

An Offline Signature Verification using Adaptive Resonance Theory 1(ART1)

Charu Jain
Department of CSE

Priti Singh, Ph.D
Department of ECE
Amity University, Gurgaon, Haryana.

Aarti Chugh
Department of CSE

ABSTRACT

Automatic signature verification is a well-established and an active area of research with numerous applications such as bank check verification, ATM access, etc. This paper proposes a novel approach to the problem of automatic off-line signature verification and forgery detection. We have designed offline signature verification and recognition system (SVRS) using Adaptive Resonance Theory-1(ART 1). In this paper a standard database of 250 signatures is used for calculating the performance of SVRS. The training of our system is done using ART-1 that uses global features as input vector and the verification and recognition phase uses a two step process. In first step, the input vector is matched with stored reference vector which was used as training set & in second step cluster formation takes place. If our given pattern matches with the stored pattern, it is accepted otherwise new cluster is formed. The presented approach achieved a classification ratio of 97.9%. The false acceptance rate (FAR) and false rejection rate (FRR) for given sample signatures is 2.7% and 3.9%.

Keywords

Offline signature verification, Global features, Neural Network, Adaptive Resonance Theory-1

1. INTRODUCTION

A signature [1-4] is a simple, concrete expression of the unique variations in human hand geometry. The way a person signs his or her name is known to be characteristic of that individual. A signature verification system must be able to detect forgeries and at the same time reduce the rejection of genuine signatures. The four legal properties of a handwritten signature are: - authentication, acceptance, integrity, non-repudiation [27].

Signature verification [6] is split into two classes according to the available data in the input. *Offline (static)* signature [5], [7] verification takes the image of a signature as input and is useful in automatic verification of signatures that may be found on bank cheques and documents. *Online (dynamic)* [5], [7] signature verification uses signatures that are captured by pressure sensitive tablets that extract dynamic properties of a signature. Signatures in offline systems usually may have noise, due to scanning hardware or paper background and contain less discriminative information since only the image of the signature is the input to the system. While genuine signatures of the same person may slightly vary, the differences between a forgery and a genuine signature may be imperceptible, which make automatic offline signature verification a very challenging pattern recognition problem.

Daksina Ranjan Kisku et.al [8] has proposed a technique Support Vector Machines (SVM) to fuse multiple classifiers for an offline signature system. H. Baltzakis et.al [9] has presented a technique for off-line SVRS using two stage perceptron OCON (one-class-one-network), the result of first

stage was fed to Radial Basis Function (RBF). Emre Özgündüz et.al [10] has implemented SVM for off-line signature verification and recognition system using the global, directional and grid features of signatures & compared with back propagation method. Meenakshi K. Kalera et.al [11] has described a novel approach for signature verification and identification in an offline environment based on quasi-technique using GSC (Gradient, Structural and Concavity) features for feature extraction. Ali Karouni et.al [12] has developed new method using artificial neural network. Sharifah Mumtazah Syed Ahmad et.al [13] presented an automatic off-line signature verification system using Hidden Markov Modeling (HMM). Vu Nguyen et.al [14] used the total energy that a writer uses to create his/her signature as a global feature and combined these features with the Modified Direction Feature (MDF) and SVM were employed to construct the signature models. Abhay Bansal et.al [15] proposed a contour matching algorithm. Miguel A. Ferrer et.al [16] used HMM, SVM and Euclidean distance classifier (EDC). Inan Guler et.al [17] presented an automatic handwritten signature verification (AHSV) using dynamic time wrapping and global features have been extracted. Madasu Hanmandlu et.al [18] has developed offline signature verification and forgery detection approach based on fuzzy Takagi-Sugeno (TS) model. Hai Rong Lv et.al [19] used HMM approach and they had built the matching relations between planar regions to get the deformable grids, and then extract grid features from them. Stephane Armand et.al [20] has proposed a Resilient Back Propagation neural network method for signature verification and compared with Radial Basis Function neural network (RBFNN). D. Bertolini et.al [21] has proposed a method for off-line signature verification through ensemble of classifiers and had tried to simulate the shape of the signature by using Bezier curves. This technique achieved a minimum FAR of 6.48% and for random and simple forgeries it was 3%. J. F. Vargas et.al [22] has proposed an offline signature verification system based on grey level information using texture features. Bailing Zhang et.al [23] proposed a offline signature verification and identification by pyramid histogram of oriented gradients (PHOGs), which represents local shape of an image by a histogram of edge orientations computed for each image sub-region, quantized into a number of bins. This method showed superb classification accuracies of 99% and 96 % for GPDS and DAVAB datasets, respectively. Most of the researchers used the artificial intelligence models for signature data preprocessing and verification.

