Automatic Static Signature Verification Systems: A Review

Vitthal K. Bhosale[1] Dr. Anil R. Karwankar[2]

[1]PG Student, Government College of Engineering, Aurangabad (M.S.),

[2]Assistant Professor, Dept. Of Electronics & Tele-Communication, Government College of Engineering, Aurangabad (M.S.), India

1

Abstract:

Handwritten signature is a distinguishing biometric feature which is the most widely employed form of secure personal authentication. Signature verification is used in a large number of fields starting from online banking, passport verification systems to even authenticating candidates in public examinations from their signatures. Even today thousands of financial and business transactions are being authorized via signatures. Therefore an automatic signature verification system is needed. This paper represents a brief review on various approaches used in Static signature verification systems.

Keywords: Biometrics, false acceptance rate, false rejection rate, forgeries, static signature, simple distance classifiers, support vector machines.

1. Introduction

Signature verification is a major area of research in the field of image processing and pattern recognition. It is widely used in the fields of finance, access control and security. Signature verification is the process which is carried out to determine whether a given signature is genuine or forged. Signature verification is different from character recognition thus consider signature as a complete image with some particular curves that represent a particular writing style of the person. Approaches to signature verification fall into two categories according to the acquisition of the data: On-line and Off-line. On-line signature verification focuses on capturing and analyzing the signature in real time, as the person is signing it. Off-line signature verification deals with analyzing images of a person's signature. In On-line signature verifications system stylus is used to obtain pen pressure, velocity, acceleration and location, as functions of time. In Off-line method an optical scanner is used to obtain handwriting data which deals with a 2-D image of the signature represented by a discrete 2D function i.e. S(x, y) Where x = 0, 1, 2… M and y = 0, 1, 2… N. (M, N) denote the spatial coordinates. The value of S in any (x, y) corresponds to the grey level at that point. This paper is organized as follows: Section 2 discusses various signature verification concepts, Section 3 introduces various steps in signature verification, Section 4 introduces different methods of signature verification, Section 5 introduces performance evaluation of different methods and Section 6 concludes the paper and shows scope of future work.

2. Signature Verification Concepts

Signature verification system involves some basic concepts that are forgeries, signature features and performance evaluation parameters i.e. error rates.

2.1. Types of Forgeries

There are mainly three types of forgeries:

- Random Forgery
- Simple Forgery
- Skilled Forgery

The random forgery is written by the person who doesn't know the shape of the original signature. Simple forgery is represented by the person who knows the shape of the original signature without much practice. While skilled forgery is produced by an individual who has appropriate knowledge about the original signature along with proper practice.

2.2. Types of Features

Features extracted for Static signature verification can be broadly divided into three main types:

- Global features
- Local features
- Geometric features

Global features which are extracted from the whole signature image. Global features can be easily extracted but depend upon the overall position alignment thus highly susceptible to distortion and style variations. Global features include – signature area, signature height to width ratio, centre of gravity etc. Local features are extracted from the small portion of signature image. These features are computationally expensive but are much more accurate than global features. Local features include – local pixel density, slant features, critical points etc. The geometric features represent the characteristic geometry of a

signature that keeps both their global as well as local feature properties. Geometrical features have the ability to tolerate with distortion, style variations, rotation variations and certain degree of translation.

2.3. Error Rate

- False Acceptance Rate
- False Rejection Rate

While dealing with any signature verification system, we consider False Rejection Rate and False Acceptance Rate as its performance evaluation parameters. The Efficiency of signature verification systems can be represented by these two types of error rates i.e. the percentage of genuine signatures rejected as forgery which is called False Rejection Rate (FRR) and the percentage of forgery signatures accepted as genuine which is called False Acceptance Rate (FAR). Generally signature verification system shall have an acceptable trade-off between a low FAR and a low FRR.

3. Processing Steps in Static Signature Verification

A signature verification (SV) system authenticates the identity of any person, based on an analysis of his/her signature through a set of processing steps. The major steps are as follows:

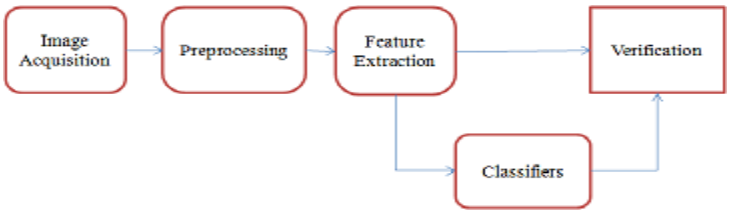

Figure 1. General overview of Static signature verification system

3.1. Image acquisition

The signatures to be processed by the system should be in the digital image format. The data for the offline signature verification system acquire from various ways like by optical pad, scanner etc. The signature samples are scanned and then scanned images are stored digitally for further processing.

