Signature Verification System Based on Support Vector Machine Classifier

[1]Sonal Borase, [2]Dr.Javed Rasheed Shaikh
[1]Ph.D Scholar, [2]Assistant Professor
[1]JJT University, Jhunjhunu, Rajasthan, India,
[2]SKN Singhgad Institute of Technology & Science, Lonavala, India

***Abstract* - The paper presents associate degree off-line signature verification system exploitation support vector machine technique. world options ar extracted from the signatures exploitation argonon rework. for every registered user within the system info variety of reference signatures ar listed and aligned for statistics info extraction concerning his signature. Dynamic time warp rule is employed to align 2 signatures. throughout support vector machine classifier coaching, variety of real and solid signatures ar chosen. A check signature's verification is established by initial positioning it with every reference signature for the claimed user. The signature is then classified as real or forgery, in keeping with the alignment scores that ar normalized by reference statistics, exploitation commonplace pattern classification techniques. employing a info of 2250 signatures (genuine signatures and good forgeries) from seventy five writers within the planned signature verification system a performance of roughly eighty two is achieved.**

***keywords* - signature verification; support vector machine; radon transform; dynamic time warping**

1. INTRODUCTION

Handwritten signature is amongst the first few biometrics to be used even before the advent of computers. Of all biometric technologies, whether biological or non-biological, signature verification offers most potential in terms of adaptability and implementation. This holds true from a number of perspectives i.e. ease of use, low implementation cost and the ease of embedding the system in an organization, without excessively disrupting or affecting existing operations [23]. Signature verification has many applications including use in financial transactions, providing electronic signatures for documents, and in providing additional security measures for computer system authentication. Signature verification also has the advantage that is culturally more accepted and less intrusive than other biometric techniques, such as fingerprinting and iris scanning [6].

Signature verification procedures can be carried out in offline and online modes. For offline signature verification, the images of signatures found on bank checks and documents are used for verification and are useful in automatic verification of signatures. On the other hand for signatures that are captured by tablets online signature verification is used. Offline signature systems are more applicable and easy to use in comparison with online systems in many parts of the world however it is considered more difficult than online verification due to the lack of dynamic information.

In signature verification systems, firstly during enrollment users provide a number of signature samples (reference signatures). Then, when a user presents a new signature as test signature claiming to be a particular individual, it is compared with the reference signatures for that individual. If the dissimilarity value is below a certain threshold value the user is authenticated, otherwise denied. Since obtaining actual forgeries is difficult, two forgery types have been defined in signature verification papers: A skilled forgery is signed by a person who has had access to a genuine signature for practice. A random or zero-effort forgery is signed without having any During verification method, the take a look at signature is compared to all or any the reference set signatures, leading to a variety of unsimilarity values.

Then one must choose a method to combine these dissimilarity values in a single number so as to represent the dissimilarity of the test signature to the reference set, and compares it to a threshold to make a decision. The single dissimilarity value can be obtained from the minimum, maximum or the average of all the distance values. Typically, a verification system chooses one of these approaches and discards the other ones. For instance, Jain et al. report the lowest error rates with the minimum distance criterion, among the other three [4]. Instead of choosing one distance as most suitable, in this system, the minimum and maximum dissimilarity values are used in deciding whether the signature is genuine or forgery. These distance values, are used as the features of a signature in its classification as genuine or forgery, after they are normalized by the corresponding values of the reference set, as explained in the following sections.

In this paper an off-line signature verification system using support vector machine (SVM) is proposed. The SVM, a learning method introduced by Vapnik et al. [23],[21], tries to find an optimal hyperplane for separating two classes.

Therefore, the misclassification error of knowledge each within the coaching set and take a look at set is decreased .

Basically, SVM have been defined for separating linearly two classes. When data are none linearly separable, a kernel function is used as polynomial function, radial basis function (RBF) or multi layer perceptron. The classification based on SVM involves training and testing stages. The training stage consists to find the optimal parameters.

