Proc. of Int. Conf. on Current Trends in Eng., Science and Technology, ICCTEST

Online Handwritten Signature Verification System Based OnBayes' Theorem

Prathiba M K [1] and Dr.Basavaraj L[2]
[1-2]ATMECE/ECE, Department, Mysore, India
prathiba.mk@atme.in
basaraj.l@atme.in

***Abstract*— Very large percentage of daily financial transactions is generally carried out on the basis of verification of signatures. Therefore signature plays an important role both for authentication and authorization of any legal documents. Signature verification is the process used to verify an individual's hand written signature is genuine or forged signature. In the proposed work SVC2004 database is used for validate the system. The accuracy obtained from the implementing system is 92.75%.**

***Index Terms*— Offline, Online, Feature Extraction and Accuracy.**

I. Introduction

Signature verification an even today has an attractive biometric method for person identification and verification. In legal transaction signature plays an important role. So it is required to develop an efficient hand written signature verification system. The objective of signature verification is to differentiate between genuine and forged signature

There are two kinds of signature verification systems depending on the extracted data from the signature. In Off-line (static) schemes shape of the signature is obtained from the scanning process and corresponding features are derived from the scanned picture of the signature.However, inon-line schemes while the user is signing extra information can be captured using digitiser tablets. These digitiser tablets can be interfaced to any personal computer. Online signatures have extra information for extraction such as time, pressure, pen up and down, azimuth, *etc*.

The objective of signature verification is to differentiate between genuine and forged signature irrespective of intra-personal and inter-personal variations in signature. The signatures from the same individuals show considerable changes between different captures known as Intra-personal variations.Skilled forgers can perform signatures with high similarity to the original's signature is known as inter-personal variation. The signatures of the majority person vary with the time and state of mind. So forger can practice the signature over the period of time and can be replicated effectively only the image of the signature. The verification of the signature whether genuine or forged one, through the visual inspection is very difficult to decide.

On–line handwritten signature verification system is more consistent than off line, it uses dynamic characteristic of signature. Because it is very difficult for the forger's to reproduce certain dynamic features of the original signature like total time taken from start to finishing the signature, velocity of the signature and acceleration characteristic of the pen are all unique characteristic of an individual's signature.

Grenze ID: 02.ICCTEST.2017.1.177

II. Previous Work

Mainly on-line signature systems developed either feature based or function based systems. In feature based systems, global information extracted from the signature such as number of pen ups, signature duration, Signature height/width ratio, Average velocity etc. from that features vector is constructed [1]. The function based systems uses local information of the signature time functions like Point wise horizontal and vertical points, point wise pressure, *etc*. for verification [2]. Usually, function-based systems have realized better performance than feature-based systems [1, 3].

In signature verification systems the influence of a skilled forgeries is explained in [4] to tolerate irregularities in genuine signatures while retaining the power to differentiate against forgeries is highlighted in on-line dynamic signature verification systems.

The research groups around the world have been proposed different algorithms in on-line signature verification system. In many publications, based on dynamic programming signatures are classified [6, 7]. Other classifier representations, such as fuzzy logic [9], the statistical model [10] the support vector machine [8], and combinations of them [11, 12], are examined.

III. System Methodology

A generalization of an online signature verification process is defined in Fig 1. Theproposed online handwritten signature verification system consists mainly of three phases acquiring of signature from the data base, feature extraction, and feature matching.

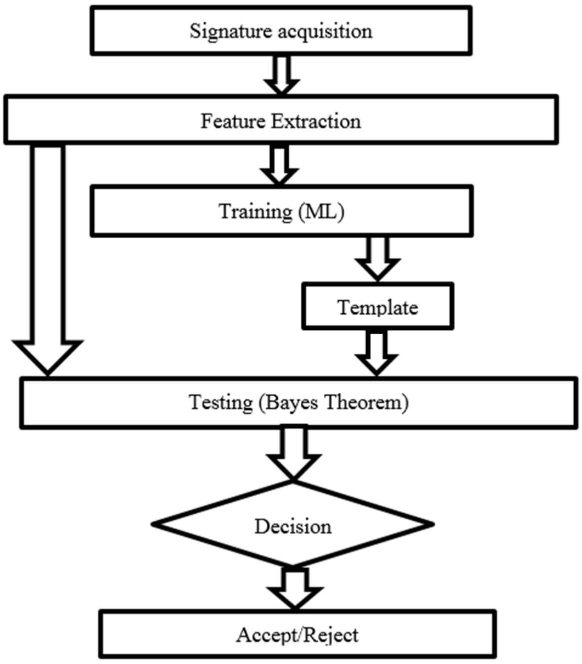

Figure 1. Process of Online Signature Verification

After acquiring the signature, the x and y positions of signature points are extracted and each is represented as 1D time domain signal. In the feature extraction stage other features are derived from pen position data points. The extracted feature vectors are trained using Maximum Likelihood Classification used for Training a model.