3.2. Preprocessing

The purpose of Signature pre-processing step is to make signatures standard and ready for feature extraction. Preprocessing is a necessary step to improve the accuracy of Feature extraction and Verification. Before processing the image for feature extracting some pre-processing algorithm are applied on the scanned image like Binarization, Denoising, Skeltonization, Thinning, Calculating exact signature area etc.

3.3. Feature Extraction

The efficiency of a signature verification system mainly depends on Feature extraction stage. Feature extraction techniques should be fast and easy to compute so that system has low computational power. Selected features should discriminate between genuine and forgery signature. Features extracted for static signature verification can be divided as Global, Local and Geometric features.

3.4. Verification

Verification step compares test signature features with genuine signature features based on various pattern classification techniques and makes a final decision for verification as genuine or forged signature.

4. Methods for Static Signature Verification

Here we discuss some of the convenient existing signature verification systems. We categorise these systems according to the pattern recognition technique used. We discuss Template matching techniques, Simple Distance Classifiers (SDCs), Neural Networks (NNs), Structural techniques, Support Vector Machines (SVMs), Hidden Markov Models (HMMs) and Hybrid systems i.e. systems that use more than one pattern recognition technique.

4.1. Template Matching Techniques

Template matching is one of the earliest and simplest approaches to pattern recognition. A pattern class is represented by a template. Such a template pattern can either be a curve or an image. Dynamic Time Wrapping is the most popular template matching technique for Static signature verification. The Dynamic Time Warping (DTW) algorithm which is based on dynamic programming finds an optimal match between two sequences of feature vectors. The total dissimilarity between reference and test node is represented by D (M, N).

$$D(m, n) = d(m, n) + \min [D(m-1, n), D(m-1, n-1), D(m, n-1)] \quad [1]$$

$$DTWdist = D(M, N)$$

The training of system using DTW is performed by equation (2) where G1 is the training score [6].

$$G1 = \frac{2}{d(d-1)} \sum_{i=1}^{d-1} \sum_{j=i+1}^{d} DTWdist(Gi, Gj) \quad : \text{where } i,j \leq d \qquad [2]$$

The verification of the system using DTW is performed by equation (3) where G2 is verification score [6].

$$G1 = \frac{1}{d} \sum_{i=1}^{d} DTWdist(Gt, Gi) \qquad : \text{where } i \leq d \qquad [3]$$

The decision to accept or reject signature is based on the value of the threshold score given by equation [4]

$$Score = G1/\ G2 \qquad [4]$$

A. Piyush Shanker and A. N. Rajagopalan [1] proposed a signature verification system based on Modified Dynamic Time Warping (DTW). Authors made modifications to the basic DTW algorithm for stability of various components of a signature. This involves assigning weights to various components of a signature depending on their stability. These weights are then used to modify the cost function involved with the warping paths. Authors reported that the system based on the modified DTW algorithm performed significantly better than the basic DTW system. The method is computationally efficient and runs in real-time. Authors reported that with a threshold value of 1.5, the system has close to 0% acceptance rate for casual forgeries, 20% acceptance rate for skilled forgeries, and about 25% rejection rate for genuine signatures. Jayadevan R., Satish R. Kolhe and Pradeep M. Patil [7] developed static handwritten signature verification based on Dynamic Time Warping (DTW). The horizontal and vertical projection features of a signature are extracted using discrete Radon transform and the two vectors are combined to form a combined projection feature vector. The feature vectors of two signatures are matched using DTW algorithm. The closed area formed by the matching path around the diagonal of the DTW-grid is computed and is multiplied with the difference cost between the feature vectors. The test signature is compared with each genuine sample and a matching score is calculated. A decision to accept or reject is made on the average of such scores. Authors used a global signature database (GPDS-Signature Database) of 2106 signatures with 936 genuine signatures and 1170 skilled forgeries to evaluate the performance of system. Authors reported FAR of 26.06% and FRR of 17.94%.

4.2. Simple Distance Classifiers

A Simple Distance Classifiers represent each pattern class with a Gaussian probability distribution function, where each PDF is uniquely defined by the mean vector and covariance matrix of the feature vectors that belong to the particular class. Serestina Viriri and Bradley Schafer [13] presented an offline signature verification system based on global features and transition features. In this paper a database of 2106 signatures was used. To train the system, a subset of this database was taken comprising of 15 genuine samples taken from each of the 30 different individual's signatures. The features for all 15 signatures would then be averaged to form one centroid feature vector. When a claimed signature is entered into the system, it is compared against the centroid feature vectors for classification of genuine signature and forged signature. During the testing phase, two approaches were tested. During testing, a claimed signature is compared against template file using the Euclidean distance and if it is below a certain threshold value, then the signature is declared valid, otherwise it is a forgery. Using the global threshold, correct classification rate of 73% and a false acceptance rate of 18.5% were obtained. Using the calculation of the localized threshold, a correct classification rate of 84.1% and a false acceptance rate of 17.8% was obtained.

