AUTOMATIC SIGNATURE VERIFICATION WITH CHAIN CODE USING WEIGHTED DISTANCE AND EUCLIDEAN DISTANCE - A REVIEW

Abhilash Deshmukh[1], Shashank Desai[2], Tejas Chaure[3], Akshay Chothe[4], Sunil B Wankhade[5]

[1]*Student, Computer Engineering, RGIT, Maharashtra, India*
[2]*Student, Computer Engineering, RGIT, Maharashtra, India*
[3]*Student, Computer Engineering, RGIT, Maharashtra, India*
[4]*Student, Computer Engineering, RGIT, Maharashtra, India*
[5]*Professor, Computer Engineering, RGIT, Maharashtra, India*

Abstract

The signature forgery can be restricted by either online or offline signature verification techniques. It verifies the signature by performing a match with the pre-processed signature dynamically by detecting the motion of stylus during signature while on other hand, offline verifies by performing a match using the two dimensional scanned image of the signature. This paper studies about the various techniques available in offline signature verification along with their shadows.

Keywords: *Signature Verification, Weighted Distance, High Pressure Factor, Normalization, Threshold Value.*

----------***----------

1. INTRODUCTION

To identify a person in real time instances, it is necessary for him to be authenticated by the system. Signature verification is one of the many methods that can be used for authentication of a person. Signature verification uses references of many signatures taken and it compares the current signature in real time instance. There is an increasing need of using signature verification techniques in different organizations especially financial institutions. With the increasing number of transactions, there is a desire of automatic signature verification to take place for authentication of the individual persons. Signature verification is primarily used for two tasks. The first task is to identify the signature owner; the second task is to take the decision, whether the signature is genuine or forged. Signature verification can be classified in two categories: One is online and other is offline signature verification.

Online signature verification scans the signature of the user by tracing the different motion on the stroke of the signature and identifies it against pre-processed signature information. Offline signature verification gives static signature verification information. In this method signature is scanned from the document and is verified against 2D scanned image of the signature. In this paper, we have studied various method such as Support vector machines (SVM), Dynamic time warping (DTW), Neural network (NN), Multi-set features (MSF), Associative Memory Net (AMN), Automatic signature verification with four-dimensional chain code using weighted distance and Euclidian distance (ASV) to discuss the variations offered in offline signature verification methods.

2. APPROACHES FOR SIGNATURE VERIFICATION

V. Vapnik [1] introduced a new learning method SVM. It uses set of examples from two classes to find the hyper plane. It refers to hyper plane which has the largest distance to the nearest training set data point and thus it results in good separation of classes. The success achieved in hand written digit recognition made SVM very popular. SVM is based on the structural risk minimization principle (SRM). SRM is based on two main principles: The first one is to control the risk on the training set and the second principle controls the capacity of decision function which used to obtain this risk value. SVM has two classes: Linear separable and Classification problem. Linear separable is used to find the hyper plane with maximum Euclidean distance from the training set. There will be just one optimal hyper plane with the maximal margin d, defined as the sum of distances from the hyper plane to the closest points of the classes. This linear classifier threshold is the optimal separating hyper plane. Then SVM can find an optimal linear separating hyper plane with the maximal margin in this higher dimensional feature space. For a two-class problem, the nonlinear decision function derived from the SVM classifier can be formulated as the kernel function. The kernel is not positive definite but offer some theoretical and empirical explanations.

DTW algorithm is used for the measurement of speed and time of two sequences [2]. DTW algorithm can be applied to video, audio, and graphics, and many different applications such as automatic speech recognition. This algorithm can also be utilized to establish linear and non-linear dimensions of the sequences. The basic principle of this method is

permitting a range of 'steps' in the space of (time frames in sample as well as in template) and to find the maximum length path between the aligned time frames, subject to the constraints implicit in the allowable steps. We determine the best matching template and sample to find the total similarity cost. Taking into consideration two signatures aligned between L and L*′*, which known as warping path, denoted as T, and it has two warping function: mean that the point in L corresponds to the element in L‟. Online context can be used to match cost between L and L‟. The path which minimizes the above cost function is the optional warping path. Dynamic programming is used to solve the optimization problem of DTW efficiently.