During the testing phasewhen a user presents a test signature and claims to be a particular individual for authentication, the feature extracted from the test signature are compared using Bayes' theoremwith that of the template of the signatures of the claimed identity. If the signature has indeed come from the original user, then the comparison process will yield a high similarity score. The user is accepted otherwise it’s rejected as forged signature.

A. Handwritten signature database

SVC2004 data base [13, 14] is used in the experiments. The same signature database used in this research is the one used in First International Signature verification Competition (SVC2004).so that the performance of different signature verification systems can be compared systematically based on common bench mark databases.

Data base consists of a two separate signature verification tasks, Task1 and Task2 which are based on a different signature database. The signature data for the first task contain coordinate information only,i.e. consists of x coordinate , y coordinate time stamp and pen status(pen-up or pen-down). But the signature data for the second task also contain additional information including pen orientation and pressure. The first task is suitable for on-line signature verification on small pen-based input devices such as personal digital assistants (PDA) and the second task on digitizing tablets.

Task2 contains 40sets of signature collected from different people and each contains 20 original genuine signatures from an individual and 20 skilled forgery skilled forgery signatures from from five other contributors

Handwritten signatures were captured electronically after signing using digitizing tablets. For each signature is represented in text file as a collection of set of measurements representing points. The signature is characterized as a sequence of x and y points. These points are used to construct the handwritten signature images, used in this research is showing Fig.2.

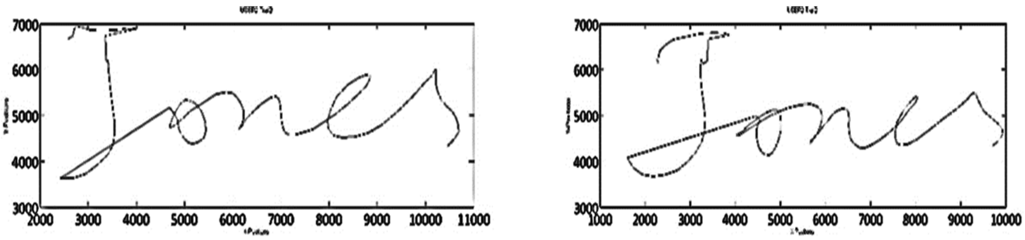

Figure 2. Two genuine signatures of User 1 from SVC20004

The corresponding signature x, y points and pen movement angle during the sign processing is shown in Fig.3.

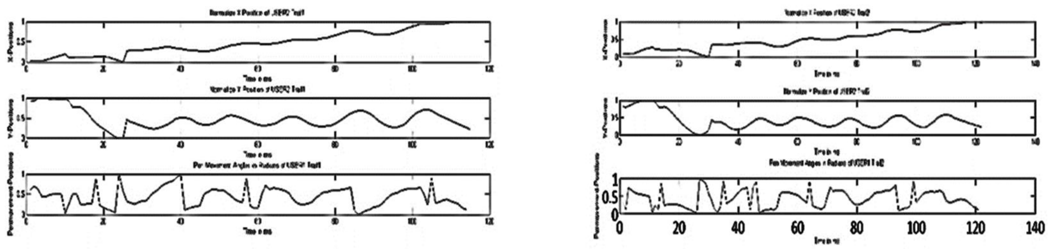

Figure 3. Two genuine signatures x, y and pen movement angle of User

B. Feature Extraction

The Feature extraction phase is one of the crucial phases of an online signature verification system.Using x (n), y (n) several other dynamic features of the signature are derived during the process of signing. The data base provides a sequence of x y coordinates pressure, azimuth angle and altitude angle of the pen as the signature is made on the surface of the tablet. Out of this sequence of x-y coordinates is then processed to obtain other features of the signature for verification.

- The straight line distance between the start and end point of the signature is obtained by calculating the Euclidean distance between the points.
- Total distance travelled by the pen. It is the sum of all the Euclidean distance between all points.
- Total number of pen-ups.
- Total time taken in performing the signature. It is the total time which elapses between the first pen-down and last pen up.