2. METHODOLOGY

This section describes the methodology behind the system development. The block diagram of Off-line Signature Verification Based on Global Features using Artificial Neural Network (ANN) is discussed in detail and is as shown in the Figure 1. The process starts with data acquisition.

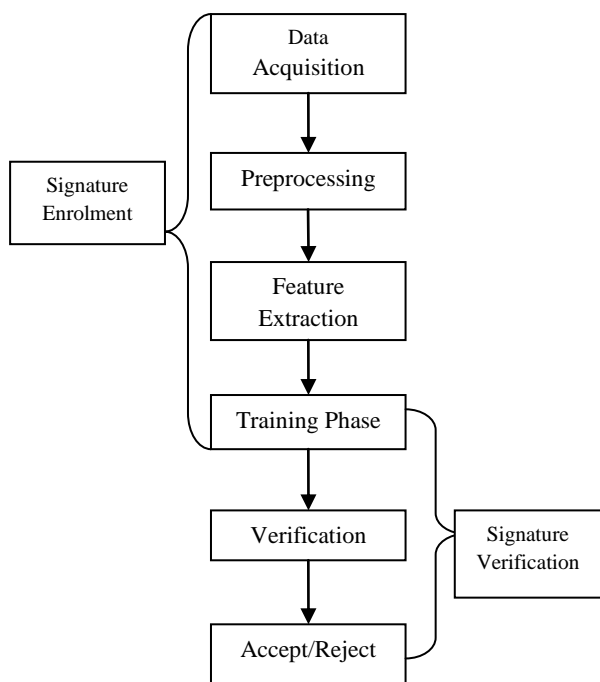


Figure 1: Block Diagram of Offline Signature Verification System

2.1 Data Acquisition

In data acquisition, handwritten signatures are collected from different individuals and some unique features are extracted from them to create a knowledge base for each individual. The system has been tested for its accuracy and effectiveness on data from 25 users with 10 specimens of each making up a total of 250 signatures. The proposed verification algorithm is tested on both genuine and forged signature sample counterparts. A scanner is set to 300-dpi resolution in 256 grey levels and then signatures are digitized.

2.2 Preprocessing

The preprocessing step is normally applied both in training and testing phases. Signatures are scanned in color. Preprocessing is a method that is usually concerned with the preparation of the related information. Generally in any image processing application pre-processing is required to eliminate noise; distortions etc., from the original image and make it ready for feature extraction. It is also applied to improve the efficiency and performance of the SVS. Our preprocessing steps are (Figure 2): RGB to grayscale image conversion where all the scanned images are converted to grayscale images, noise removal for removing spurious pixels that can be attached to the image during scanning time, image cropping is used to remove unwanted region using the Region of Interest (ROI), grayscale image to binary image and thinning for reducing a connected region in the image to a smaller size and minimum cross-sectional width character [24].

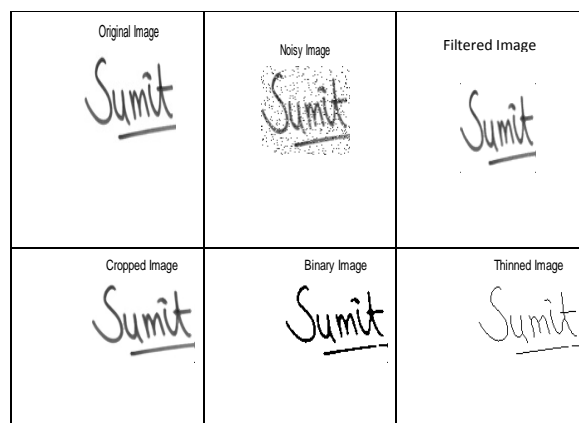


Figure 2: Preprocessing Steps

2.3 Feature Extraction

In this paper, we have extracted global features. Global features depict or categorize the signature as a whole. These features are usually extracted from all the pixels that lie within the region circumscribing the signature image such as the length, width or baseline of the signature. Global features are easily extractable and less sensitive to noise as small distortions in isolated regions of the signature do not cause a major impact on the global feature vector. Features extracted for the system are listed in table 1.

