RULE BASED SIGNATURE VERIFICATION AND FORGERY DETECTION

M. Hanmandlu Multimedia University Jalan Multimedia 63100, Cyberjaya Selangor, Malaysia E-mail:madasu.hanmandlu@mmu.edu.my	M. Vamsi Krishna Dept. of Electronics & Communication Engg., S.S.N.Engineering College Ongole-523 001, India E-mail:mvkrsna@hotmail.com

Abstract

A rule based signature verification system has been devised based on Adaptive Network Based Fuzzy Inference System (ANFIS). The histogram of the angle differences along the signature trajectory is used as a descriptor of the signatures. We partition the histogram to obtain a number of rules, which is limited to 4 at a time. The performance of the proposed system is found to be satisfactory on the samples of signatures tested.

1. Introduction

Signature verification is very important in realizing tele-banking and tele-networking system where signatures can be used to identify the subscriber. An automated verification process would enable banks and other financial situations to significantly reduce cheque and money order forgeries, which account for a large monetary loss each year. Reliable signature verification can be of great use in many other application areas such as law enforcement, industry security control and so on. Handwritten signatures appear on many types of documents such as bank cheques and credit slip etc. The large volume of such documents makes automatic signature verification desirable. A system for signature verification requires high reliability. A lot of efforts have been focused on the investigation of automatic signature verification methods.

Signature authentication deals with verifying whether a given signature belongs to a person whose signature characteristics are known in advance in the form of extracted features. These features are fed to an adaptive network that is used as a discriminator to classify which signature as genuine or fraud.

A computerized system for signature verification is feasible only if the computer is “sensitive” to variation occurring in the following forgeries.

∗. *Random forgery* characterized by a different semantic meaning and consequently a different overall shape when compared to genuine signature.

∗. *Simple forgeries*, with the same semantic meaning as genuine signature but an overall shape that differ greatly.

∗ *Freehand and simulated forgery* produced with prior knowledge of semantic meaning and the graphical model of the target signature by skilled forger or an occasional forger respectively.

∗. Finally, *tracing forgeries and photocopies*, with almost the same graphical aspect as genuine signatures, but with different pseudo dynamic properties such as dissimilarities in gray level related features like texture, contrast etc.

The system may give two types of errors:

∗ *False rejection*, in which genuine signature is rejected as a forged signature

***** *False acceptance*, in which forged signature is accepted as a genuine signature.

The first step in developing such a system is to search for a computer representation of the signature that can maximize the distance between signature of different individuals.

A lot of research has been done on signature verification. A wide range of feature representations has been applied to signature verification system. Nemeck and Lin [1] have used the Fast Hadmard Transform much like the Fourier transform which preserves the energy and entropy of the original image and also decorrelates the features on a detailed basis. Ammar et al. [2] have proposed the structural description of a signature. In this method, the signature image is demarcated based on vertical and horizontal projections of the image. A number of global and local features have been derived from this segmentation. Sun [3] has suggested rule based structure identification in an adaptive network based fuzzy inference system. This system uses gradient methods for updating nonlinear parameters. Qi and Hunt [5] have used both global and detailed features of a signature image for verification. The global features include geometric characterstics of a signature such as size and slant angle. The detailed features are an approximation of grid level structures of a signature image. In [6] Directional PDF is used as a global feature vector for eliminating random forgeries. Takagi and Sugeno [4] have proposed fuzzy identification of systems and its applications to modeling and control.

The aim of the paper is to model the verification system through fuzzy if-then-rules in the framework of network structure, so that we should be able to classify the signature into genuine or forged categories. The basic learning rule of an adaptive network is based on the gradient descent and chain rules. Here, hybrid learning rule is used which speeds up the learning process substantially.

The organization of the paper is as follows: In Section 2, we discuss extraction of features from the signature using an angle frequency histogram technique. We then go on to discuss the development of the fuzzy model from the rule base in Section 3. Here we also discuss the architecture of the adaptive network as well as the hybrid learning algorithm. Results of the implementation are given in Section 4 and finally the conclusion and future work are discussed in Section 5.