- The average speed of the moving pen tip during the course of performing the signature.
- The number of zero velocity points is effectively indicates the number of halts in the course of performing a signature without the occurrence of actual pen ups.
- Ratio of length to breadth of a signature is calculated by finding the maximum and minimum x and y values.
- The average distance of every point from the first pen down point is calculated. This feature effectively helps to document the original path traced by the pen during a signature process.

C. Training

Out of twenty genuine signatures of 40 user, the first 10 trails of the data base genuine signatures of the Task2 session, are used for development training the system. The signatures are selected for training using Maximum Likelihood Classification used for Training a model. Maximum likelihood classification has usually been used as a baseline for the classification of acquired data base. It is a method of estimating parameters of a statistical model by choosing the parameter value that optimizes the probability of observing the given sample. Given certain regularity conditions i.e. the support of the density function does not depend on the unknown parameter, maximum-likelihood estimators are consistent and efficient.

D. Testing

Bayes' Theorem is a rigorous method for interpreting test signature in the context of previous experience or knowledge by using the training model.In signature verification system when test signature is applied, it will be tested with template obtained from the genuine signatures patterns. It produces a probability (likelihood, score) is used to submit a decision accept or reject of the signature.the schematic representation of the verification of signature using Bayes' theorem is as shown in Fig. 4.

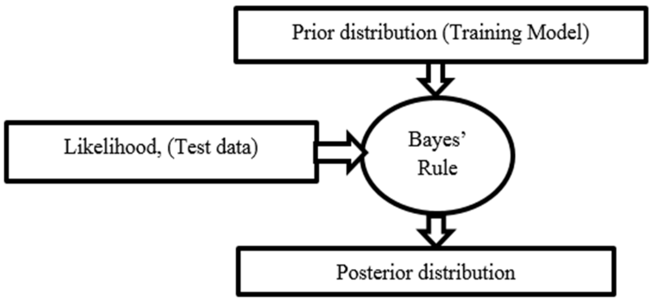

Figure 4. Schematic representation of Bayes' rule.

In the Bayesian paradigm, current knowledge about the model parameters *i.e.*, reference feature vector is expressed by placing a probability distribution on the parameters, called the "prior distribution".
When test signature become available, the information they contain regarding the model parameters is expressed in the "likelihood," which is proportional to the distribution of the observed data given the model parameters,
This information is then combined with the prior to produce an updated probability distribution called the "posterior distribution".
In essence, Bayes' rule is used to combine prior experience (in the form of a prior probability) with observed data (in the form of a likelihood) to interpret these data (in the form of a posterior probability). This process is known as Bayesian inference.
The combination of the ML features along with powerful Bayesian classifiers allow us to achieve significant improvement in verification accuracy as compared to conventional Euclidean distance based methods reported predominantly in previous works. This is because Bayesian classifiers have the flexibility to incorporate prior information, and can predict how a system's performance will change when going from one environment to another or when going from one type of testing to another.

IV. EXPERIMENTAL RESULTS

To validate the implemented system, we compute the Accuracy of the system. Which in turn depends upon the FAR and FRR. Therefore the performance online Signature Verification systems are mainly evaluated by two most important performance metrics. The False Acceptance Rate (FAR) and the False Rejection Rate (FRR). FAR or type II error is the percentage of forged signatures that were falsely verified as genuine. FRR or type I error is the percentage of genuine signatures that were falsely rejected as unauthentic. These two error rates should be as low as possible for a good online signature verification system. The two types of error usually have different effects associated with them depending on the security requirements of the application. The experiments are carried out separately for genuine and skilled forgeries. Both are available in SVC2004 database. Out of twenty signatures the first ten signatures are used for training. This procedure is repeated for skilled forgeries. While the remaining 10 trails of the genuine signatures and 10 trails of the skilled forged signatures of 40 users are used for testing. A writer dependent threshold is selected to obtain the high acceptance rates of genuine signature and significantly lower rates for the forgeries. For each users FAR, FRR and Accuracy is calculated for individual user. It has been observed that overall accuracy of the on line signature verification system is 92.75% is indicated in the table1.

