Augmented Reality Based Signature Verification

Krutika Kene[1] , Vrushti Raut[2], Suchita Jogdand[3] , *Aditi Raut

Department of Computer Engineering
St. John College of Engineering and Management

Abstract : The fact that the signature is widely used as a means of personal verification emphasizes the need for an automatic verification system. Verification can be performed either Offline or Online based on the application. Online systems use dynamic information of a signature captured at the time the signature is made. Offline systems work on the scanned image of a signature. We have worked on the Offline Verification of signatures using a set of shape based geometric features. The features that are used are Baseline Slant Angle, Aspect Ratio, Normalized Area, Center of Gravity, number of edge points, number of cross points, and the Slope of the line joining the Centers of Gravity of two halves of a signature image. Before extracting the features, preprocessing of a scanned image is necessary to isolate the signature part and to remove any spurious noise present. The system is initially trained using a database of signatures obtained from those individuals whose signatures have to be authenticated by the system. For each subject a mean signature is obtained integrating the above features derived from a set of his/her genuine sample signatures. This mean signature act as the template for verification against a claimed test signature. Euclidian distance in the feature space between the two. If this distance is less than a predefined threshold(corresponding to minimum acceptable degree of similarity),the signature is verified to be that of the claimed subject else detected as a forgery.

Keywords: Augmented Reality, Signature, Biometric, Computational Intelligence.

1. INTRODUCTION

Signature has been a distinguishing feature for person identification through ages. Signatures for long have been used for au become a national epidemic. Since commercial banks pay little attention to system capable of screening casual forgeries will prove authenticates documents based on the owners handwritten signature. Approaches to signature verification fall into two categories according to the acquisition of the data: On-line and Offline. On-line data records the motion of the stylus while the signature is produced, and includes location, and possibly velocity, acceleration and pen pressure, as functions of time. Online systems use this information captured during acquisition. These dynamic characteristics are specific to each individual and sufficiently stable as well as repetitive. Off-line data is a 2-D image of the signature. Processing Off-line is complex due to the absence of stable dynamic characteristics. Difficulty also lies in the fact that it is hard to segment signature strokes due to highly stylish and unconventional writing styles. The non- repetitive nature of variation of the signature, because of age, illness, geographic location and perhaps to some extent the emotional state of the person, accentuates the problem. All these coupled together cause large intra-personal variation. A robust system has to be designed which should not only be able to consider these factors but also detect various types of forgeries. The system should neither be too sensitive nor too coarse. It shouldhave an acceptable trade-off should neither be too sensitive nor too coarse. It should have an acceptable trade-off between a low False Acceptance Rate (FAR) and a low False Rejection rate (FRR).

2. RELATED WORK

In 2008, Wayne Read Alan McCabe Jarrod Treva than developed Handwritten Signature Verification using Neural Network: A number of biometric techniques have been proposed for personal identification in the past. Among the vision-based ones are face recognition, fingerprint recognition, iris scanning and retina scanning. Voice recognition

or signature verification are the most widely known among the non-vision-based ones. As signatures continue to play an important role in financial, commercial and legal transactions, truly secured authentication becomes more and more crucial. A signature by an authorized person is considered to be the seal of approval and remains the most preferred means of authentication. The method presented in this paper consists of image prepossessing, geometric feature extraction, neural network training with extracted features and verification. A verification stage includes applying the extracted features of test signature to a trained neural network, classify it as a genuine or forged.

In 2016, Samit shivadekar, Stephen Raj Abraham developed Document Validation and Verification System: 'E-Governance system will be an online platform for deliverance Government to Citizen Services and storage of digital certificates, documents etc. The system consists of a Digi Vault [Digital Storage] website which can be linked with different websites of various government departments. In this Project the Documents generated by the government will be digitally signed and verified by government authority entitled for the same. Digital Signature of documents will be implemented through Public Key Infrastructure. Certificates serve as identity of an individual for a certain purpose, e.g. a drivers license identifies someone who can legally drive in a particular country. Likewise, a Digital Signature Certificate (DSC) can be presented electronically to prove your identity or your right to access information or services on the Internet. Document Validation will be provided at the user end where he wants to apply for certain governments documents like Pan Card and Licenses.