2. Feature Extraction

Information of writing sequence of a signature is normally lost in an off-line environment. Information of writing sequence provides a means to transform a 2-D signature skeleton into a 1-D sequence of pixels, which helps in easy extraction of static as well as dynamic features.

2.1 Signature Tracing

It is not necessary to recover the exact sequence of a signature but may be sufficient to get a set of operators that transform a 2-D spatial representation into a 1-D in a consistent manner. The algorithm that we have used is considerably influenced by the one proposed by Lee and Pan[1]. The heuristic rules have been developed keeping in mind English character users and right handed people. It attempts to trace the signature in a manner a human would do normally. A stroke is a sequence of pixels sequenced according to their tracing order.

2.2 Signature Representation

In order to apply any signature verification technique, it is very important to find an appropriate encryption for signatures, which is independent of translation, rotation and scaling of the signature. In the present system, signatures are represented in the form of the Histogram of the Angle Vs Frequency of occurrence of the angle. First, the tracing sequence of the signature is recovered using the tracing algorithm. The tracing sequence converts the 2-D representation of the

signature skeleton into an unambiguous 1-D representation. The tracing sequence of the signature is recovered using the tracing algorithm [1]. We take segments of equal length along the signature trace to find the angle theta as shown in the figure

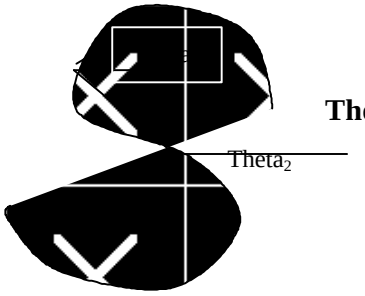

Fig.1

This feature based on the difference of two consecutive angles is invariant to rotation but not to scaling. We normalize the frequency with respect to the total number of angular observations. For interpolation the end of the last stroke and the starting point of the current stroke are joined with a straight line. In this description the total number of pixels having a particular angle is counted and the whole procedure is recorded for the entire signature. The angles are then quantified with a fixed-degree increment (say 10). For scaling invariance it is necessary to take a fixed number of segments in a signature. Thus we get a normalized angle distribution of the signature. The normalized frequency of each angle range can then be fed as input to a neural network.

3. Neuro-Fuzzy Model

The proposed system is a fuzzy inference system implemented in the framework of an adaptive network, which is in fact a superset of all kinds of feedforward neural networks with supervised learning capability. An adaptive network has a structure consisting of nodes and directional links through which the nodes are connected. Moreover, part or all of the nodes are adaptive, which means their outputs depend on the parameters pertaining to these nodes and learning rules specify how these parameters should be changed to minimize a prescribed error measure.

The basic learning rule of an adaptive network is based on the gradient descent and chain rules. Here hybrid learning rule is proposed which speeds up the learning process substantially.

3.1 Fuzzy Inference Systems

Fuzzy inference systems are also known as fuzzy-rule-based systems, fuzzy models consisting of fuzzy associative memories (FAM). Basically a fuzzy inference system is composed of five functions:

- A *rule base* containing a number of fuzzy if-then rules.
- A *database*, which defines the membership functions of the fuzzy sets, used in the fuzzy rules.
- A *decision making unit* which performs the inference operations on the rules.
- A *fuzzification interface* which transforms the crisp inputs into degrees of match with linguistic values.
- The *defuzzification interface* which transforms the fuzzy results of the inference into a crisp output.

Usually, the rule base and database are jointly referred to as the knowledge base.

The steps of fuzzy reasoning performed by fuzzy inference systems are:

1) Compare the input variables with membership function on the premise part to obtain the membership values of each linguistic label.
2) Combine the membership values on the premise part to obtain the overall membership.
3) To get firing strength of each rule.
4) Generate the qualified consequent of each rule depending on the Firing strength.