TABLE I : ACCURACY OF THE SYSTEM

User ID	FRR(%) (Genuine)	FAR(%)(Skilled Forgery)	Accuracy (%)
User 1	0	20	90
User 2	0	10	95
User 3	10	20	85
User 4	0	20	90
User 5	10	0	95
User 6	0	10	95
User 7	10	10	90
User 8	0	10	95
User 9	10	10	90
User 10	0	10	95
User 11	10	10	90
User 12	0	10	95
User 13	10	10	90
User 14	0	10	95
User 15	0	20	90
User 16	0	10	95
User 17	0	20	90
User 18	0	10	95
User 19	0	0	90
User 20	0	10	95
User 21	0	10	95
User 22	0	20	90
User 23	0	10	95
User 24	10	10	90
User 25	0	10	95
User 26	10	0	95
User 27	10	0	95
User 28	0	0	95
User 29	10	10	90
User 30	0	10	95
User 31	0	10	95
User 32	0	20	90
User 33	10	0	95
User 34	10	10	90
User 35	10	0	95
User 36	10	10	90
User 37	10	0	95
User 38	0	10	95
User 39	10	10	90
User 40	0	10	95
Average (Accuracy %)			92.75

V. CONCLUSION AND FUTURE WORK

Preliminary implementation of signature verification system is done with only few among many possible features of the signature and the techniques used were also selected to suite the features selected. The marginal improvement of 1.25% when compared to previous works is a very substantial considering the impact of the same in the signature verification field.

Including more number of significant features and excluding few insignificant features result in optimal use of the computational ability of the system. Also the use of advanced techniques for acquiring, training and testing of signatures can improve the results further.

REFERENCES

[1] J. Fierrez-Aguilar, L. Nanni, J. Lopez-Pealba, J. Ortega- Garcia, and D. Maltoni, “An on-line signature verification system based on fusion of local and global information,” in Proc. 5th IAPR Intl. Conf. on Audio- and Video-based Biometric Person Authentication, AVBPASpringer .vol. 3546 of LNCS, pp. 523–532, July 2005.

[2] J. Fierrez, J. Ortega-Garcia, D. Ramos, and J. Gonzalez- Rodriguez, “Hmm-based on-line signature verification: feature extraction and signature modelling,”Pattern Recognition Letters, vol. 28, no. 16, pp. 2325–2334, December 2007.

[3] M. Martinez-Diaz, “Dynamic signature verification for portable devices,” M.S. thesis, Universidad Autonoma de Madrid, November 2008.

[4] FernandezFA, FierrezJ ,Gilperez A, GalballyJ, Ortega-GarciaJ.Spain robustness of signature verification systemstoimitators with increasing skills. In: 10th international conference on document analysis and recognition, 2009.

[5] Lee Luan L, Berger Toby, Aviczer Erez. Reliable on-line human signature verification systems. IEEE Trans Pattern Anal Mach Intell 1996;18(6):643–7. doi:10.1109/34.506415.

[6] Parezeau, M. and Plamendon, R. ‘‘A comparative analysis of regional correlation, dynamic time warping and Skeleton matching for signature verification’’, IEEE Transactions on Pattern Analysis and Machine Intelligence,12(7), pp. 710–717 (1990).

[7] Fang, P., Wu, Z.C., Shen, F., Ge, Y.J. and Fang, B. ‘‘Improved DTW algorithm for online signature verification based on writing forces’’, Advances in Intelligent Computing, 3644, pp. 631–640 (2005).

[8] Kholmatov, A. and Yanikoglu, B. ‘‘Identity authentication using improved on-line signature verification method’’, Pattern Recognition Letters, 26, pp. 2400–2408 (2005).

[9] Ma, M.M., Wijesoma, W.S. and Sung, E. ‘‘An automatic on-line signature verification system based on three models’’, Proceedings of the Canadian Conference on Electrical and Computer Engineering, pp. 890–894 (2000).

[10] Hastie, T., Kishon, E., Clark, M. and Fan, J. ‘‘A model for signature verification’’, Technical Report, AT&T Bell Laboratories (1992).

[11] Letjman, D. and George, S. ‘‘On-line handwritten signature verification using wavelets and back-propagation neural networks’’, Proceedings, International Conference on Document Analysis and Recognition (Seattle), pp.596–598 (2001).

[12] Fuentes, M., Garcia-Salicetti, S. and Dorizzi, B. ‘‘On line signature verification: fusion of a hidden Markov model and a neural network via a support vector machine’’, Proceedings 8th International Workshop Frontiers in Handwriting Recognition, pp. 253–258 .2002.

[13] Muhammad Sarfraz and Syed M. A. J. Rizvi , “An Intelligent System for Online Signature Verification”proceedings of the IEEE,ISBN:978-1-4673-6988-6, 2015.

[14] Abdul Quaiyum Ansari and Jaspreet Kour “Uniform Segmentation in Online Signature Verification” proceedings of the IEEE, ISBN:978-1-4673-6540-6\15, 2015.