Hence 2 parameters ought to be determined: the kernel parameter and also the regularization parameter.

These two parameters are found experimentally depending on the dataset. The testing stage allows evaluating the robustness of the classifier.

In order to make your mind up if a signature is real or forgery, a choice rule is performed on the outputs of the SVMs wherever values ar positive or negative.

Hence, the output of the SVMs should be transformed to the objective evidences expressed the membership degree.
In follow, no commonplace type is outlined for the membership degree.
The only constraint is that it must be limited in the range of 0,1 whereas SVM produce a single output [24].
There are many approaches that are used for offline signature verification, for example, template matching techniques, neural networks, minimum distance classifiers, elastic image matching and others. Many approaches have been developed in the pattern recognition area, which approached the off-line signature verification problem.
Numerous methods and approaches are summarized in a number of survey articles [16],[18],[10],[11],[17],[12]. The state of the art in automatic signature verification is presented by Impedovo [7], who addresses the most valuable results obtained so far and highlights the most profitable directions of research to date.
It includes a comprehensive listing of quite three hundred elect references as associate degree aid for researchers operating within the field.
SVMs have been used successfully in both offline and online signature verification [7].
Paper presented by Yadav, Kumar, and Patnaik, discuss a brief survey of various offline approaches used by the researchers. In the paper declared that main phases of the signature verification follow the sequence: preprocessing, feature extraction, data training, and signature verification. Feature extraction phase can be based on following types of features: global features, local features, and transition feature. In the verification techniques different methods are used like: graph matching technique, geometric center, critical points approach [14].
A brief overview of the recent works on static signature verification is presented by Bhosale and Karwankar. Different existing approaches used for signature verification are discussed and compared in the review. They discussed template matching techniques, simple distance classifiers, neural networks, structural techniques, support vector machines, hidden Markov models. The results show that 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 [25].
Substantial analysis has been undertaken within the field of signature verification involving English signatures.
In order to convey the state-of-the-art in the field to researchers, a survey of non-English and non-Latin signature verification systems is presented by Pal, and Blumenstein. Different existing approaches are discussed and compared. They observed that among the literature of non-English signature verification research, the maximum work has been performed for Chinese language systems. For Japanese, Arabic and Persian only a few pieces of work have been done. Despite the many works in this area, from this survey, they conclude that there are still many challenges in this research area [20].
In the reviewed papers it is agreed that the accuracy rates obtained so far from the available systems is not sufficiently high.
Thus there's a desire of analysis in feature extraction and classification techniques supported dynamic ways that extract dynamic information from static images [14], [25], [20].
S. Audet, P. Bansal, and S. Baskaran [19], designed offline signature verification and recognition using support vector machine. They used international, 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. [8] proposed offline signature verification system using support vector machines.
Author used support vector machines so as to observe random and sure-handed forgeries.
Author used extracted international geometric options, 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 [8].
Another very interesting method proposed by Ferrer et al.[3] calculates geometric features of a signature in fixed- point arithmetic for offline verification. The proposed features are then checked with different classifiers, such as Hidden Markov Models, Support Vector Machines, and the Euclidean distance verifier. The results show that it is better to follow the SVM research line in order to detect different forgeries.
Nguyen et al [24] presents a new method in which structural features are extracted from the signature's contour using the (MDF) and its extended version: the enhanced MDF (EMDF) and
further 2 neural network-based techniques and support vector machines (SVMs) ar investigated and compared for the method of signature verification.
The classifiers were trained victimisation real specimens and different haphazardly chosen signatures taken from a publically offered information of 3840 real signatures from one hundred sixty volunteers and 4800 targeted solid signatures.
A distinguishing error rate (DER) of 17.78% was obtained with the SVM whilst keeping the false acceptance rate for random forgeries (FARR) below 0.16%.
Earlier work on offline signature verification deals primarily with casual and random forgeries, but nowadays, needs to more elaborated classifiers techniques are increased, because signature databases became larger and researchers moved toward more difficult skilled forgery detection tasks.
The rest of the paper is organized as follows: Section II presents the proposed method for feature extraction, signature alignment and enrolling in the system. Section III shows the experimental methodology, experiments and results. The paper ends with summary and conclusion in section IV.