Table 1: Features extracted from sample signatures.

Features	Sample Signature 1	Sample Signature 2	Sample Signature 3
Skew	-4.5825	-4.5878	-4.5874
Kurtosis	21.994	22.6512	22.5690
Area	8864	8900	8904
Height	74	76	75
Width	124	124	125
Density of smoothed image	227.8826	227.9006	228.4213
Density of thinned image	0.9583	0.9604	0.9636
Aspect Ratio	0.5968	0.6192	0.6
Centre of Gravity	62.2217, 37.3140	64.2070, 38.1345	64.5079, 39.2378
Normalized area of black pixels	0.9920	0.9924	0.9926

2.4 Training Phase

For training, Adaptive Resonance Theory 1 (ART-1) has been used. ART-1 refers to a class of self organizing network that clusters pattern space and produce appropriate weight vector templates. Conventional neural networks do not have the property of plasticity, i.e. learning new patterns without washing away previously learned patterns. Normally, in real life patterns keep on changing and network will not be able to see any pattern twice. Under such conditions, back propagation or perceptron will do nothing. It will simply keep on updating weights and all in vein. Another property of ART-1 is that it achieves stability when it cannot return any patterns

to previous clusters (in other words, a pattern oscillating among different clusters at different stages of training indicates an unstable net. Some nets achieve stability by gradually reducing the learning rate as the same set of training patterns is presented many times. However, this does not allow the net to readily learn a new pattern that is presented for the first time after a number of training epochs have already taken place [26].

ART-1 is a vector classifier (Figure 3). It accepts the input and classifies it into clusters if it matches any stored pattern. If it does not match any stored pattern, then a new cluster is created that will behave just like the input vector. It is form of unsupervised learning.

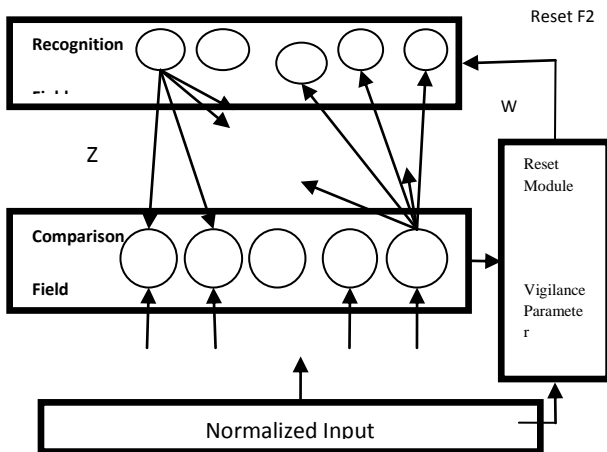


Figure 3: Basic ART-1 Architecture

In training phase, a total of 50 signatures have been used comprising of random, casual and skilled forgeries. For each signature global features have been extracted leading to a database used for training. In this system ART-1 is used which gives better performance.

Table 2: Neural Network Specifications

No. of layers	2
No. of input units	13
No. of output units	2
Learning rate	(0.1-0.9)
Training algorithm	ART-1
Initial weights	Randomized
Initial biases	Randomized
No. of signatures used for training	50
No. of tested signatures	200
No. of epochs	100

2.5 Testing Phase

The testing of a signature is done in two steps i.e. verification and recognition. The verification step compares the signature that is to be tested with the reference signatures stored in the database. The comparison is based on the assumption that the values of the feature sets or structural description extracted from genuine signatures are more stable than the signatures that are forged. That is, the intra-personal variations are smaller than inter-personal variations. So, the given test signature may be accepted or rejected based on its similarity to the reference signature set. In this process, the test specimen is given as input to the system to check whether it is

genuine or forged. The feature values of the test specimen are extracted in the same way as the feature values of training samples are extracted. Recognition is the process in which identity of the signature owner is found. In this step original signature are compared with test signatures and classification ratio is computed. The performance of any signature verification system is typically described by calculating the terms; the false accept rate (FAR) and a corresponding false reject rate (FRR) [5] [27].