Neural Network is used for authentication and verification of hand written signature [3].Pattern recognition is the main area in which NN is used. The signature verification process parallels this learning mechanism. Neural network uses two kind of different processes: training and learning. The first process is training with the help of extraction method a feature set representing the signature with several samples from different signers. The second process is learning the relationship between a signature and its class. After the second process is completed then the network can be classified to a particular signer. Hence NNs are highly suited to modeling global aspects of handwritten signatures. Alan McCabe et al [4]. He proposed a method for verifying handwritten signatures by using NN architecture. To train NN different types of static and dynamic signature features are extracted. Static features are height, slant etc while dynamic features are velocity, pen tip pressure etc. Now all these and other Network topologies are tested and comparison is made to get accuracy. The resulting system has an overall error rate of 3.3% that was being reported for the best case. Rasha Abbas in his earlier research [5] investigated the suitability of using back propagation neural networks for the purpose of offline signature verification however later on multi-layered feed forward neural network was investigated.

Off-line signatures are signatures which usually use in paper works like letters, contracts, and bank checks. This method is related to offline signatures specially. According to Edson J. R. Justino and F.Bortolozzi[6], ASV is processed with the one feature set but to increase the usability of designed ASV in the sense of increasing security best feature set of signatures is used in this technical method. This method is popularly known as new novel MSF based ASV technique. At first, features are examined in two ways these are shape features like handwriting slants and pseudo dynamic features. Distance measure and verification threshold are also calculated. By taking these values for comparison, at the second stage, probability of forgery is decided if DM<VTH. In this condition, signature is processed with the n X n matrix. By fitted signature in the matrices are n X n matrix, three resulted matrices are calculated which are backbone of MSF technique, SR (System Reliability), PCR (Per cent Correct Rejection), PCA (Per cent Correct Acceptance). As the system reliability PCR, PCA has high values, and then signature ids totally matched to best features set that particular sign. There are mainly two steps in MSF technique:

560 genuine signatures are used in MSF technique and forgery signatures are obtained from different 26 writers. The number of genuine signatures and forgeries differ from one person to another. Signatures were extracted from various documents like business documents, bank checks so that the signature data is naturally written under widely different conditions. Reason behind such an extraction of signatures is that forgeries were created with a good attention in order to have convincing forgeries, and some forgeries are real ones obtained from actual caseworks.
The second step is to extract signature using different technologies as:

a) Feature extraction: This stage of the signature verification and feature selection includes pre-processing. Features in off-line systems have two types mainly. These are Shape features like handwriting slants which can be positive, vertical, negative, and horizontal etc. and relative measures of signature height and width, middle zone width and signature width .Pseudo dynamic feature is nothing but High Pressure Factor. These both type of features are extracted in two ways such as globally on the signature as a whole and locally on the signature divided into specific parts.
b) Distance measure: Distance Measure (DM) is used to calculate similarity between input signature and reference by using the Euclidean distance.
c) Threshold value: The value of the threshold VTH is calculated by feature selection technique that selects the best feature set which minimizes the error rate as well as maximizes the correct decisions.
d) Verification decision: The verification decision to determine whether signature is reliable is proceed with the help of calculated distance measure and threshold value. There are two cases for determination of genuine signature.

Effectiveness of the individual features, and their contribution to the effectiveness of the different feature sets, if augmented by, to form a new one.
SR (System Reliability = (PCA+PCR)/2).

PCA (Percentage of Correct Acceptance that is percentage of genuine signatures accepted as genuine) and PCR (Percentage of Correct Rejection that is percentage of forgeries rejected and classified as attempted forgeries).

MSF helps to improve the forgery detection. In other words, the MSF technique is a process of collecting the sparse effectiveness that can be provided by the EFS but cannot be captured by the best feature set.

The Associative Memory Net (AMN) detects the forged signature quickly [7]. To handle the cost function detail parametric studies and parallel processing using Open MP is must. These algorithms are used to verify actual signature and tested with a reference of 10 nearly similar signatures.

The AMN technique finds forgery with accuracy 94.3%, which can be compare with other methods.