4.3. Neural Networks

An NN is a parallel computing system that consists of a large number of simple processors with many interconnections. Neural Network has the ability to learn complex non-linear input-output relationships, use sequential training procedures and adapt itself to the data. A Neural Network model uses organisational principles in a network of weighted directed graphs, in which the nodes are artificial neurons and the directed edges are connections between neuron outputs and neuron inputs. H. Baltzakisa, N. Papamarkos [15] developed a signature verification technique based on a two-stage neural network classifier. The proposed system was based on global, grid and texture features. For each one of these feature sets a special two stage Perceptron OCON (one-class-one-network) classification structure was implemented. In the first stage, the classifier combines the decision results of the neural networks and the Euclidean distance obtained using the three feature sets. The results of the first-stage classifier feed a second- stage radial base function (RBF) neural network structure, which makes the final decision. The performance of the system was checked by the use of the remaining subset (TS) of 500 signatures. A FAR of 9.81%, FRR of 3% and an overall efficiency of 90.09% was achieved. R.Abbas [4] developed the off-line signature recognition based on a back propagation neural network prototype. Authors used feed forward neural networks and three different training algorithms Vanila, Enhanced and batch were used. Author reported FAR between the ranges of 10.0 % for casual forgeries and FRR of 6.0%.

4.4. Hidden Markov models

Hidden Markov Models represent a signature as a sequence of states. According to the associated probability distribution, in each state an observation vector is generated. Transitions between the states are represented as a set of

transition probabilities. These probabilities of an HMM are trained using observation vector extracted from sample signature database. Justino, Bortolozzi and Sabourin [8] proposed an off-line signature verification system using Hidden Markov Models to detect random, casual, and skilled forgeries. Three features: a pixel density feature, a pixel distribution feature and an axial slant feature are extracted from a grid segmentation scheme. A False Acceptance rate of 2.83% is obtained and a False Rejection rate of 1.44%, 2.50%, and 22.67% are obtained for random, casual, and skilled forgeries, respectively.

4.5. Structural Techniques

In Structural pattern recognition techniques a pattern is viewed as being composed of simple sub-patterns which are built from further simpler sub-patterns. Abhay Bansal, Bharat Gupta, Gaurav Khandelwal, and Shampa Chakraverty [2] developed an Offline Signature Verification System based on Critical Region Matching. The system was designed to detect the skilled forgeries and was mainly dealt with the extraction of the critical regions and matched them following a modular graph matching approach. The method includes critical points extraction, critical region extraction, and formulation of signature verification problem as a graph matching problem. For semi-skilled forgeries accuracy of 95.69% and for skilled forgeries an accuracy of 89.09% was obtained. Majhi, Reddy and Prasanna [5] proposed a morphological parameter for signature recognition, authors proposed centre of mass of signature segments, and the signature was split again and again at its centre of mass to obtain a series of points in horizontal as well as vertical mode. The point sequence is then used as discriminating feature; the thresholds were selected separately for each person. They achieved FRR 14.58% and FAR 2.08%. Ismail et al. [10] proposed an off-line Arabic signature recognition and verification technique. Authors proposed a system of two separate phases for signature recognition and verification is developed. In the first phase some features based on Translation, circularity feature, image enhancement, partial histogram, centres of gravity, global baseline, thinning etc. are extracted. In the second phase some more features are also extracted such as Central line features, Corner line features Central circle features, Corner curve features and Critical point features. A set of signature data consisting of 220 genuine samples and 110 forged samples is used for experimentation. They obtained a 95.0% recognition rate and 98.0% verification.

4.6. Support Vector Machines

V.Vapnik et al. introduced this new learning method. SVMs are machine learning algorithms for binary classification based on recent advances in statistical learning theory. S. Audet, P. Bansal, and S. Baskaran [3], designed Off-Line Signature Verification and Recognition using Support Vector Machine. They used global, directional and grid features of signatures. Virtual Support Vector Machine (VSVM) was used to verify and classify the signatures and FAR of 16.0% and FRR of 13.0% was obtained. Ozgunduz et al. [12] proposed off-line signature verification system using Support vector machines. Author used Support Vector Machines in order to detect random and skilled forgeries. Author used extracted global geometric features, direction features and grid features for SVM classifier. In the experiments, a comparison between SVM and ANN is performed. Using a SVM with RBF kernel, an FRR of 0.02% and an FAR of 0.11% are obtained.