False Accept Rate (FAR)

$$= \frac{\text{No.ofaccepted from out of database}}{\text{Total no.of persons in database}} \dots\dots\dots (1)$$

False Reject Rate (FRR)

$$= \frac{\text{No.of correct persons rejected}}{\text{Total no.of persons in database}} \dots\dots\dots (2)$$

3. RESULTS & DISCUSSION

Experiments have been conducted to evaluate the performance of the system. Total number of 200 signatures is used for testing. Table 3 shows the results of the performance obtained with the varying vigilance parameter i.e. ‘ρ’ ranging between 0.1 < ρ < 0.9. The performance evaluation is based on accuracy gained by the system.

Table 3: Performance variations with different vigilance parameter and achieved efficiency

Vigilance Parameter	Efficiency (%)	Training Time (seconds)
0.1	51.7	1.2206
0.2	57.7	1.3908
0.3	60.2	1.4901
0.4	64.4	1.5129
0.5	79.2	1.4720
0.6	76.2	2.0340
0.7	83.2	2.4205
0.8	92.2	2.6795
0.9	97.9	2.7497

From the above table, we can easily interpret that by setting vigilance parameter at 0.9, we can achieve maximum efficiency. The training time at this vigilance parameter is 2.7497 seconds or classification ratio of our system is 97.9%. This is shown in graph in Figure 4.

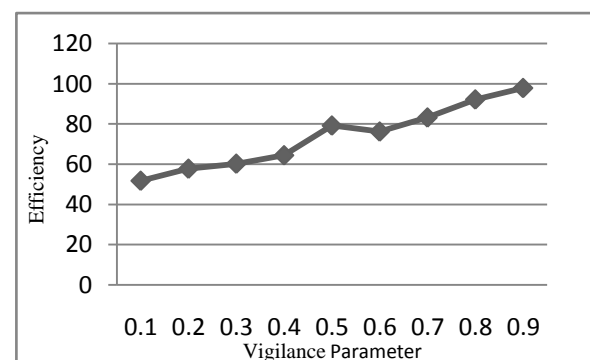


Figure 4: Efficiency versus Vigilance Parameter

Both FAR and FRR depend on the threshold taken to decide whether the signature is genuine is forged. If we choose a high threshold, then the FRR is reduced, but at the same time the FAR also increases. If we choose a low threshold, then the FAR is reduced, but at the same time the FRR also increases.

We obtain a FAR of 2.7% and a FRR of 3.9% taking a threshold value of 90%.

4. CONCLUSION

A neural network technique based on Adaptive Resonance Theory 1 (ART-1) has been presented in this paper for offline signature verification and recognition. A standard database of 250 signatures is used for calculating the performance of SVRS. Conventional neural networks do not have the property of plasticity and stability, hence ART-1 has been used which has both these properties. Developed system is able to recognize counterfeit in case of random, skilled and semi skilled forgeries efficiently. However, the classification ratio achieved by the system was 97.9% and FAR and FRR are 2.7% and 3.9% respectively.