There are various methods for ASV implementation but there is only one or two signature references used by considering memory storage as well as current image based verification speed. There will be 20 signature references. Each reference signatures is converted to a small number of pre-computed features resulting in verification speeds in excess of 60 verifications per second. These features of specific signer signature are stored in the database. There are features like edge distribution, pixel, slant, pixel density, aspect ratio of signature are stored in dataset. Even if fraudster stole this featured information then also he cannot predict the how is the signature actually. So, important data is being safe and loss can be avoided.

The proposed system matches tested signature with reference signature. Test signature features are considered as x and n is the reference signature feature stored in database, where n<=20. System first extract features of the tested signature and that features match with the extracted features of reference signatures. Various Algorithms like extracted features are used for calculating matching function , four-dimensional chain code and normalization are used for computing features of signature. As per the value of matching function, signature is real or fake is decided by system.

A step-wise method has been followed in this work.

1. Take signature as an input from document which has to be verified.
2. All the pre-computed features of reference is stored in database.
3. Extract the features of current input signature like Pixel Distribution, Chain Code, Pixel Density, or Aspect Ratio by processing through various stages.
4. Apply Gaussian Filter Formula on the resulted image in step 3.
5. Calculate pixel density cost and Aspect Ratio cost for signature has to be verified by using reference.
6. Calculate Average Match Function for number of references by using formula.
7. If value is 0 then signature is fake and if 100 then it's accurately matched.
8. By normalizing Match function by using formulae of average and standard deviation, it becomes a Match Function.
9. If value of Match Function is in between 0 to 1 then signature is totally matched.

The table compares all the different techniques studied above. Two major criteria that had been used for comparison are False Acceptance Rate (FAR) and False Rejection Rate (FAR). Each technique has varying FAR and FRR. The objective is to choose best technique with acceptable error rates. Although FAR % for Associative Memory Net is least but its FRR % is on higher side. Hence we select ASV as preferred method as it has low FAR and FRR.

Table -1: Comparison of FAR and FRR

Sr.no	Method	FAR(%)	FRR(%)
1	Support Vector Machine		
	Linear	21.06	18.53
	Poly	15.41	15.64
	RBF	15.41	13.12
2	Dynamic Time Wrapping	34.91	28.93
3	Neural Network	13.26	11.89
4	Multi Set Feature For Offline Signature Verification	16.36	14.58
5	Associative Memory Net	9.7	17.9
6	Feature Based Automated Signature Verification using chain code with Euclidean's distance	12.6	10.2

3. CONCLUSIONS

The signature is becoming most important for authentication and so it becomes necessary to enhance its application with automated systems to avoid forgeries and ultimately the fraud. In this paper we have studied various methods of Signature Verification on the basis of various factors related to it like, no. of references, edge distribution, pixel, slant, pixel density, aspect ratio of signature security, memory management, accuracy including FAR and FRR, which plays important role in verification of signature.

REFERENCES

[1]. E.Ozgunduz, T.Senturk and M.E Karsligil, "Off-Line Signature Verification and Recognition by Support Vector Machine", *Proceedings of Europian Signal Processing, 2005.*

[2]. M.S Arya and V. S Inamdar, "A Preliminary Study on Various Off-line Hand Written Signature Verification Approaches", *Proceeding of International Journal of Computer Applications, vol. 1, no.9, 2010*

[3]. S.A. Daram T. S. Ibiyemi ola, "Offline Signature Recognition using Hidden Markov Model", *proceeding of International Journal of Computer Applications, vol. 10, no.2, 2010.*

[4]. K. Huang and Y. Hong, Off-line signature verification based on geometric feature extraction and neural network classification, Patten Recognition, *Vol. 30, No. 1, pp. 9-17, 1997.*

[5]. C. Sansone and M. Vento, Signature verification: increasing performance by a multi-stage system, Pattern Analysis and Applications, *Vol. 3, pp. 169-181, 2000*.

[6]. Anu Rathi, Amrita Ticku, Niti Gupta, Accuracy enhancement in offline signature verification with the use of associative memory, *IJCSNS International Journal of computer science and network security*, vol14, no.3,March 2014.

[7]. Priya Metri , Ashwinder Kaur, "Handwritten Signature Verification using Instance Based Learning", International Journal of Computer Trends and Technology- March to April Issue 2011.