2. PROPOSED METHOD

The introduced system is divided into three major parts: (i) signatures enrollment (model creation) (ii) signatures training
(iii) verification of given signature.
The diagram of the system is given in Fig. 1.
During the enrollment section, a collection of reference signatures ar accustomed verify user dependent parameters

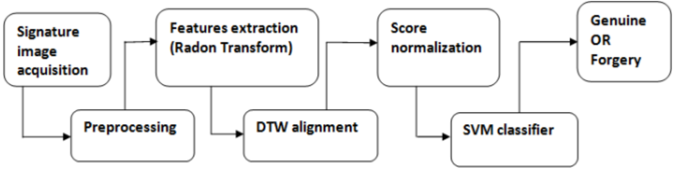
characterizing the variance among the reference signatures.

The reference set of signatures, along with these parameters, ar keep with a singular user symbol within the system's info.

In the training phase we choose a number of genuine and forged signatures for training the SVM classifier. In the verification phase when a test signature is input to the system, it is compared to each of the reference signatures of the claimed person. The person is authenticated if the resulting dissimilarity measure is below or equals a threshold value of the classifier, otherwise denied. The details of the system are described in the following sections.

decimated vectors are then shrunk or expanded to the required dimension (d) through linear interpolation. Each vector is subsequently normalized by the variance of the intensity of the entire set of feature vectors. In order to ensure rotation invariance, the projections at angles that range from 180_o to 360_o are also included in the observation sequence [1], [2].

An observation sequence therefore consists of T = 2Nθ feature vectors, that is



X^T □ $\{x , x ,..., x \}$

(2)

1 1 2 T

Fig. 1. Signature verification system

2.1 SIGNATURE'S FEATURE EXTRACTION

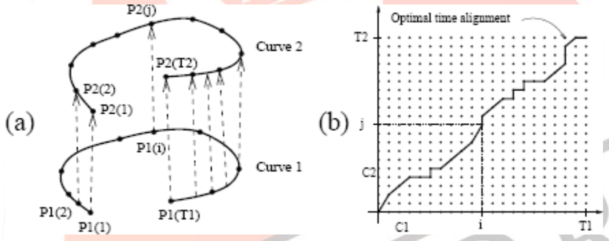
The separate atomic number 86 rework (DRT) may be a matrix, wherever every column represents a projection or shadow of the first image at a definite angle.

DRT can be expressed as follows [15], [22]:.

2.2 SIGNATURE ALIGNMENT

In order to compare two signatures of differing lengths, we use the dynamic time warping (DTW) algorithm [9]. DTW algorithm finds the best linear alignment of two vectors such that the overall distance between them is minimized *(see Fig. 3).*

R_j



R_j= the cumulative intensity of the pixels that lie within the j_{th} beam.
Ψ= total pixels in an image.
w_{ij}= the contribution of the i_{th} pixel to the j_{th} beam-sum. I_i= the intensity of the ith pixel.
N_φ= non-overlapping beams per angle N_θ= number of total angles.
For extracting the global features, firstly the background of the signature image is mapped to zero and the pen strokes to one. After that, median filtering is applied to remove speckle noise. Subsequently the DRT of the signature image is calculated. Fig.2 shows a signature and its DRT. This algorithm calculates the DRT at N_θ angles. These angles are equally distributed between 0_o and 180_o[1],[2].

