AR BASED SIGNATURE VERIFICATION

Waseem Shaikh[1], Raghuvar Nishad[2], Shobha Rai[3], Surayya Shaikh[4]

Department of Computer Engineering, Theem College of Engineering

---***---

Abstract - *Human signatures have been shown to be the most significant factor in gaining entry. The importance of a person's signature as a biometric feature that can be used to authenticate human identity has been confirmed. Face recognition, fingerprint detection, iris examination, and retina scanning are only a few of the biometric characteristics that can be used to establish one's identity. Among the non-vision-based ones, voice recognition or signature authentication are the most well-known. Since signatures are becoming increasingly important in financial, commercial, and legal transactions, truly secure authentication is becoming increasingly important. The "seal" is described as a signature by an approved individual. and is still the most common method of identification. Online signature systems make use of complex information captured at the time the signature is generated. The scanned picture of a signature is used by offline systems. We've been working on Offline Signature Verification using a collection of shape-based geometric features. Baseline Slant Angle, Aspect Ratio, Normalized Area, Center of Gravity, number of edge points, number of cross points, and the Slope of the line connecting the Centers of Gravity of two halves of a signature picture are the features that are used. Preprocessing of a scanned image is needed before extracting the features in order to isolate the signature part and eliminate any spurious noise. The system is trained using a database of signatures collected from those whose signatures must be authenticated by the system at first. A mean signature is calculated for each subject by combining the above features extracted from a collection of his or her genuine sample signatures. This bogus signature serves as a template for comparing it to a claimed test signature. In the feature space between the two, there is a Euclidian gap between them. If the difference between the signature and the claimed subject is less than a predetermined threshold (corresponding to the minimum reasonable degree of similarity), the signature is validated to be that of the claimed subject; otherwise, it is detected as a forgery. The report includes information on pre-processing as well as the above-mentioned functionality, as well as implementation details and simulation performance.*

***Key Words*: Augmented Reality, Signature, Biometric, Computational Intelligence**

1.INTRODUCTION

Throughout history, a person's signature has served as a distinguishing characteristic for identifying them. Signatures have long been used for au, which has now spread throughout the country. Since commercial banks pay no attention to systems capable of detecting forgeries, documents would be proved authenticated by the owner's handwritten signature. Signature authentication methods are divided into two groups based on how the data is collected: online and offline. On-line data tracks the movement of the stylus as it creates the signature, including location, velocity, acceleration, and pen pressure as functions of time. Online applications make use of the data gathered during the acquisition process. These complex characteristics are unique to each individual and are both stable and predictable. A 2-D image of the signature is stored as off-line info. Since there are no stable dynamic characteristics, processing off-line is difficult. The fact that it is difficult to segment signature strokes due to extremely stylish and unusual writing styles adds to the difficulty. The problem is exacerbated by the non-repetitive nature of signature variance caused by age, disease, geographic location, and perhaps to some degree the person's emotional state. When both of these factors are combined, there is a lot of intra-personal variation. A robust framework must be developed that can not only take these factors into account but also identify different forms of forgeries. The machine should not be too sensitive or overly coarse. It should strike a reasonable balance between being neither too sensitive nor too coarse. It should strike a good balance 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: In the past, a variety of biometric methods for personal recognition have been suggested. Face recognition, fingerprint recognition, iris scanning, and retina scanning are examples of vision-based technologies. Among the non-vision-based ones, voice recognition or signature authentication are the most well-known. Given the importance of signatures in financial, commercial, and legal transactions, truly safe authentication is becoming increasingly necessary. A seal of approval is called a signature by an approved individual, and it is still the most common method of authentication. Image prepossessing, geometric feature extraction, neural network training with extracted features, and verification are all part of the approach discussed in this paper. The extracted features of the test signature are fed into a qualified neural network, which classifies it as genuine or forged.