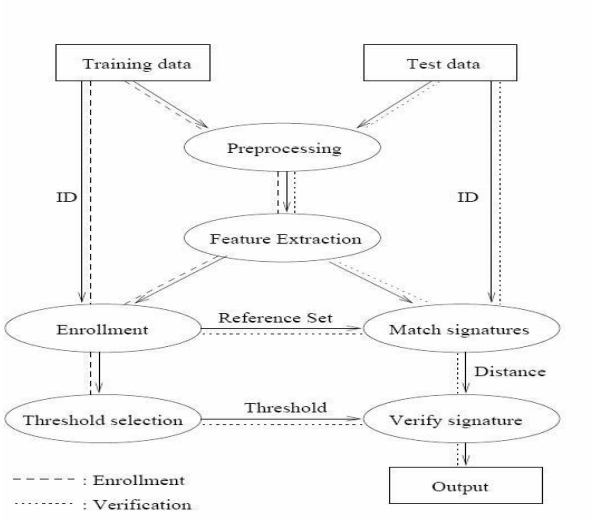
In 2017, Luiz G. Hafemann, Robert Sabourin and Luiz S. Oliveira developed Offline Handwritten Signature Verification: The area of Handwritten Signature Verification has been broadly researched in the last decades, but remains an open research problem. The objective of signature verification systems is to discriminate if a given signature is genuine (produced by the claimed individual), or a forgery (produced by an impostor). This has demonstrated to be a challenging task, in particular in the offline (static) scenario, that uses images of scanned signatures, where the dynamic information about the signing process is not available. Many advancements have been proposed in the literature in the last 5-10 years, most notably the application of Deep Learning methods to learn feature representations from signature images. In this paper, we present how the problem has been handled in the past few decades, analyze the recent advancements in the eld, and the potential directions for future research.

In 2018, Raul Sanchez-Reillo, Judith Liu-Jimenez, Ramon Blanco-Gonzalo developed Forensic Validation of Biometrics Using Dynamic Handwritten Signatures: Forensic examination of handwritten signatures is an important task that has been used to resolve conflicts for centuries. The incorporation of new technologies into the process of signing documents has created new challenges for this task. In particular, the use of electronic capture devices may compromise the capabilities of forensic examination. However, the forensic examination may not be challenged and may even be improved if, in addition to the signature graph, the temporal signals that are generated during the process of signing are captured. In biometric terms, the acquisition and processing of such temporal signals are referred to as dynamic signature biometric recognition. Unfortunately, the data are captured in a format that a forensic examiner is unable to understand. Therefore, there is a need of adapting this information to allow a forensic examiner to manipulate it and obtain the required measurements. This paper explains this need using the design and development of a desktop application as the guiding thread. After covering this need, a forensic examiner can extract the relevant graphometry features that are necessary for applying graphonomics to signatures and determining the authenticity of a questioned signature compared with a certain signature.

3. PROPOSED SYSTEM

We approach the problem in two steps. Initially a set of signatures are obtained from the subject and fed to the system. These signatures and the mean value of these features is obtained. In the next step the scanned signature image to be verified is fed to the system. It is pre-processed to be suitable for extracting features. It is fed to the system and various features are extracted from them. These values are then compared with the mean features that were used to train the system. The Euclidian distance is calculated and a suitable threshold per user is chosen.

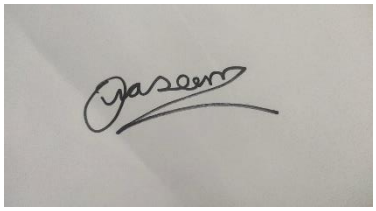
Depending on whether the input signature satisfies the threshold condition the system either accepts or rejects the signature. Pre-processed Then the pre- processed images are used to extract relevant geometric parameters that can distinguish signatures of different persons. These are used to train the system, deals with the prep-processing steps and explains the features that are extracted followed by the verification procedure explained below. Implementation details and simulation results are also listed. A flow chart illustrating the various steps that have been used is shown below.