3.2 Architecture of the Network

An adaptive neural network is a multilayer feedforward network in which each node performs a particular function (node function) on incoming signals as well as on a set of parameters pertaining to this node. The formulas for the node functions may vary from node to node and choice of each node function depends on the overall input-output function which the adaptive network is required to carry out. Links in the adaptive network only indicate the direction of flow of signals between nodes; no weights are associated with the links.

3.3 Hybrid Learning Rule [7]

For simplicity we assume that the adaptive network under consideration has only one output written in functional form as :

Output = F(I , S)

where I is the set of input variables and S is the set of parameters .If there exists a function H such that the composite function H @ F is linear in some of the elements of S and then these elements can be identified by the least square method . More formally, if the parameters set S can be decomposed into 2 sets

$S = S1 \oplus S2$

where $\oplus$ represents direct sum and H @ F is a linear in the elements of S2 then upon applying H to the above equation

H(Output) = H@F(I, S)

which is linear in the elements of S2 . S2 parameters can be estimated by LSE like Kalman filter while S1 parameters have been estimated by the gradient descent method. We have used if-then rules of Takagi and Sugeno's type [4]. i.e.

If x is A1 and y is B1 then $f1=p1x + q1y +r1$

Here the consequent parameters are (p1,q1,r1...). H(.) and F(.) are the identity function and the function of the fuzzy inference system, respectively. The final output *f* is the weighted sum of individual rule outputs. *F* is linear in consequent parameters.

3.4 Steps involved in Signature verification

Various steps involved in the Signature verification are:

1) Input
2) Forward pass
3) Backward pass
4) Development of rules
5) Output

Input: Input is the histogram of angle Vs frequency. This is angle distribution of different strokes in a signature. Here we have considered 10 samples of the signature. We have considered 6 angular intervals.

Input Vector: (X_1, 1 X1,2 X_1,3 …….. X_1,6)

Forward Pass: This involves

(a) To find the derivatives of all nodes.

(b) Identification of consequent parameters by the least square method

Error measurement

Error = Standard Output - actual output

Backward Pass: This involves

(a) Error propagation

(b) Identification of parameters by using the gradient descent method.

Development of rules:

Rules are of the type as shown below:

If x1 is p1 and x2 is p2 and..... then f = q1*x1 + q2*x2+ ...+r1.

Here,

Number of rules = (membership-function) $^{\text{number of inputs}}$

Number of inputs means length of input vector.

For our application, the number of membership functions for each input is taken to be 2. The type of membership functions is Gaussian.

Fig. 2: Sample signature

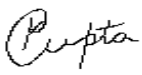

Fig. 3: Thinned Signature

4. Results of Implementation

The sample signature and thinned version are shown in Figs.2-3. The characterization of the signature is done using angle histogram. A typical angle histogram is shown in Fig. 4.

The ANFIS used here contains 64 rules with 2 membership functions being assigned to each input variable. The total number of modifiable parameters is 484. The initial step size is taken to be 0.5 while the step increase and decrease rates are both taken to be 0.1. 10 sets of training data are used. The training data are used for training of ANFIS, while the testing data are used for verifying the identified