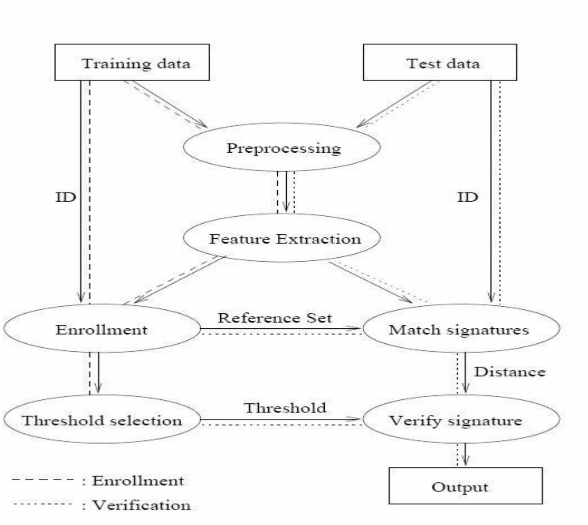
In 2016, Samit shivadekar, Stephen Raj Abraham developed Document Validation and Verification System: 'The e-Government system will be an online platform for delivering government services to citizens and storing digital certificates, records, and other information. The framework is made up of a Digi Vault [Digital Storage] website that can be connected to various government departments' websites. Documents created by the government will be digitally signed and validated by government authorities who are authorized to do so. Public Key Infrastructure can be used to introduce document digital signatures. Certificates act as proof of an individual's identification for a specific purpose; for example, a driver's license recognizes someone who is legally permitted to drive in a specific nation. Similarly, you can use a Digital Signature Certificate (DSC) to confirm your identity or your right to access information or services on the Internet. Document validation would be available at the user's end when applying for government documents such as Pan cards and licenses.

In 2017, Luiz G. Hafemann, Robert Sabourin and Luiz S. Oliveira developed Offline Handwritten Signature Verification: Handwritten Signature Verification has gotten a lot of attention in recent decades, but it's still a work in progress. Signature verification systems are used to determine if a signature is genuine (created by the alleged individual) or a forgery (produced by an impostor). This has proven to be a difficult task, especially in the offline (static) scenario, which uses images of scanned signatures and does not have access to dynamic information about the signing process. In the last 5-10 years, several advances have been proposed in the literature, most notably the use of Deep Learning approaches to learn feature representations from signature images. In this paper, we discuss how the issue has been addressed over the last few decades, as well as recent advances in the field and future research directions.

In 2018, Raul Sanchez-Reillo, Judith Liu-Jimenez, Ramon Blanco-Gonzalo developed Forensic Validation of Biometrics Using Dynamic Handwritten Signatures: Handwritten signature forensic analysis is a vital task that has been used to settle disputes for decades. The introduction of emerging technology into the signing process has posed new challenges for this mission. The use of electronic capture devices, in particular, can jeopardise forensic analysis capabilities. However, if the temporal signals produced during the signing process are recorded in addition to the signature graph, the forensic analysis will not be questioned and may even be strengthened. The acquisition and processing of such temporal signals is referred to as dynamic signature biometric recognition in biometric terminology. Unfortunately, the information is stored in a format that a forensic investigator cannot comprehend. As a result, this data must be adapted in order for a forensic examiner to manipulate it and obtain the necessary measurements. This paper illustrates this requirement by focusing on the design and creation of a desktop application. After addressing this requirement, a forensic examiner may extract the pertinent graphometry features required for applying graphonomics to signatures and evaluating the validity of a questioned signature in comparison to a known signature

3. PROPOSED SYSTEM

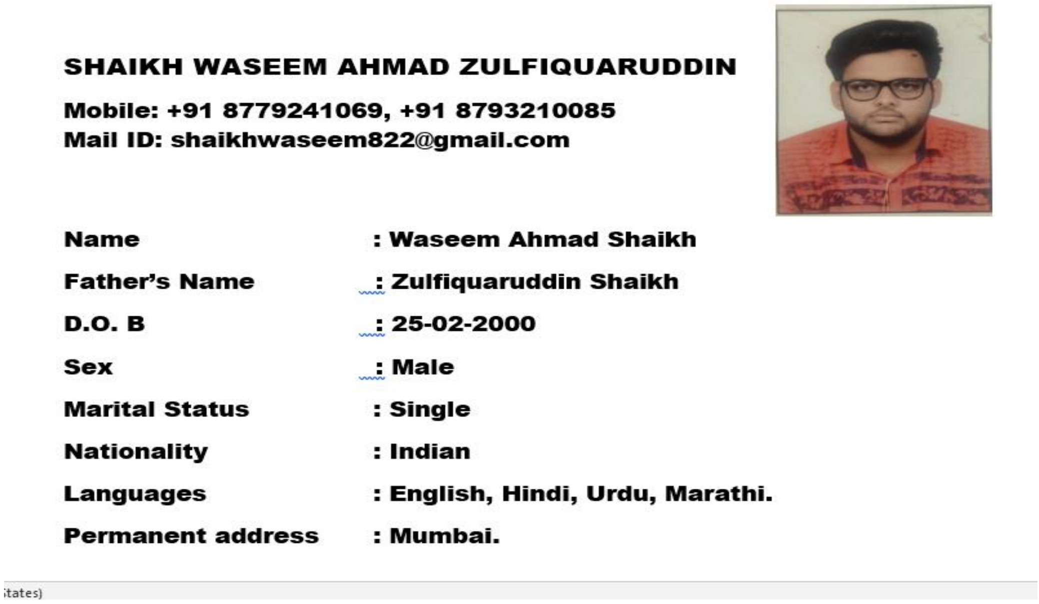
The problem is approached in two stages. Initially, the subject's signatures are collected and fed into the device. These signatures are collected, as well as the mean value of these functions. The device is then fed the scanned signature image that needs to be checked. It has been pre-processed to make it suitable for feature extraction. It is fed into the machine, and different characteristics are extracted. The mean features that were used to train the device are then compared to these values. The Euclidian distance is determined, and for each user, a suitable threshold is selected. The device either accepts or refuses the input signature depending on whether it meets the threshold condition. Prepared in advance the pre-processed images are then used to extract relevant geometric parameters that can be used to differentiate between various people's signatures. These are used to train the machine, deal with the prep-processing steps, and clarify the features that are extracted, all of which are followed by the verification procedure described below. There are also implementation information and simulation results mentioned. Below is a flow chart that depicts the different measures that were taken.



