A Survey on Offline Signature Verification

Madhuri Yadav, Alok Kumar, Tushar Patnaik, Bhupendra Kumar

Abstract—In the era of growing technology, security is the major concern to avoid fakes and forgeries. There are various biometric systems which help in personal identification, amongst those verification systems, one system is Signature Verification System. Signatures can be verified using online and offline systems. This paper explains the significance of offline systems and presents the survey of various approaches related to offline signature verification systems. Further, this paper provides the comparison of those approaches along with the features used, to help the researchers working in this field.

Index Terms—Data Training, Forgery, Global Features, Local Features, Signature Verification.

I. INTRODUCTION

Signatures act as a strong authentication feature of the signer and thus, preserve their valuable assets such as authenticating bank cheques, attendance monitoring, property documents and other confidential documents. But, the manual verification of signatures by humans is a difficult task. Thus, an automated Signature verification system is required which will improve the authentication process and provide secure means for authorization of legal documents. The objective of signature verification system is to discriminate between two classes i.e. original and forgery. These automated systems are designed based upon two techniques: online and offline. In online systems signer signs on the electronic pad and the dynamic characteristics such as writing speed, stroke length, pressure applied are extracted at that particular instant only [1], whereas, in offline systems extraction of dynamic data is not so easy because the input to this system will be 2-D image of the signature and the dynamic information will not be available. Due to lack of information it is very tough to provide accuracy in offline systems. Despite of this, offline systems are designed because they provide various advantageous over online systems such as absence of signer during signature verification because the signed signatures are compared with template signatures already stored in the database at the time of data training. The two types of variation found in the signatures are: Inter personal and Intra personal variability. The variation among the signatures of the same person is called as Intra personal variation. This variation can be due to age, illness, time, eather or other abnormal conditions and the variation between the originals and the forgeries is called Inter personal variations. A signature forgery means an attempt to copy someone else’s signature and use them against him to steal his identity there can be basically three types of forgeries [2]:

- Random Forgeries: the signer just knows the name of the person whose signature is to be signed.
- Simple forgeries: the signer knows the signature shape and has seen the signature examples prior to signing.
- Skilled forgeries: the signer knows the signature shape very well and has practiced the signature prior to signing it.

Signature verification cannot be done by character recognition because the alphabets of signature cannot be read out separately and it appears as an image with some curves representing the writing style of an individual. So, a signature image can be considered as a special distribution of pixels representing writing style rather than a collection of alphabets. Thus, separate approaches were required for signature recognition and character recognition. The rest of the paper is structured as follows. The parameters for signature verification concept are explained in Section II, Section III discusses various signature verification techniques, Section IV compares their results and then the conclusion is derived.

II. SIGNATURE VERIFICATION BASIC CONCEPTS

The main phases of the signature verification follow the sequence:

- (a) Preprocessing,
- (b) Feature Extraction,
- (c) Data Training and
- (d) Signature verification.

A: Preprocessing:

Preprocessing is the set of subsequent operations applied for the improvement of quality of signature image [2], [5]. This improvement in quality of image increases the accuracy of further steps involved in processing without losing relevant information. It improves the quality of elements of the digital images called pixels. The various sub-processes which can be considered in image preprocessing are Binarization, Noise removal, Skeletonization, Skew removal etc. [5]. The above sub-processes may vary according to the approach used.

B: Feature Extraction:

Feature means similar characteristics and Extraction means accurately retrieve those features. A proper feature extraction can increase the recognition ratio. It plays an
important role in development of the robust system as all other phases are based on these features. This phase can be based on following types of features: Global features [4], Local features [4] and Transition feature [6].

- Global features describe the entire signature image such as width, height, aspect ratio. These features are used in combination with other features. These features are less sensitive to noise [1].
- Local features describe the properties of signature image in specific parts. They are calculated by partitioning the signature image into parts by help of geometric center or some other means.
- Transition features counts the transition in the signature image from ‘black’ to ‘white’ pixel or vice versa in binarised signature images. It is used in combination with the above features.

C: Data Training and Verification:

Data Training is the stage in which the signature database is created by collecting signatures from the individuals. This collection involves both forgeries and original signatures. From these signatures, feature vectors are generated which acts as template for verification stage. Signature verification authenticates the individuals by comparing their signatures with the features stored in the database as templates. To generate the output of the system and to compare their approaches with others, the researchers have introduced a technique which divides the signature in two classes [3]: Class I and Class II. Class I represent genuine signature set and Class II represent forgery signature set. For Performance evaluation usually four types of categories are considered:

- False rejection
- False Acceptance
- True rejection
- True acceptance

Thus, in total, there are four error rates: False rejection rate (FRR), False Acceptance Rate (FAR), True Rejection Rate (TRR), True acceptance Rate (TAR) based on these error rates the results of various approaches have been analyzed and techniques have been specified.