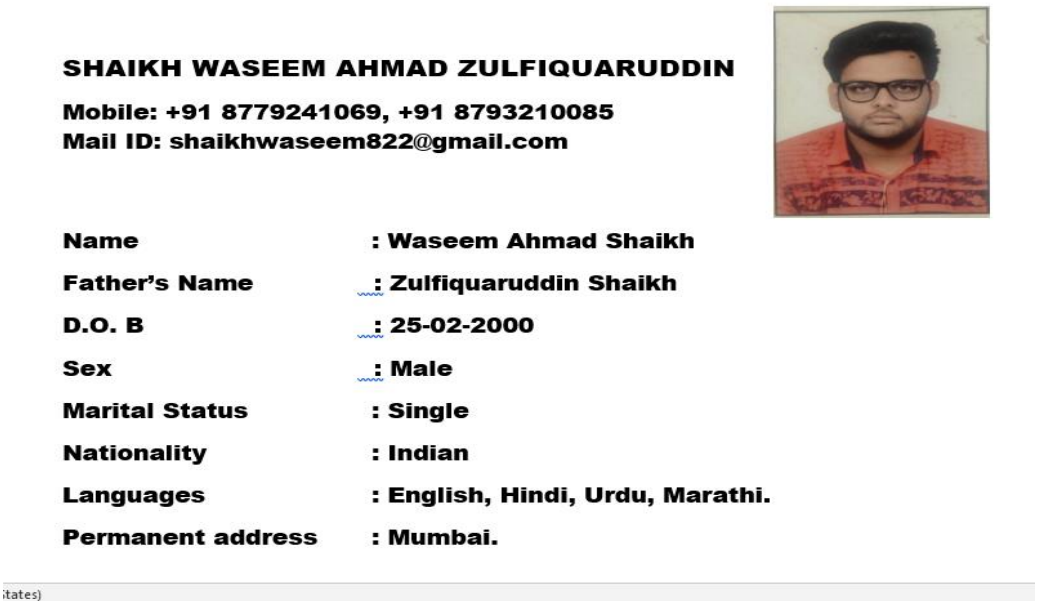


4. Data Collection & Pre-processing

Data Collection: Research involves the Database of about 22 Signatures which was built by collecting Signatures from 22 respective people. The Database was collected by means of a form or survey were the details like Name, Address, Office Address, Photograph, Designation and two Signatures per person was collected respectively. Collected Data was then stored in the JPG format for further use in the research work. The following are some the few examples of the Database of 22 Respective individuals that has been used in this research

Here are 1 out of 22 signatures and forms filled by the respective individuals has been shown they are as follows





Pre-processing: The scanned signature image may contain spurious noise and has to be removed to avoid errors in the further processing steps. The gray image Io of size M*N is inverted to obtain an image Ii in which the signature part consisting a row averaging process to generate the row averaged image Ira, which is given by, values between that of background and foreground. These are removed by performing of higher gray levels forms the foreground.

$$I_i(i,j) = Io, max - Io(i,j)$$

Where , is the maximum gray-level. The background, which should be ideally dark, may consist of pixels or group of pixels with gray.

$$I_r(i,j) = I_i(i,j) - {}_{I=1}\sum^{M} I_i(i,j)/M$$

$$I_rn(i,j) = I_r(i,j) if I_r(i,j) > 0$$

=0 otherwise

Further noise removal and smoothening is achieved using an n*n averaging filter to generate the cleaned image.

1. The gray image is converted into binary image by using automatic global thresholding. Following algorithm [5] was used to automatically calculate the global threshold: An initial value, midway between the maximum and minimum grey level value, was selected for the threshold T.

$$I_a(i,j) = 1/9(I = i = 1 \sum^{i+1} k)$$

$$0$$

$$= j - 1 \sum^{j+1} I_ra(l,k)$$

$$0$$

2. Image was segmented using T.
3. Average gray level values 1 and 2 for the two groups of pixels was computed.
4. Based on step 3, new threshold value was computed.

$$T = 0.5 * (u1 + u2)$$

Steps 2 through 4 were repeated until the difference in T in successive iterations was smaller than 0.5.

5. VERIFICATION

The values derived from each sample group are used in deriving a mean signature for each subject. The mean values and standard devia- tions of all the features are computed and used for final verification. A user defined threshold corresponding to the minimum acceptable degree of similarity for each person was manually estimated. Since users do not like their original signatures to get rejected, we chose the threshold on the lower side to avoid rejection of original signatures. Let and denote the mean and standard deviation for the feature and denote its value for the query image. The Euclidian distance in the feature space measures the proximity of a

query signature image to the mean signature image of the claimed person.

$$\delta = \left(\frac{1}{n}\right)_{i=1} \sum^{n} [(F_i - \mu_i)/\sigma_i]^2 \ldots\ldots (9)$$

If this distance is below a certain threshold then the query signature is verified to be that of the claimed person otherwise it is detected as a forged one.

6. EXPECTED RESULT:

Below are the results that has been captured from the Desktop Windows screen with their respective inputs.