4. Data Collection & Pre-processing

The study uses a database of approximately 22 signatures that was generated by gathering signatures from 22 different individuals. The database was compiled using a form of survey that asked for information such as name, address, office address, photograph, designation, and two signatures per person. The data was then saved in JPG format for use in future research projects. The following are a few examples from the Database of 22 Respectful Individuals that was used in this study.

The following are examples of one of 22 signatures and forms filled out by the respective individuals:

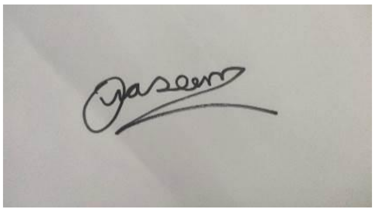


SHAIKH WASEEM AHMAD ZULFIQUARUDDIN

Mobile: +91 8779241069, +91 8793210085
Mail ID: shaikhwaseem822@gmail.com

Name	**: Waseem Ahmad Shaikh**
Father's Name	**: Zulfiquaruddin Shaikh**
D.O. B	**: 25-02-2000**
Sex	**: Male**
Marital Status	**: Single**
Nationality	**: Indian**
Languages	**: English, Hindi, Urdu, Marathi.**
Permanent address	**: Mumbai.**

itates)



4.1 Pre-processing:

To prevent errors in the subsequent processing steps, spurious noise in the scanned signature image must be eliminated. The grey image Io of size M*N is inverted to produce an image Ii, with the signature element consisting of a row averaging process to produce the row averaged image Ira, which is provided by values between background and foreground. Higher grey levels from the foreground are used to suppress these.

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

Where is the highest gray-level and is the maximum gray-level. The backdrop, which should preferably be black, may be made up of grayscale pixels or groups of pixels..

$$Ir(i, j) = Ii(i, j) - I = 1\ \Sigma\ Ii(i, j)/M \qquad M$$

$$Irn(i, j) = Ir(i, j) if\ Ir(i, j) > 0$$

$$= 0\ otherwise$$

To generate the cleaned image, a n*n averaging filter is used to remove more noise and smooth it out.

1. Using automatic global thresholding, the grey image is transformed to a binary image. The global threshold was calculated automatically using the following algorithm [5]: For the threshold T, a value was chosen that was halfway between the maximum and minimum grey level value.

$$i{+}1$$

$$Ia(i, j) = 1/9(I = i = 1 \qquad k)$$

$$0$$

$$j{+}1$$

$$= j - 1 \qquad Ira(l, k)$$

$$0$$

1. Image was segmented using T.
2. Average gray level values 1 and 2 for the two groups of pixels was computed.
3. 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:

Each subject's mean signature is calculated using the values obtained from each sample set. Many of the features' mean values and standard deviations are measured and used for final verification. Each person's minimum appropriate degree of similarity was manually calculated using a user-defined threshold. Since users don't like it when their original signatures are rejected, we set the threshold low to prevent rejection of original signatures. Let and stand for the feature's mean and standard deviation, respectively, and for the query image's value. In feature space, the Euclidian distance determines how near a question signature image is to the stated person's mean signature image.

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

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.