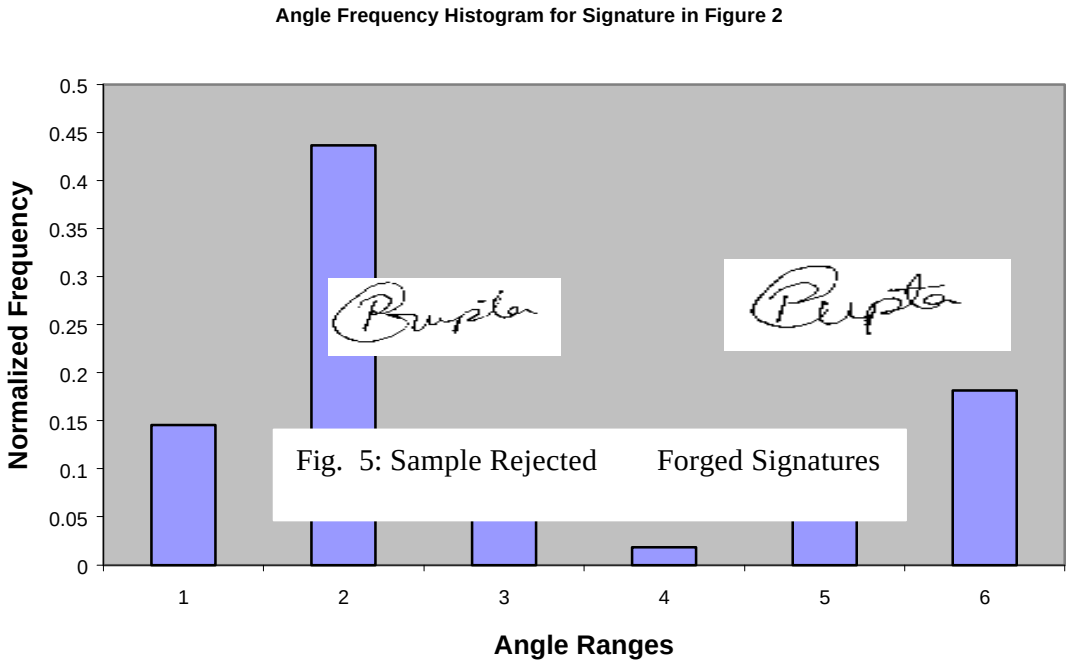

Fig. 5: Sample Rejected Forged Signatures

ANFIS only. The minimal training error $RMSE_{trn}$ = 0.000005 has been obtained after 200 epochs. The errors converged usually within 200 epochs. The rejection threshold for a signature has been kept at 0.0001. We have tested the system for 20 test samples of a signature out of which 6 are forged. Only 1 out of the forged signatures has been falsely accepted while 3 falsely rejected giving a false rejection rate of 21% and false acceptance rate of 18%.

5. Conclusions

This paper characterizes the signatures by the angle distribution, which is obtained by tracing the signature. Using this distribution, the parameters of the Takagi-Sugeno fuzzy model are obtained by the hybrid learning using the neural network in which the forward pass learns the linear parameters by LSE and the backward pass learns the nonlinear parameters by the gradient descent method. The performance of this is tested on the forged samples of a signature and the results are quite encouraging.

References

[1] Jack C. Pan and Sukhan Lee, " Offline Tracing and Representation of Signatures," Proceedings of Conference on Pattern Recognition, pp.679-680, 1991.

[2] Rafael C. Gonzalez and Richard E. Woods**,** Digital Image Processing, Addison Wesley Publishers.

[3] C.-T. Sun, "Rule base structure identification in an adaptive network based fuzzy inference systems," IEEE Trans. Fuzzy Syst., accepted for publication, 1993.

[4] T. Takagi and M. Sugeno, "Fuzzy identification of systems and its applications to modeling and control" , IEEE Trans. Syst., Man, Cybernetics, vol. 15, pp. 116-132, 1985.

[5] Yingyong Qi and Bobby R. Hunt, "Signature Verification using Global and Grid Features," Pattern Recognition, Vol 27, No. 12, pp. 1621-1629, 1994.

[6] R. Sabourin and R. J. Plamondon, "Preprocessing of Hand written Signatures from Image Gradient Analysis," Proceedings of IEEE Conference on Pattern Recognition and Artificial Intelligence, pp. 576-578, 1986.

[7] Jyh-Shing Roger Jang, "ANFIS: Adaptive-Network-Based Fuzzy Inference System," IEEE Trans. on Syst., Man and Cybernetics, vol. 23, no. 3, May/June 1993.