Embedded Platform For Online Signature Verification

Sangeet Kumar, V.V.S.R.K.K. Pavan BH, M.Tech

M.TECH Student, Assistant Professor in Department of Electronics and Communication Engineering Kakinada Institute of Engineering and Technology-II, Eastgodavari Dist., A.P., INDIA

sangeet.mtec@gmail.com, bhavaraju.pavan5@gmail.com

Abstract — in my project the proposed system is used for verifying the signature of particular person with help of embedded platform on mobile devices. This paper studies online signature verification on PC interface-based mobile devices. 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 signatures are acquired using a digitizing tablet which captures both dynamic and spatial information of the writing. After preprocessing the signature, several features are extracted. The authenticity of a writer is determined by comparing an input signature to a stored reference set (template) consisting of three signatures. The similarity between an input signature and the reference set is computed using string matching and the similarity value is compared to a threshold. Several approaches for obtaining the optimal threshold value from the reference set are investigated. The results demonstrate the problem of within-user variation of signatures across multiple signatures and the effectiveness of cross session training strategies to alleviate these problems.

I. Introduction

HANDWRITTEN signatures are commonly used to approbate the contents of a document or to authenticate a financial transaction. Signature verification is usually done by visual inspection. A person compares the appearance of two signatures and accepts the given signature if it is sufficiently similar to the stored signature, for example, on a credit card. In the majority of situations where a signature is required, no verification takes place at all due to the amount of time and effort that would be required to manually verify signatures. Automating the signature verification process will improve the current situation and eliminate fraud. Digital signatures employ a type of asymmetric cryptography.

For messages sent through a non-secure channel, a properly implemented digital signature gives the receiver reason to believe the message was sent by the claimed sender. In many instances, common with Engineering companies for example, digital seals are also required for another layer of validation and security. Digital seals and signatures are equivalent to handwritten signatures and stamped seals.

Digital signatures are equivalent to traditional handwritten signatures in many respects, but properly implemented digital signatures are more difficult to forge than the handwritten type. Digital signature schemes, in the sense used here, are cryptographically based, and must be implemented properly to be effective. Digital signatures can also provide non-repudiation, meaning that the signer cannot successfully claim they did not sign a message, while also claiming their private key remains secret; further, some non-repudiation schemes offer a time stamp for the digital signature, so that even if the private key is exposed, the signature is valid.

Digitally signed messages may be anything representable as a bit string: examples include electronic mail, contacts, or a message sent via some other cryptographic protocol.

Figure: example of signature for preprocessing
II. Block Diagram:

III. Design Implementation Overview of the System

Connection-Less Authentication System:
A password is generated without connecting the client to the server. The phone will act as a token and use certain factors unique to it among other factors to generate a one-time password locally. The server will have all the required factors including the ones unique to each mobile phone in order to generate the same password at the server side and compare it to the password submitted by the client. The client may submit the password online or through a device such as an ATM machine. A program will be installed on the client’s mobile phone to generate the OTP.

SMS-Based Authentication System:
In case the first method fails to work, the password is rejected, or the client and server are out of sync, the mobile phone can request the one-time password directly from the server without the need to generate the OTP locally on the mobile phone. In order for the server to verify the identity of the user, the mobile phone sends information unique to the user to the server via an SMS message. The server checks the SMS content and if correct, returns a randomly generated OTP to the mobile phone. The user will then have a given amount of time to use the OTP before it expires. Note that this method will require both the client and server to pay for the telecommunication charges of sending the SMS message.

A. Standard Deviation
To understand standard deviation, we need a data set. Statisticians are usually concerned with taking a sample of a population. To use election polls as an example, the population is all the people in the country, whereas a sample is a subset of the population that the statisticians measure. The great thing about statistics is that by only measuring (in this case by doing a phone survey or similar) a sample of the population, you can work out what is most likely to be the measurement if you used the entire population. In this statistics section, I am going to assume that our data sets are samples of some bigger population. There is a reference later in this section pointing to more information about samples and populations. I could simply use the symbol \( \mu \) to refer to this entire set of numbers. If I want to refer to an individual number in this data set, I will use subscripts on the symbol \( \mu \) to indicate a specific number. There are a number of things that we can calculate about a data set. For example, we can calculate the mean of the sample. I assume that the reader understands what the mean of a sample is, and will only give the formula: All this formula says is “Add up all the numbers and then divide by how many there are”. Unfortunately, the mean doesn’t tell us a lot about the data except for a sort of middle point. For example, these two data sets have exactly the same mean (10), but are
E. Choosing components and forming a feature vector

In general, once eigenvectors are found from the covariance matrix, the next step is to order them by eigenvalue, highest to lowest. This gives you the components in order of significance. Now, if you like, you can decide to ignore the components of lesser significance. You do lose some information, but if the eigenvalues are small, you don’t lose much. If you leave out some components, the final data set will have less dimensions than the original. To be precise, if you originally have dimensions in your data, and so you calculate eigenvectors and eigenvalues, and then you choose only the first eigenvectors, then the final data set has only dimensions.

What needs to be done now is you need to form a feature vector, which is just a fancy name for a matrix of vectors. This is constructed by taking the eigenvectors that you want to keep from the list of eigenvectors, and forming a matrix with these eigenvectors in the columns.