III. DIFFERENT SIGNATURE VERIFICATION TECHNIQUES

Dr. Daramola Samuel [5], used 100 genuine signatures and 200 forged signatures in his database [5], the signature image was partitioned into 64 cells based upon center of gravity. Then three feature vectors were developed for each cell namely, image cell size (F1), image center angle relative to the cell lower right corner (F2) and pixels normalized angle relative to the lower right corner (F3). Further for the training stage, they proposed an algorithm which calculated threshold for each feature vector. The classification stage is based on calculation of Euclidean distance of the test signature with template signature. If the distance was less than the threshold then the input signature was accepted otherwise rejected. The FAR for skilled signatures was 1% and FRR for genuine signatures was 0.5% [5]. Ibrahim S. I. Abuhaiba [6], this approach presents a signature verification method that depends on the raw binary pixel intensities instead of complex set of features. In this approach, signature verification problem is viewed as a graph matching problem, for which the Hungarian method was used to solve. The method was tested using genuine and forgery signatures produced by five subjects. Three types of tests were conducted: (1) genuine test, where genuine signatures were verified, (2) random forgery test, where for every subject, all genuine signatures of all other subjects are considered random forgeries of signature of the subject under consideration, and (3) skilled forgery test, where for every subject, skilled forgeries are tested. An equal error rate of 26.7% and 5.6% for skilled and random forgeries, respectively, was achieved at size 32 × 64 pixels. A positive property of their algorithm is that the false acceptance rate of random forgeries vanishes at the point of equal false rejection and skilled forgery false acceptance rates. Sepideh Afsharoddost [7], used geometric center features concept. This technique used vertical splitting, horizontal splitting and diagonal splitting. Six center points were computed both for horizontal and vertical splitting, similarly diagonal splitting provided eight points, and in total twenty feature points were used to authenticate the signatures. Diagonal splitting was very sensitive to rotation and size of samples should be well rotated and normalized before training and testing. In the classification stage he used statistical approaches such as variance and standard deviation for calculations of thresholds. After estimating thresholds in the training stage, the testing stage proceeds by comparing the thresholds of trained signature with the threshold of incoming signature. If the incoming signature’s threshold was less than trained threshold the signature was accepted otherwise it was rejected. The skilled FAR was 15% and unskilled FAR was 10%. Bradley Schafer and Serestina Viriri [1], their approach used global and transition features. Global features which were used included normalized area of the signature, maximum histogram, aspect ratio, centroid feature, and number of edge points, trisurface feature and six-fold feature. In combination with global and transition features a feature vector of 25 dimensions was created. The results given in this paper are obtained using the “Grupo de Procesado Digital de Senales” (GPDS) signature database. The verification of the signature was accomplished by using Euclidean distances. They used global and local thresholds and using the global threshold they obtained a correct classification rate of 73% and a false acceptance rate of 18.5%. Using the second approach, the localized threshold, they obtained a correct classification rate of 84.1% and a false acceptance rate of 17.8%. Ramachandra C, Jyothi Srinivasa Rao, K B Raja, K R Venugopla and L M Patnaik [2], They worked to produce a robust offline signature verification system in which only global features like
maximum horizontal and vertical histogram, horizontal and vertical centers of signature, aspect ratio and edge points of the signature were used. For experimentation, 21 persons were considered and for each person 15 genuine signatures were taken and 10 skilled forgery samples were taken for each person. The database had 315 genuine signatures and 210 forgery samples. For each person sample features are trained and Euclidean distance is used to validate the signatures. The FRR obtained was 5.4% and FAR was 4.6%. Abhay Bansal [8], used critical points concept for signature verification. The flow of the pattern matching was triangle matching using the k_d ratio, area matching using threshold comparison, and point matching using graph matching algorithm. FAR in case of Random Forgery was found to be 0.08% and in case of Simple and Skilled forgery it was 13.02%. FRR was 2.64%.

**IV. COMPARISON OF VARIOUS APPROACHES**

<table>
<thead>
<tr>
<th>Sr no</th>
<th>Approaches</th>
<th>Features used</th>
<th>FRR</th>
<th>FAR</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Novel Feature Extraction[5]</td>
<td>(a) image cell size (b)image center angle relative to the cell lower right corner (c) and pixels normalized angle relative to the lower right corner.</td>
<td>0.5%</td>
<td>1%</td>
</tr>
<tr>
<td>2.</td>
<td>Graph Matching Technique[6]</td>
<td>Hungarian Method.</td>
<td>15%</td>
<td>10%</td>
</tr>
<tr>
<td>3.</td>
<td>Geometric center features[7]</td>
<td>(a)vertical splitting, (b)horizontal splitting and (c)diagonal splitting</td>
<td>84.1%</td>
<td>17.8%</td>
</tr>
<tr>
<td>4.</td>
<td>Global feature approach[1]</td>
<td>(a)normalized area of the signature, (b)maximum histogram, (c) aspect ratio, (d)centroid feature, (e)number of edge points, (f)trisurface feature and six-fold feature</td>
<td>5.4%</td>
<td>4.6%</td>
</tr>
<tr>
<td>5.</td>
<td>Robust signature verification[2]</td>
<td>(a) maximum horizontal and vertical histogram, (b)horizontal and vertical centers of signature, (c) Aspect ratio and edge points of the signature.</td>
<td>2.64%</td>
<td>(a)Random Forgery - 0.08%</td>
</tr>
</tbody>
</table>

**V. CONCLUSION**

This paper presents a brief survey of various offline approaches used by the researchers and it highlights the need to develop more robust and more constructive offline signature verification approach. The main advantage of using offline systems is liability in the presence of user and freedom from carrying identity cards, or smart cards etc.

**REFERENCES**


**AUTHOR’S PROFILE**

Ms. Madhuri Yadav pursuing M.Tech from CDAC, Noida. She is working on the project “Offline Signature Verification".
Mr. Alok Kumar pursuing M.Tech from CDAC, Noida. He is working on the project “Touching Character Segmentation”.

Mr. Tushar Patnaik (Sr. Lecturer/Sr. Project Engineer) joined CDAC in 1998. He has eleven years of teaching experience. His interest areas are Computer Graphics, Multimedia and Database Management System and Pattern Recognition. At present he is leading the consortium based project “Development of Robust Document Image Understanding System for Documents in Indian Scripts”.

Mr. Bhupendra Kumar (Senior Technical Officer) joined CDAC in 2005, he received his M.Tech. degree from IIIT Allahabad with the specialization in wireless communication and computing. His interest areas are Advanced Image processing, pattern recognition, computer network, wireless network, MANETs. Currently he is involved in project “Development of Robust Document Image Understanding System for Documents in Indian Scripts”.