Dynamic Signature Verification System

Dr. A. R. Karwankar
Department of Electronics
Government College of Engineering, Aurangabad
Aurangabad, India

Dipak S. Chincholkar
Department of Electronics
Government College of Engineering, Aurangabad
Aurangabad, India

***Abstract*— A signature is the most accepted method to declare someone's identity as the authenticated or not, although one's signature may change overtime and it's not nearly as unique or difficult to imitate, such as fingerprints. In this paper, we describe a method for dynamic signature verification system. The signatures are acquired by using pen tablet which captures function based or local features such as x and y co-ordinates as a function of time. Along with this we are considering the parametric or global features for classification of the test signature as genuine or forgery. As this system uses local and global features it will provide a very good performance for dynamic signature verification. Performance of the system will be evaluated by using parameters such as false acceptance rate (FAR), false rejection rate (FRR) and equal error rate (EER).**

Keywords*— *Dynamic signature verification system, Local features, Global features, False acceptance rate, False rejection rate, Equal error rate.

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 [1].

A signature verification system must be able to detect forgeries and at the same time reduce rejection of genuine signatures. Analysis of signatures based on the method used to capture the signatures is divided into two main categories, off-line and on-line. In the off-line verification, the signature patterns were signed on the papers, and then scanned by the plate-form scanners. The on-line signature patterns possess more information than the off-line patterns. There are not only the static geometrical shapes but also the dynamic writing information such as the velocity, the acceleration, the pressure, etc. On-line signature verification methods have proved to be more accurate than off-line methods [2].

Approaches to on-line signature verification are generally classified into two groups: ones based on global or parametric-based approaches and the others often referred to as local or function-based approaches [3]. In parametric approaches, a set of parameters is selected to describe a signature pattern, and the parameters of the reference and test signatures are compared to decide if the signature is genuine. On the contrary, function-based approaches represent a signature pattern as a function of time and compare the characteristics of the signatures locally on a point-to-point or segment-to-segment basis [2].

II. SYSTEM MODELLING

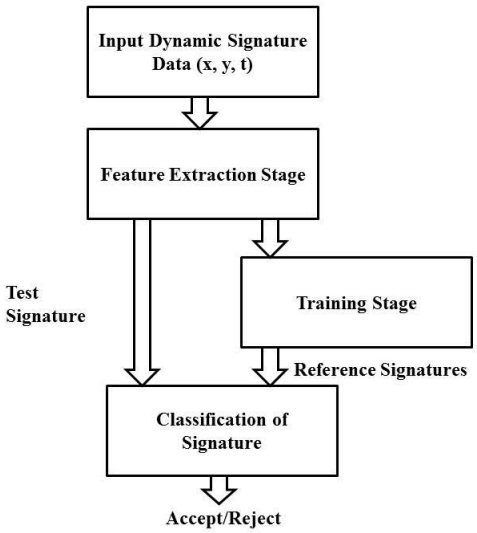

Fig. 1. Proposed System For Dynamic Signature Verification

The proposed dynamic signature verification algorithm flows is shown in Fig.1. It consists of input dynamic data acquisition, feature extraction stage, training stage, and classification method stage. In this paper, signatures preprocessing is not carried out on raw dynamic data in order to preserve the timing characteristics of the user signatures. Actually preprocessing stage is an important stage in automatic signature verification systems particularly when acquired signatures have been corrupted but in many cases unique properties of the user signatures are lost during preprocessing [4].

A. Data Acquisition Device

In this work we are using pen tablet as a capturing device. The tablet is as shown in fig. 2. This pen tablet provides values of x and y co-ordinate points for every sample. The raw signature data available from the tablet consists of two

dimensional series data as represented by (1) where (x(t), y(t)) is the pen position at time t .

Fig. 2. Device for capturing data

$$S(t) = [x(t), y(t)] \quad (1)$$

Example of sample signature acquired by this capturing device is as shown in fig. 3.

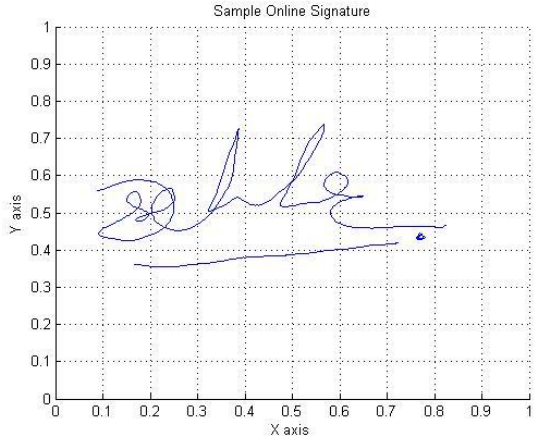

Fig. 3. Sample Dynamic Signature

B. Dynamic Feature Extraction

Feature extraction stage is one of the important stages of an on-line signature verification system. Features can be classified as global or local, where global features represents signature's properties as a whole and local ones correspond to properties specific to a sampling point. The global features examples are signature bounding box, trajectory length or average signing speed, and distance or curvature change between consecutive points on the signature trajectory are local features.