5. REFERENCES

- [1] K. Bowyer, V. Govinda Raju, and N. Ratha, "Introduction to the special issue on recent advances in biometric systems," *IEEE Transactions on Systems, Man and Cybernetics*, vol. B 37, no. 5, pp. 1091-1095, 2007.
- [2] D.Zhang, J.Campbell, D.Maltoni, and R.Bolle, "Special issue on biometric systems," *IEEE Transactions Systems, Man and Cybernetics*, vol. C35 no. 3, pp. 273-275, 2005.
- [3] S.Prabhakar, J.Kittler, D.Maltoni, L.O'Gorman, and T.Tan, "Introduction to the special issue on biometrics: progress and directions," *PAMI* vol. 29, no. 4, pp. 513-0516, 2007.
- [4] S.Liu and M.Silverman, "A practical guide to biometric security technology," *IEEE IT Professional* vol. 3, no. 1, pp. 27-32, 2001.
- [5] S. Lee and J. C. Pan, "Off-line tracing and Representation of Signatures," *IEEE Transactions on Systems, Man, Cybernetics*, vol. 22, no. 4, pp. 755-771, July/August 1992.
- [6] Rasha Abbas, "Backpropagation networks prototype for offline signature verification," *Computer Science*, RMIT, 1994.
- [7] [7] Jingbo Zhang, Xiaoyun Zeng, Yinghua Lu, Lei Zhang, and Meng Li, "A Novel Off-line Signature Verification Based on One-class-one network," *Third International Conference on Natural Computation (ICNC 2007)*.
- [8] Dakshina Ranjan Kisku, Phalguni Gupta, and Jamuna Kanta Sing, "Offline Signature Identification by Fusion of Multiple Classifiers using Statistical Learning Theory," *proceeding of International Journal of Security and It's Applications*, vol.4, no.3, pp. 35-44 , July 2010.
- [9] H. Baltzakisa and N. Papamarkos, "A new signature verification technique based on a two-stage neural network classifier," *Engineering Applications of Artificial Intelligence*, Elsevier (Pergamon), vol. no.14, pp. 95-103, 2001 .
- [10] Emre Özgündüz,Tülin Şentürk and M. Elif Karşılıgil, "Offline Signature Verification and Recognition By Support Vector Machine," *Antalya, Turkey*, pp. 113-116, September 2005.
- [11] Meenakshi K. Kalera, "Offline Signature Verification And Identification Using Distance Statistics," *International Journal Of Pattern Recognition and Artificial Intelligence*, vol.18, no. 7, pp. 1339-1360, 2004.
- [12] Ali Karouni, Bassam Daya, and Samia Bahlak, "Offline signature recognition using neural networks approach," *Procedia Computer Science*, Elsevier, vol. no. 3, pp. 155-161, 2011.
- [13] Ahmad S M S, Shakil A, Faudzi M A, Anwar R M and Balbed M A M, "A Hybrid Statistical Modeling, Normalization and Inferencing Techniques of an Off-line Signature Verification System," *World Congress on Computer Science and Information Engineering*, 2009.
- [14] Nguyen V, Blumenstein M and Leedham G, "Global Features for the Off-Line Signature Verification Problem," *IEEE 10th International Conference on Document Analysis and Recognition*, 2009.
- [15] Bansal A, Garg D, and Gupta A, "A Pattern Matching Classifier for Offline Signature Verification," *IEEE Computer Society First International Conference on Emerging Trends in Engineering and Technology*, 2008.
- [16] Miguel A. Ferrer, Jesu's B. Alonso and Carlos M. Travieso, "Offline Geometric Parameters for Automatic Signature Verification Using Fixed-Point Arithmetic," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 27, no. 6, pp. 389-394, June 2005.
- [17] I'nan Guler, Majid Meghdadi, "A different approach to off-line handwritten signature verification using the optimal dynamic time warping algorithm", *Digital Signal Processing*, vol. no. 18 , pp. 940-950, 2008.
- [18] Hanmandlu M, Hafizuddin M. Yusof M. and Madasu V K , "Off-line signature verification and forgery detection using fuzzy modeling," *Pattern Recognition (Elsevier)*, vol. no. 38, pp. 341-356, 2005.
- [19] Hai Rong Lv, Wen Jun Yin and Jin Dong, "Offline Signature Verification based on Deformable Grid Partition and Hidden Markov Models," *IEEE Conference on Multimedia and Expo, New York*, 2009.
- [20] Armand S, Blumenstein M and Muthuk kumarasamy V, "Off-line Signature Verification based on the Modified Direction Feature," *18th IEEE International Conference on Pattern Recognition*, 2006.
- [21] Bertolini D, Oliveira L S, Justino E and Sabourin R, "Reducing forgeries in writer-independent off-line signature verification through ensemble of classifiers," *Pattern Recognition (Elsevier)*, vol. no. 43, pp. 387-396, 2010
- [22] Vargas J. F., Ferrer M. A., Travieso C. M. and Alonso J. B, "Off-line signature verification based on grey level information using texture features," *Pattern Recognition (Elsevier)*, vol. no.44, pp. 375-385, 2011.
- [23] Bailing Zhang, "Off-line signature verification and identification by pyramid histogram of oriented gradients", *Emerald, International Journal of Intelligent Computing and Cybernetics*, vol. 3 no. 4, pp. 611-630, 2010.
- [24] T.Y.Zhang and C.Y.Suen, "A Fast Parallel Algorithm for Thinning Digital Patterns", *Communications of ACM*, vol. 27, pp. 236-239, 1984.
- [25] M. A. Ismail, and S. Gad, "Offline Arabic Signature Recognition and Verification", *Pattern Recognition*, vol. 33, no. 10, pp. 1727-1740, 2000.
- [26] Plamondon R and Srihari S N, "Online and offline handwriting recognition : A comprehensive survey", *IEEE transactions, Pattern analysis, Machine Intelligence*, vol. 22, no. 1, pp. 63-84, 2000.