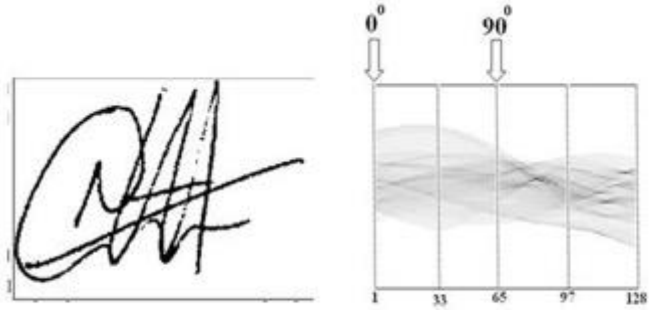


Fig. 2. A signature and its DRT. The DRT is displayed as a gray-scale image. This image has Nθ=128 columns, where each column represents a projection

Although the DRT is not a shift invariant representation of a signature image, shift invariance is ensured by the subsequent image processing. This is done by removing (decimation) all the zero-valued components from each projection. These
Fig. 3. Two curves with the correspondence between points indicated. (b) Warping plane and warping path.

In order to ensure that each observation sequence is a rotation invariant representation of the corresponding signature image, observation sequence alignment is necessary. The optimal alignment of two observation sequences can be achieved in a linear way. Iteratively shifts the observation sequences with respect to each other. During any iteration the distances between the corresponding observations (feature vectors) are calculated. The alignment is optimal when the average distance between the corresponding observations is a minimum. The distance between two signatures is simply the average of the distances between the optimally aligned feature vectors.

2.3 ENROLLMENT

During enrollment to the system, we use a number of signatures (five in our system) for each user. These signatures are pair wise aligned to find the distance between each pair, using the DTW algorithm.
From these alignment scores, the subsequent reference set statistics area unit calculated:

i. Average distance to farthest signature, (dmax)
ii. Average distance to nearest signature , (dmin)

2.4 TRAINING

A training data set consisting of two five- signatures, ones is genuine signatures and the other is forgery, are used in order to obtain the threshold value separating the forgery and genuine classes. These signatures are separate from the signatures used as reference signatures.
First, each training signature is compared to the reference set of signatures it claimed to belong, using the DTW algorithm described previously, giving a 2-dimensional feature vector (pmin, pmax). The feature values are then normalized by the corresponding averages of the reference set (dmin, dmax) this is calculated as in equations (3) and (4) to give the distribution of the feature set.
In order to classify a test signature as genuine or forgery, we first proceed as in the training stage: the signature is compared to all the reference signatures belonging to the claimed ID using the DTW algorithm. Then, the resulting distance values (pmin, pmax), normalized by the corresponding averages of the claimed reference set (dmin, dmax), after that these normalized values are used in classifying the signature as genuine or forgery, by the trained classifier (see Fig. 5)

$$N_{max}=d_{max}/p_{max} \ldots (3) \quad N_{min}= d_{min}/p_{min} \ldots (4)$$

The distribution of this normalized knowledge supports that real and forgery samples within the coaching set square measure well separated with these normalized options.

Note that by normalizing the measured distance vectors by the corresponding reference set averages, we eliminate the need for user-dependent thresholds commonly used in deciding whether a signature is similar enough to the reference set [2].

Finally, we train the SVM classifier using the 2- dimensional feature vectors to separate the genuine and forgery samples in this normalized feature space as shown in Fig. 4.

Then, a linear classification is formed by choosing a threshold price separating the 2 categories among the coaching set.

The threshold is fixed and later used in the verification process. The results are summarized in the following section 3.