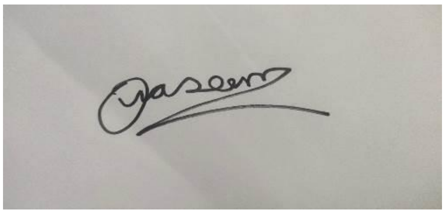
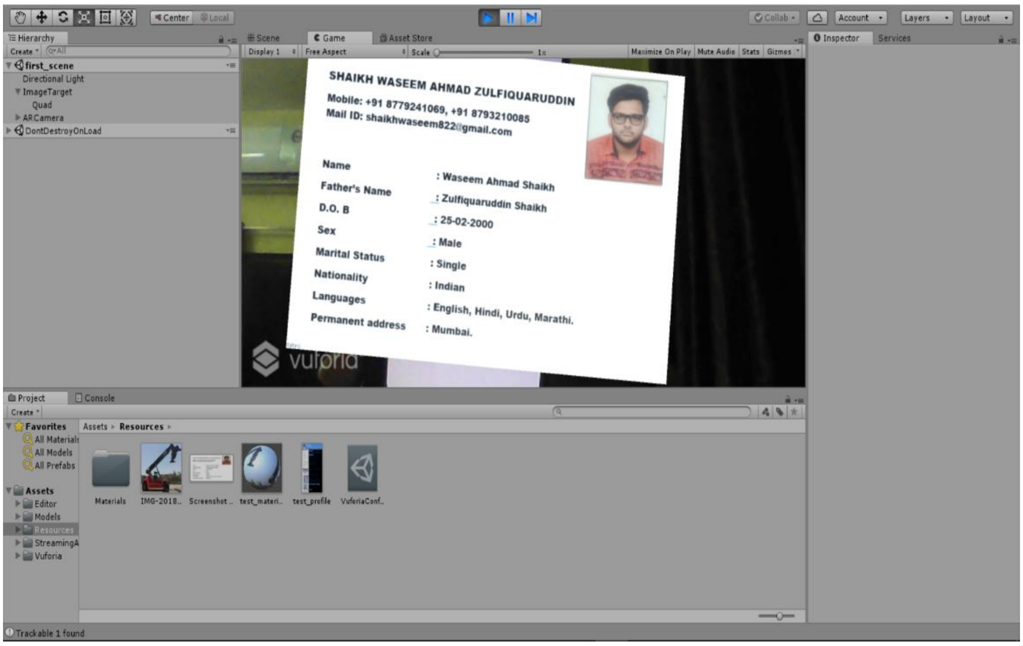


Figure 6.1: Input Signature 1



SHAIKH WASEEM AHMAD ZULFIQUARUDDIN
Mobile: +91 8779241069, +91 8793210085
Mail ID: shaikhwaseem822@gmail.com

Name : Waseem Ahmad Shaikh
Father's Name : Zulfiquaruddin Shaikh
D.O. B : 25-02-2000
Sex : Male
Marital Status : Single
Nationality : Indian
Languages : English, Hindi, Urdu, Marathi.
Permanent address : Mumbai.

Figure 6.2: Output 1 on Windows

7. CONCLUSION AND FUTURE WORK

Signatures are verified based on parameters extracted from the signature using various techniques in which we will collect small databases of signatures and our first step will be to capture a human signature and scan it using a webcam, presenting it in image format, and then we will do pre-processing of that capture image, using techniques such as Scaling. Our next step will be to remove features from the images after we've completed all of these functions. Our next step is to extract some important features from that image, such as global features, texture features, and mask features. The algorithm we developed uses a variety of geometric features to classify signatures, which effectively distinguishes signatures from one another. The system is reliable and can detect forgeries that are random, plain, or semi-skilled, but its efficiency degrades when it comes to skilled forgeries. Using a higher-dimensional feature space and integrating dynamic data collected during the signature process can also help to enhance efficiency.

REFERENCES

Journal Article

[1] Plamondon, R., and Lorette, G.: The state of the art in automatic signature authentication and writer recognition. Pattern Recognition, vol. 22, no. 1, pp. 107–131 (2018)

[2] Use of dynamic features for signature authentication, W. Nelson and E. Kishon. 201–205 in Proc. of the IEEE Intl. Conf. on Systems, Man, and Cybernetics, vol. 1. (2016)

[3] The CRPT algorithm is used to authenticate and verify digital signatures on smart phones. Prof.Geeta Naval, Aishwarya Mali, Chinmay Mangude4 04th volume (2017)

[4] Sandra Blakeslee, "Behind the Curtain of Thought: Advances in Brain Research; Timetable May Be Critical in Brain's Early Development." 1995, The New York Times.

[5] Patrice Simard, Kumar Chellapilla, and Sidd Puri. Convolutional neural networks with high efficiency for document processing. International Workshop on Handwriting Recognition Frontiers, 2006

[6] Ciresan, D. C., Meier, J. Masci, and Schmidhuber, J. A trac sign classification committee made up of neural networks. Pages 1918–1921, International Joint Conference on Neural Networks (IJCNN), 2011