F. Touch Screen:

The course ECE 476: Microcontroller Design requires many tools that allow its students to fully experience the possibilities of designing projects using Microcontrollers. In order for instructors to design laboratory experiments and demonstrations it is essential that he have the tools necessary to make them as easy to put together as possible. The goal of this project is select a low-cost graphical LCD and design a driver that would allow such experiments and demonstrations to be designed around it. In most of the experiments used for ECE 476, a 16x2 Crystalfontz Alphanumeric LCD is used as the major user output and represents the user interface. Alphanumeric LCDs display characters in pre-designated blocks and the LCD screen and this limits their use to simple number and character displays and crude images drawn from numbers or characters (a bouncing ball using the character ‘o’ or other such graphical techniques using text). While this is suitable for many applications, there are some which would benefit greatly from an easy to use graphical LCD. Most graphical LCDs are not supported by standard C libraries as are simple alphanumeric displays so it becomes much more time consuming to use them in projects.

This can be especially prohibitive during regular laboratory experiments because they are often designed to prove a specific instructive idea, and generating a driver for a graphical LCD cannot be done during the allotted time. This paper and project outline the design of a graphical LCD driver for the Crystalfontz CFAG12864B series (128 x 64 pixel) graphical display which can be easily modified to drive any Samsung KS0108 based graphical LCD.
G. Wireless Communication

A GSM modem is a wireless modem that works with a GSM wireless network. A wireless modem behaves like a dial-up modem. The main difference between them is that a dial-up modem sends and receives data through a fixed telephone line while a wireless modem sends and receives data through radio waves.

A GSM modem can be an external device or a PC Card / PCMCIA Card. Typically, an external GSM modem is connected to a computer through a serial cable or a USB cable. A GSM modem in the form of a PC Card / PCMCIA Card is designed for use with a laptop computer. It should be inserted into one of the PC Card / PCMCIA Card slots of a laptop computer. Like a GSM mobile phone, a GSM modem requires a SIM card from a wireless carrier in order to operate. As mentioned in earlier sections of this SMS tutorial, computers use AT commands to control modems. Both GSM modems and dial-up modems support a common set of standard AT commands. You can use a GSM modem just like a dial-up modem.

H. Signal Conditioner

A signal conditioner is a device that converts one type of electronic signal into another type of signal. Its primary use is to convert a signal that may be difficult to read by conventional instrumentation into a more easily read format.

In performing this conversion a number of functions may take place. They include:

Amplification

When a signal is amplified, the overall magnitude of the signal is increased. Converting a 0-10mV signal to a 0 -10V signal is an example of amplification.

Electrical Isolation

Electrical isolation breaks the galvanic path between the input and output signal. i.e. no physical wiring between the input and output. The input is normally transferred to the output by converting it to an optical or magnetic signal then it is reconstructed on the output. By breaking the galvanic path between input and output, unwanted signals on the input line are prevented from passing through to the output. Isolation is required when a measurement must be made on a surface with a voltage potential far above ground. Isolation is also used to prevent ground loops.

Linearization

Converting a non-linear input signal to a linear output signal. This is common for thermocouple signals.

Excitation

Many sensors require some form of excitation for them to operate. Strain gages and RTDs are two common examples. The signal conditioning unit accepts input signals from the analog sensors and gives a conditioned output of 0-5V DC corresponding to the entire range of each parameter. This unit also accepts the digital sensor inputs and gives outputs in10 bit binary with a positive logic level of +5V. The calibration voltages* (0, 2.5 and5V) and the health bits are also generated in this unit. The unit is powered through DCSTS unit.

The DCSTS unit controls the entire operation of a DCP field station. It consists of power supply regulator, timing generator, control logic circuit, multiplexer-cum-A/D converter, health monitor circuit, memory, pseudo-random burst sequence generator and a UHF transmitter. It operates on +12V uninterrupted power. The hourly sequence of operations performed by DCSTS is as given below:

a. Provides +12V switched power to signal conditioner 3 minutes and 30 sec prior to full hour.
b. Converts the calibration voltages and sensor data (outputs of signal conditioner) into digital form and stores in memory.
c. Generates one pseudo random burst command in each three minutes 3-sub-slot during the allotted ten minutes transmission window of a particular AWS, to enable the random transmission of stored data three times. These data along with station identification code, start and end signals are transmitted.

I. PIR Sensor:

PIR LED at 900nm-GaAlAs Infrared Light Emitting Diode. Shines invisible PIR light on the user’s eye PIR 900nm sensor. Light Detector-

Detects reflected PIR light. We decided to use blinking as we wanted the device to be functional for non-vocal or ventilated users (blowing or sucking was another option). Our first idea, and the one we implemented, was to use a led/photodiode paper to reflect light off the eye. We found that Optec Inc. makes a round receiver, consisting of a LED and a photo transistor mounted on the same unit. This detected a strong increase in signal upon blinking.

We were worried about detecting the difference between normal and intentional blinks, but we found that for most users the intentional blinks produced a much stronger signal, and they were always much longer the ~300ms normal blink duration.
I. flow chart:

IV. Conclusion

A system for on-line signature verification has been implemented. Experimental results on this data set conform the effectiveness of the proposed algorithm in mat lab section. Our signature database does not contain any data from skilled forgers. It is still unclear how such data should be collected. The results would be more valuable if true forgeries that imitate the shape of the original signature were available. Evaluations of human performance on distinguishing such a set of forgeries from the true signatures could provide a baseline for system performance evaluation. 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.

V. References


Authors:


Mr. V. V. S. R. K. R. Pavan.BH is Assistant professor with department of Electronics and Communication Engineering. He received the M.Tech degree in VLSI Design from KIET Engineering College. A.P., INDIA.