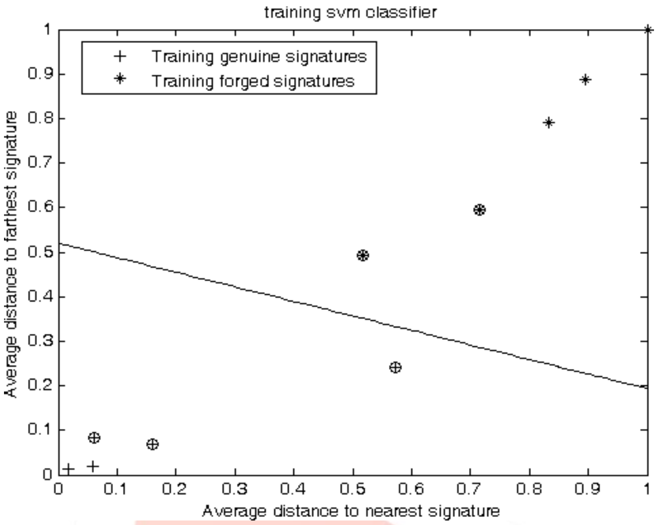


Fig. 4. Training of SVM classifier with respect to the 2- dimensional normalized distance vector.

2.5 CLASSIFICATION

A classification data set, consisting of five genuine signatures and five forgery signatures, is used in order to test the trained classifier. These signatures are separate from the signatures used in the enrollment and in the training phases.

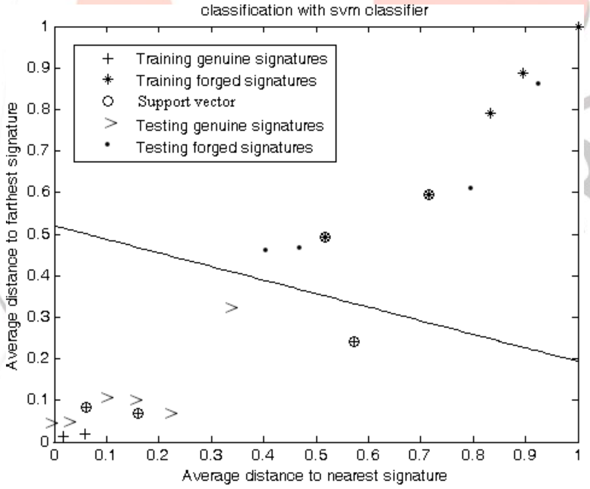


Fig. 5. Verification results obtained by SVM classifier using the 2- dimensional normalized data

3. EXPERIMENTS AND RESULTS

Experiments are carried out on a dataset; which called “MCYT-100 signature CORPUS” [13]; that contain static signature images. The dataset contains 2250 signatures from 75 writers.

Each author has fifteen real signature and fifteen adept forgeries.

For each individual enrollment 5 genuine signatures are used as a reference set and the rest of the signatures are used for training and testing. Note that training data is separate from both the reference set of genuine signatures and the test data used in experiments.

Based on the experiments previously discussed we can obtain a performance of approximately (82%) when using SVM as a classifier

4. SUMMARY AND CONCLUSION

An offline signature verification system is presented in this paper, which approaches the problem as a two-class pattern recognition problem using SVM classifier.

DRT for global feature extraction from the signatures is used and it shows us that it is a stable and robust method. The DRT creates simulated time evolution from one feature vector to the next and enables us to create a model for a signature with DTW. We experimented with SVM classifier and obtained 82% overall performance for a data set of 75 people and 2250 signatures (genuine signatures and skilled forgeries). The obtained results are quite good, given the fact that the forgeries used on the experiments were skilled forgeries.

REFERENCES

[1] Zhirkov, "Off line signature verification mistreatment element rework and svm/knn classifiers", TSTU Trans. Vol. 15. № 1. pp. 62-69, 2009. Вестник ТГТУ. Том 15. № 1.Ferrer Miguel, Jesu´s B. Alonso, and Carlos M.

[2] Travieso, " Offline Geometric Parameters for Automatic Signature Verification mistreatment Fixed-Point Arithmetic", IEEE Transactions On Pattern Analysis And Machine Intelligence, vol.

[3] 27, No. 6, June 2005. Jain, F. Griess, S. Connell, "On-line signature verification," Pattern Recognition vol. 35 PP. 2963–2972, 2002.

