via an RF transmission medium upon receipt of a trigger signal. Solder bridges TJ1 and TJ2 are used to set the address and data bits.



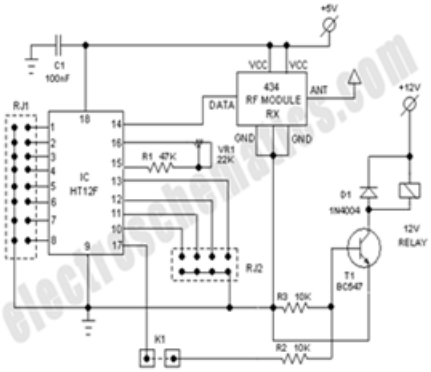
Rf transmitter

2.2 RF RECEIVER:

This circuit complements the RF transmitter built around the small 434MHz transmitter module. The receiver picks up the transmitted signals using the 434Mhz receiver module. This integrated RF receiver module has been tuned to a frequency of 433.92MHz ,exactly same as for the RF transmitter



Decoder



Rf Receiver

RS-232 CABLE:

The standard defines the electrical characteristics and timing of signals, the meaning of signals, and the physical size and pin out of connectors. The current version of the standard is TIA-232-F Interface Between Data Terminal Equipment and Data Circuit-Terminating Equipment Employing Serial Binary Data Interchange. When we look at the connector pin out of the RS232 port, we see two pins which are certainly used for flow control. These two pins are **RTS**, request to send and **CTS**, clear to send. With **DTE/DCE** communication (i.e. a computer communicating with a modem device) **RTS** is an output on the **DTE** and input on the **DCE.**

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

CTS are the answering signal coming from the **DCE.** Before sending a character, the **DTE** asks permission by setting its **RTS** output. No information will be sent until the **DCE** grants permission by using the **CTS** line. If the **DCE** cannot handle new requests, the **CTS** signal will go low. A simple but useful mechanism allowing flow control in one direction. The assumption is that the **DTE** can always handle incoming information faster than the **DCE**can send it. In the past, this was true. Modem speeds of 300 baud were common and 1200 baud was seen as a high speed connection. For further control of the information flow, both devices have the ability to signal their status to the other side. For this purpose, the **DTR** data terminal ready and **DSR** data set ready signals are present. The **DTE** uses the **DTR** signal to signal that it is ready to accept information, whereas the **DCE** uses the **DSR**signal for the same purpose. Using these signals involves not a small protocol of requesting and answering as with the **RTS/CTS** handshaking. These signals are in one direction only. The last flow control signal present in **DTE/DCE** communication is the **CD** carrier detect. It is not used directly for flow control, but mainly an indication of the ability of the modem device to communicate with its counter part. This signal indicates the existence of a communication link between two modem devices.

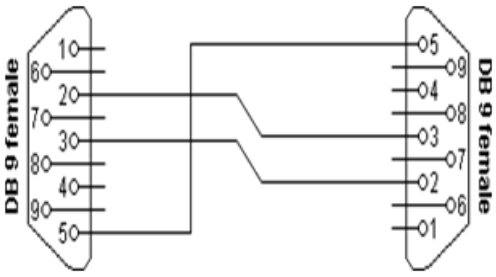


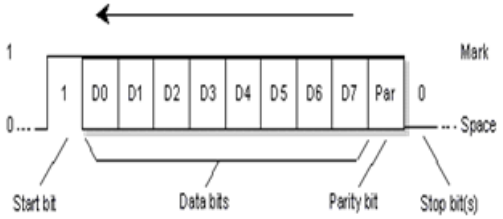
Fig: RS232 Handshaking Process

Connector 1	Connector 2	Function
2	3	Rx ← TX
3	2	TX → Rx
5	5	Signal ground

Simple RS232 without handshaking

3. SERIAL COMMUNICATION:

Serial communication is basically the transmission or reception of data one bit at a time. Today's computers generally address data in bytes or some multiple thereof. A byte contains 8 bits. A bit is basically either a logical 1 or zero. Every character on this page is actually expressed internally as one byte. The serial port is used to convert each byte to a stream of ones and zeroes as well as to convert a stream of ones and zeroes to bytes. The serial port contains a electronic chip called a Universal Asynchronous Receiver/Transmitter (UART) that actually does the conversion. The serial port has many pins. We will discuss the transmit and receive pin first.



Data transmission bits

INTRODUCTION:

Serial communication is basically the transmission or reception of data one bit at a time. Today's computers generally address data in bytes or some multiple thereof. A byte contains 8 bits. A bit is basically either a logical 1 or zero. Every character on this page is actually expressed internally as one byte. The serial port is used to convert each byte to a stream of ones and zeroes as well as to convert a stream of ones and zeroes to bytes. The serial port contains a electronic chip called a Universal Asynchronous Receiver/Transmitter (UART) that actually does the conversion The serial port has many pins. We will discuss the transmit and receive pin first. Electrically speaking, whenever the serial port sends a logical one (1) a negative voltage is effected on the transmit pin. Whenever the serial port sends a logical zero (0) a positive voltage is affected. When no data is being sent, the serial port's transmit pin's voltage is negative (1) and is said to be in a MARK state.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Note that the serial port can also be forced to keep the transmit pin at a positive voltage (0) and is said to be the SPACEor BREAK state. (The terms MARK and SPACE are also used to simply denote a negative voltage (1) or a positive voltage (0) at the transmit pin respectively).When transmitting a byte, the UART (serial port) first sends a STARTBIT which is a positive voltage (0), followed by the data (general 8 bits, but could be 5, 6, 7, or 8 bits) followed by one or two STOP Bits which is a negative(1) voltage. The sequence is repeated for each byte sent.