The selection of features for extraction is difficult for the performance of a bio-metric authentication system. The features extracted must have able to describe the signature, separable between classes and also invariant within the same class. Two types of features can be extracted are both dynamic and static feature sets. For both dynamic and static feature sets, they are parameter based features and function based features. In general, function based features give better performance than parameters, but they usually time-consuming matching procedures. Parameter based features are easily computed and matched because of its simplicity.

In this study, we engaged parametric approach along with the function based approach. The raw data at each of the sampling points are used to generate robust feature that captured the variability within signatures of the same class. Δx corresponds to change of x between two successive sampling points, Δy corresponds to change of y between two successive sampling points, and these values are calculated using (2), (3) and with this features we are considering global features such as total signing time and number of strokes for the signature.

$$\Delta x = x(t) - x(t-1) \quad (2)$$

$$\Delta y = y(t) - y(t-1) \quad (3)$$

The mean vectors of Δx and Δy are obtained using (4) and (5) respectively while the variances are obtained using (6) and (7) respectively.

$$\bar{\mu}_{\Delta x} = \frac{1}{N}\sum_{i=1}^{N} \Delta x_i \quad (4)$$

$$\bar{\mu}_{\Delta y} = \frac{1}{N}\sum_{i=1}^{N} \Delta y_i \quad (5)$$

$$\sigma_{\Delta x}{}^2 = \frac{1}{N}\sum_{i=1}^{N} (\Delta x_i - \bar{\mu}_{\Delta x}) \quad (6)$$

$$\sigma_{\Delta y}{}^2 = \frac{1}{N}\sum_{i=1}^{N} (\Delta x_i - \bar{\mu}_{\Delta y}) \quad (7)$$

Each of user signatures is represented by a two dimensional feature vector $F = [f_x \ f_y]$. This feature vector is formed using equation (6) and (7). The feature vector is composed of $F = [\sigma^2{}_{\Delta x}, \sigma^2{}_{\Delta y}]$ and the magnitude of feature vector is obtained using (8).

$$|F| = \sqrt{\overline{fx^2} + \overline{fy^2}} \quad (8)$$

C. Training and Classification

Each of the registered users submitted 5 genuine signatures to the system, out of which 4 signatures are used to generate the signature template so as to set user-specific threshold for accepting or rejecting a test signature. Given 4 reference signature samples S1, S2, S3 and S4, they are represented by their feature as in (9).

$$F1 = [\sigma^2{}_{\Delta x1}, \sigma^2{}_{\Delta y1}]$$
$$F2 = [\sigma^2{}_{\Delta x2}, \sigma^2{}_{\Delta y2}]$$
$$F3 = [\sigma^2{}_{\Delta x3}, \sigma^2{}_{\Delta y3}]$$
$$F4 = [\sigma^2{}_{\Delta x4}, \sigma^2{}_{\Delta y4}] \quad (9)$$

Each of the users signature template is obtained by finding the mean and variance of the feature vector components using (9), (10), (11) and (16), (17), (18) respectively.

$$\bar{\mu}_{fx} = \sum_{i=1}^{K} \sigma^2{}_{\Delta xi} \quad (10)$$

$$\bar{\mu}_{fy} = \sum_{i=1}^{K} \sigma^2{}_{\Delta yi} \quad (11)$$

$$\sigma_{fx}{}^2 = \frac{1}{K}\sum_{i=1}^{K}(\sigma^2{}_{\Delta xi} - \bar{\mu}_{fx}) \quad (12)$$

$$\sigma_{fy}{}^2 = \frac{1}{K}\sum_{i=1}^{K}(\sigma^2{}_{\Delta yi} - \bar{\mu}_{fy}) \quad (13)$$

The mean values of each of the corresponding feature vector components are used to form the template feature vector (T) as represented by (15). The magnitude of the template feature vector is obtained using (16).

$$T = [\overline{\mu_{fx}}, \overline{\mu_{fy}}]$$
$$|T| = \sqrt{\overline{\mu^2{}_{fx}} + \overline{\mu^2{}_{fy}}} \quad (15)$$