[4] Nassim and Youcef Chibani, "SVM-DSmT Combination for Off- Line Signature Verification", International Conference on Computer, Information and Telecommunication Systems (CITS) , Amman, Jordan,

[5] Pippin, "Dynamic signature verification mistreatment native and international features", Georgia Institute of Technology, July 2004.

[6] D. Impedovo and G. Pirlo, "Automatic signature verification: the state of the art". IEEE Transactions on Systems, Man, and Cybernetics, Part C: Applications and Reviews, vol. 38, 5, pp. 609–635, september 2008.

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

[8] E. Munich Mario, Pietro Perona. Continuous Dynamic Time warp for translation-invariant curve alignment with applications to signature verification. Published in Proc. of the seventh International Conference on laptop Vision (ICCV'99). Korfu. Greece. September 1999.

[9] F. Leclerc and R. Plamondon, "Automatic signature verification: the state of the art, 1989–1993," International Journal of Pattern Recognition and Artificial Intelligence, vol. 8, no. 3, pp. 643–660, 1994.

[10] J. Gupta and A.McCabe, "A review of dynamic written signature verification," Tech. Rep., James Cook University, Australia, 1997.

[11] J. K. Guo, D. Doermann, and A. Rosenfeld, "Forgery detection by native correspondence," International Journal of Pattern Recognition and AI, vol. 15, no. 4, pp. 579–641, 2001.

[12] J. Ortega-Garcia, J. Fierrez-Aguilar, D. Simon, J. Gonzalez, M. Faundez-Zanuy, V. Espinosa, A. Satue, I. Hernaez, J.-J. Igarza, C. Vivaracho, D. Escudero and Q.-I.

[13] Moro, "MCYT baseline corpus: a bimodal biometric database", IEE Proc.-Vis. Image Signal Process., Vol. 150, No. 6, December 2003.

[14] [M. Yadav, A. Kumar, T. Patnaik, B. Kumar , "A Survey on Offline Signature Verification" , International Journal of Engineering and Innovative Technology (IJEIT) Volume 2, Issue 7, January 2013

[15] R. N. Bracewell, Two-Dimensional Imaging, Prentice-Hall, Englewood Cliffs, NJ, USA, 1995.

[16] R. Plamondon and G.Lorette, "Automatic signature verification and author identification—the state of the art," Pattern Recognition, vol. 22, no. 2, pp. 107–131, 1989.

[17] R. Plamondon and S. N. Srihari, "On-line and off-line handwriting recognition: a comprehensive survey," IEEE Trans. On Pattern Analysis and Machine Intelligence, vol. 22, no. 1, pp.63–84, 2000.

[18] R. Sabourin, R. Plamondon, and G. Lorette, "Off-line identification with handwritten signature images: survey and perspectives," in Structured Document Image Analysis, H. Baird, H. Bunke, and K. Yamamoto, Eds., pp. 219–234, Springer-Verlag, NY, USA, 1992.

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

[20] S. Pal, M. Blumenstein, U. Pal, "Non-English and Non-Latin Signature Verification Systems: A Survey", Proceedings of the 1st International Workshop on Automated Forensic Handwriting Analysis (AFHA) 2011

[21] T. Mitchell, Machine Learning, McGraw-Hill, 1997. Peter, The noble gas remodel - Theory and Implementation, Ph.D. thesis, Technical University of Denmark, June 1996.

[22] Vapnik, the character Of applied mathematics Learning Theory, Springer, 1995.

[23] V. Nguyen; Blumenstein, M.; Muthukkumarasamy V.; Leedham G., "Off-line Signature Verification Using Enhanced Modified Direction Features in Conjunction with Neural Classifiers and Support Vector Machines", in Proc. 9th Int Conf on document analysis and recognition, vol 02, pp. 734-738, Sep 2007.

[24] V. K. Bhosale, A. R. Karwankar, "Automatic Static Signature Verification Systems: A Review", International Journal Of procedure Engineering analysis (ijceronline.com) Vol.3 Issue. 2, February 2013, 8-12