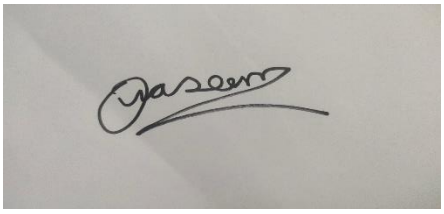


Figure 6.1: Input Signature 1

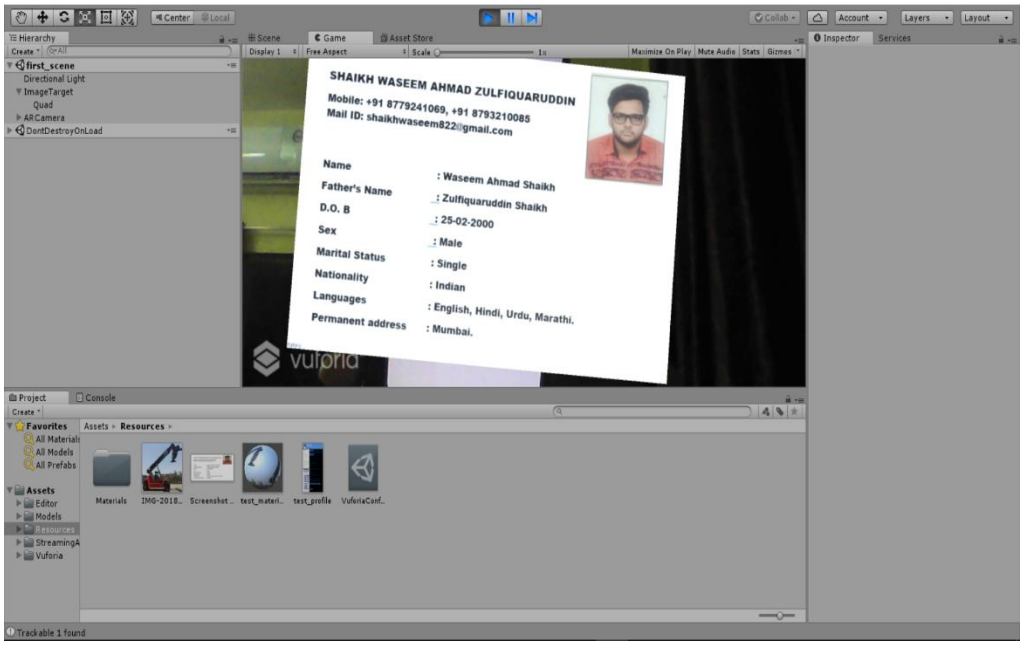


Figure 6.2: Output 1 on Windows

7. CONCLUSION AND FUTURE WORK

The algorithm developed by us, uses various geometric features to characterize signatures that effectively serve to distinguish signatures of different persons. The system is robust and can detect random, simple and semi-skilled forgeries but the performance deteriorates in case of skilled forgeries. Using a higher dimensional feature space and also incorporating dynamic information gathered during the time of signature can also improve the performance. The concepts of Neural Networks as well as Wavelet transforms hold a lot of promise in building systems withhigh accuracy.

.

REFERENCES

8.1 Journal Article

[1] Luiz G. Hafemann1, Robert Sabourin1and Luiz S. Oliveira21 Ecole de technologie sup ´ erieure, Universit ´ e du Qu ´ ebec, Montreal, Canada ´e-mail: lghafemann@livia.etsmtl.ca, robert.sabourin@etsmtl.ca2 Federal University of Parana, Curitiba, PR, Brazil ´e-mail: luiz.oliveira@ufpr.br

[2] Samit Shivadekar (IT, SIES GST, Navi Mumbai, India,)Stephen Raj Abraham (IT, SIES GST, Navi Mumbai, India,)Sheikh Khalid (IT, SIES GST, Navi Mumbai, India)

[3] Forensic Validation of Biometrics Using Dynamic Handwritten Signatures RAUL SANCHEZ-REILLO , (Member, IEEE), JUDITH LIU-JIMENEZ,AND RAMON BLANCO-GONZALReceived April 23, 2018, accepted June 4, 2018, date of publication June 21, 2018, date of current version July 12, 2018.

[4]Aishwarya Mali1, Chinmay Mahalle2, Mihir Kulkarni3, Tejas Nangude4, Prof. Geeta Navale51234 Final Year Student, Department of Computer Engineering, Sinhgad Institute of Technology and Science, Maharashtra, India5 Project Guide, Department of Computer Engineering, Sinhgad Institute of Technology and Science, Maharashtra, India 5 May 2017

[5]•Tomasz PałysMilitary University of Technolog•Artur ArciuchMilitary University of Technology September 2019