At this point you may want to know what the duration of a bit is. In other words, how long does the signal stay in a particular state to define a bit. The answer is simple. It is dependent on the baud rate. The baud rate is the number of times the signal can switch states in one second. Therefore, if the line is operating at 9600 baud, the line can switch states 9,600 times per second. This means each bit has the duration of 1/9600 of a second or about 100µsec. when transmitting a character there are other characteristics other than the baud rate that must be known or that must be setup

Signature Verification Procedure:

For Signature verification for both database image and current image was matched depend upon the feature values of the both images.For generating the feature values we apply histogram equalization and then we apply DWT(Discrete Wavelet Transformation) to images and then we apply correlation to them.

4. SIMULATION RESULTS:

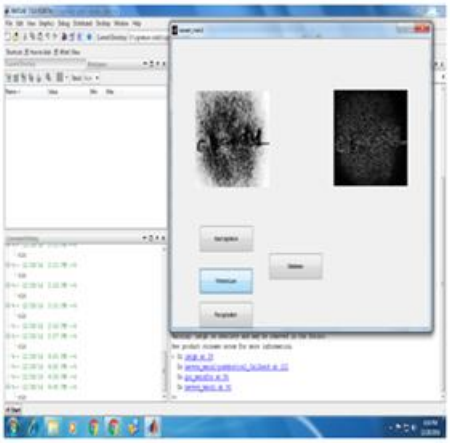
After making all possible connections and connecting hardware kit to the p.c the following observations are made

STEP 1:

After sending rf signal the rf receiver automatically decoded and below pop up is opened to select the signature for recognition

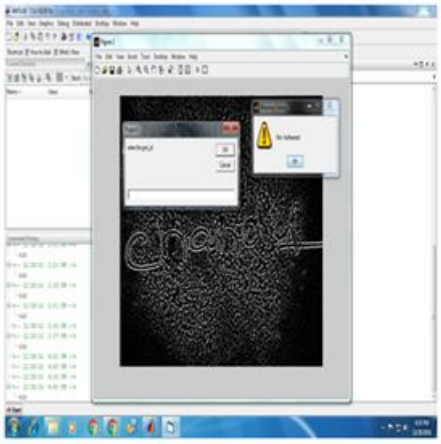
Step 2: Taking the database image signature for scanning

Step 3: Applying the werbers law

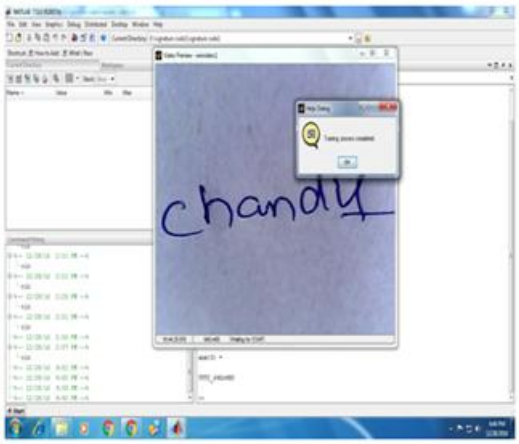


ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Step 4: after verifying signature is not matched, result displaying not authorized



Step 5: verifying the signature is matched, result is displayed successfully.



ADVANTAGESAND APPLICATIONS:

ADVANTAGES:

The main advantages of using online signature verification are

- Simple and easy to control the mobiles
- Low power consumption
- Easy to provide security to mobiles
- Effective in implementation

APPLICATIONS:

- Currency note checking applications
- Online monitoring applications
- Home monitoring applications
- Security applications

Conclusion:

The results demonstrate the problem of within-user variation of signatures across multiple images and the effectiveness of cross session training strategies to alleviate these problems.

REFERENCES:

[1]Napa Sae-Bae and NasirMemon, Fellow, IEEE ”Online signature verification on mobile device” IEEE transaction on information forensic and security, vol. 9, no. 6, june 2014.

[2]L. G. Plamondon and R. Plamondon, “Automatic signature verification and writer identification—The state of the art,” Pattern Recognit., vol. 22, no. 2, pp. 107–131, 1989.

[3]D. Guru and H. Prakash, “Online signature verification and recognition: An approach based on symbolic representation,” IEEE Trans. PatternAnal. Mach. Intell., vol. 31, no. 6, pp. 1059–1073, Jun. 2009.

[4]J. Fierrez, J. Ortega-Garcia, D. Ramos, and J. Gonzalez-Rodriguez, “HMM-based on-line signature verification: Feature extraction and signature modeling,” Pattern Recognit. Lett., vol. 28, pp. 2325–2334,Dec. 2007.

[5]E. ArgonesRua, E. Maiorana, J. Alba Castro, and P. Campisi, “Biometric template protection using universal background models: An application to online signature,” IEEE Trans. Inf. Forensics Security, vol. 7, no. 1,pp. 269–282, Feb. 2012.

[6]H. Feng and C. C. Wah, “Online signature verification using a new extreme points warping technique,” Pattern Recognit.Lett., vol. 24, no. 16, pp. 2943– 2951, 2003.

[7]N. Sae-Bae and N. Memon, “A simple and effective method for online signature verification,” in Proc. Int. Conf. BIOSIG, 2013,pp. 1–12.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

[8]N. Seabee, K. Ahmed, K. Isbister, and N. Memon, "Biometric-rich gestures: A novel approach to authentication on multi-touch devices,"

[9]H. Feng and C. C. Wah, "Online signature verification using a new extreme points warping technique," Pattern Recognit.Lett., vol. 24,no. 16, pp. 2943–2951, 2003.

[10]M. Faundez-Zanuy, "On-line signature recognition based on VQ-DTW," Pattern Recognit., vol. 40, no. 3, pp. 981–992, 2007.