The magnitude of the variance within the feature vector components of the five training signatures is calculated using (16). The value of T and V are used to obtain individual threshold (Th) value for each of the registered users as given in (17).

$$|V| = \sqrt{(\sigma_{fx}{}^2)^2 + (\sigma_{fx}{}^2)^2} \quad (16)$$

$$|T| - |V| \geq Th \leq |T| - |V| \quad (17)$$

Whenever a test signature comes into the system, the signature pass through the feature extraction algorithm and the magnitude of feature vector of the test signature is calculated, along with this global features such as number of strokes required and total singing time is calculated and first the classification is done based on this two features and then further classification will be continued and then compare with the magnitude of the template vector. If the value obtained is within the assigned threshold then the test signature is accepted as genuine signature otherwise it is rejected as forged signature.

III. PERFORMANCE EVALUATION OF SIGNATURE VERIFICATION SYSTEM

For evaluating the performance of a signature verification system, there are four important factors: the false rejection rate (FRR) of genuine signatures, the false acceptance rate (FAR) of forgery signatures, equal error rate (EER), receiver operating characteristics (ROC). As these two are inversely related, lowering one often results in increasing the other. The equal error rate (EER) which is the point where FAR equals FRR.

A. False Acceptance Rate

The rate at which a non-authorized person is accepted as authorized is called False Acceptance Rate (FAR). FAR is a non-stationary statistical quantity, which does not only show a personal correlation, it can even be determined for each individual feature. FAR is important, because a higher false acceptance rate can often lead to damages. FAR is calculated as follows:

$$FAR = \frac{Number\ of\ accepted\ forged\ signature\ samples}{Total\ number\ of\ forged\ signature\ samples}$$

B. False Rejection Rate

Rate at which an authorized signature is rejected is called False Rejection Rate (FRR). FRR is a non-stationary statistical quantity, which does not only show a strong personal correlation, it can even be determined for each individual feature. FRR is generally thought of as a comfort criteria, because a false rejection is most of all annoying. FRR is calculated as follows:

$$FRR = \frac{Number\ of\ rejected\ original\ signature\ samples}{Total\ number\ of\ original\ signature\ samples}$$

C. Receiver Operating Characteristic

The "similarities" or, inversely, "distances" are defined differently in different biometric systems, and therefore threshold values often have incomparable meanings. This difficulty is avoided by Receiver Operating Characteristic (ROC), in which the similarity threshold parameter is eliminated and FRR is visualized as a function of FAR. The error graphs of FAR and FRR are respectively defined as the probability that an unauthorized user is accepted as authorized, and that an authorized user is rejected as unauthorized. The curves are dependent upon an adjustable decision threshold for the similarity of a scanned feature to a saved reference value feature in the templates.

D. Equal Error Rate

The FAR/FRR curve pair is well suited to set an optimal threshold for the biometric system. This is partially due to the interpretation of the threshold and similarity measures. The definition of the similarity measures often involves scaling and transformations, which affect the appearance of FAR/FRR curves but not the FAR-FRR values at a certain threshold. A useful method is to represent the FAR/FRR values at Equal Error Rate (EER: FAR = FRR), thus making the system appear less sensitive to threshold changes [6].

IV. CONCLUSION

In this paper, we are trying to implement the dynamic signature verification system using local and global features of the signature. As the classification is done based on the local and global features, the system will provide better, accurate and fast result. So, that it will give better performance parameters as compared over the existing systems.

REFERENCES

[1]A. K Jain, F. D. Griess and S. D Connell, "On-line Signature Verification System*", Pattern Recognition*, vol. 35, No.12, pp. 2963 2972, 2002.

[2] S. Rashidi, A. Fallah and F. Towhidkhah, "Dynamic Signature Verification Based on DCT of Local Features", 18th Iranian Conference on BioMedical Engineering, 14-16 December 2011, Tehran, Iran.

[3] F. Leclerc and R. Plamondon, "Automatic Verification and Writer Identification: The state of the Art 1989-1993", *International Journal of Pattern Recognition and Artificial Intelligence*, vol. 8, pp. 643 – 660, 1994.

[4] Dr.S.A. Daramola and T. S.Ibiyemi, Dynamic Signature Verification System using Statistics Analysis, International Journal on Computer Science and Engineering IJCSE, 2010.

[5]Dr.S.A. Daramola and T. S.Ibiyemi, Efficient on-line Signature Verification System, International Journal of Engineering and Technology IJET-IJENS, 2010.

[6] S. Choudhary and Dr. Arun J. B., "Soft Computing Model For Handwritten Signature Verification", International Journal of Emerging Technology and Advanced Engineering, Vol. 4 Special Issue 1, April 2014.