5. Performance Evaluation with Results

The performance of system is determined based on the accuracy of classification between the genuine and forged signature. Evaluation parameters for any signature verification system are FAR and FRR. The performances of different methods with results are shown in Table 1.

Table 1. Performance evaluation of different methods

Serial No.	Method	FAR (%)	FRR (%)
1.	Modified Dynamic Time Wrapping [1]	20.0	25.0
2.	Hidden Markov Model [8]	02.83	22.67
3.	Two Stage Neural Network classifier [15]	09.81	03.00
4	Back-propagation Neural Network Prototype [4]	10.00	06.00
5.	Morphological Parameter based [5]	02.08	14.58
6.	Wavelet-based verification [9]	10.98	05.60
7.	Support Vector Machine [11]	04.83	05.30
8.	Virtual Support Vector Machine [3]	16.00	13.00
9.	Dynamic features based [16]	13.78	14.25

6. Conclusion

This review article presents a brief overview of the recent works on Static signature verification. Different existing approaches used for signature verification are discussed and compared along with their FAR and FRR. The results shows that the accuracy of existing available signature verification systems is not enough to implement in public use thus more research on Static Signature verification is required. There are still many challenges in this domain which includes the signatures from the same person are similar but not identical. In addition, a person's signature often changes during their life due to age, illness and up to some extent the emotional state of the person. Thus there is a need of research in feature extraction and classification techniques based on dynamic methods that extract dynamic information from static images. That would make it possible for researchers to achieve a better performance in this domain.

References

[1] A. Piyush Shanker and A. N. Rajagopalan, Off-line signature verification using DTW, Pattern Recognition Letters, v.28 n.12, 2007 1407-1414.

[2] Abhay Bansal, Bharat Gupta, Gaurav Khandelwal, and Shampa Chakraverty "Offline Signature Verification Using Critical Region Matching", International Journal of Signal Processing, Image Processing and Pattern, 2009.

[3] S. Audet, P. Bansal, and S. Baskaran ,"Off-line signature verification using virtual support vector machines", ECSE 526 – Artificial Intelligence, April 7, 2006

[4] R.Abbas, "Back propagation Neural Network Prototype for off line signature verification", thesis Submitted to RMIT, 2003

[5] B. Majhi, Y. Reddy, D. Babu, "Novel Features for Off-line Signature Verification", International Journal of Computers, Communications & Control Vol.I (2006), No. 1, pp. 17-24.

[6] Hifzan Ahmed, Shailja Shukla, "Global Features based Static Signature Verification system Using DTW", International Journal of Systems , Algorithms & Applications, vol 2, Issue 4, pp. 13-17, April 2012.

[7] Jayadevan R., Satish R. Kolhe, Pradeep M. Patil, "Dynamic Time Warping Based Static Hand Printed Signature Verification", Journal of Pattern Recognition Research 1 (2009) 52-65.

[8] J.Edson, R.Justino, F.Bortolozzi and R. Sabourin, "Off-line signature verification using HMM for Random, Simple and Skilled Forgeries", 2001.

[9] P. Deng, H. Yuan Mark Liao & H. Tyan, "Wavelet Based Off-line Signature Recognition System", Proceedings 5th Conference on Optical Character Recognition and Document Analysis, 1996, Beijing, China.

[10] M.A. Ismail, Samia Gad, "Off-line Arabic Signature Recognition and Verification", 2000.

[11] H. Lv, W. Wang, C. Wang, and Q. Zhou, ―Off-line Chinese signature verification based on support vector machines, PRL 2005, vol. 26, no. 15, pp. 2390–2399

[12] Emre Ozgunduz, Tulin Senturk and M. Elif Karslıgil "Offline Signature verification and Recognition by Support Vector Machine", EUSIPCO, 2005.

[13] B.Schafer and S.Viriri - An Off-Line Signature Verification System□, 2009, (ICSIPA- 2009), pp.95-100.

[14] S. Armand, M. Blumenstein - Off-line Signature Verification based on the Modified Direction Feature□ ICPR-2006, pp.509-512

[15] H. Baltzakis, N. Papamarkos, "A new signature verification technique based on a two-stage neural network classifier", Engineering Applications of Artificial Intelligence ,2001

[16] L. Basavaraj and R. D Sudhaker Samuel, "Offline-line Signature Verification and Recognition: An Approach Based on Four Speed Stroke Angle", International Journal of Recent Trends in Engineering, Vol 2, No. 3, November 2009