Signature Verification by using Radial Basis Function (SVM)

Gurpreet Singh[#], Gurbinder Singh*, Mandeep Singh[#]

Research Scholar, AIET, Faridkot

[#] *Department of CSE, PTU, AIET, Faridkot*

Abstract:- **Computerization has definitely revolutionized the way banking is done these days. However, even today all banking transactions, especially, financial require our signatures to be authenticated. The identifiable side-effect of signatures is that they are vulnerable to forgery. In order to avoid misuse or manipulations on account of forged signatures the need for research in efficient automated solutions for signature recognition and verification has increased in recent years. A concrete system has to be developed which should not only be able to consider these factors but also detect various types of forgeries. Signature verification approaches using information technology can be categorized according to the acquisition of the data: On-line and Off-line. On-line data records the motion of the stylus while the signature is produced, and includes location, and possibly velocity, acceleration and pen pressure, as functions of time. Online systems could be used in real time applications like credit cards transaction or resource access. While off-Line signature verification systems take as input the 2-D image of a signature. Offline systems are useful in automatic verification of signatures found on bank checks and documents. Artificial Neural Network (ANN) which has been modeled on human brain has been successfully used classifier in numerous fields. The present study focuses on detection of these forgeries using Support Vector Machine with Radial Basis Function (SVM – RBF) kernel. For evaluating our system's performance and to know the output unit response accuracy we have developed a classification/confusion matrix and kept our performance goal based on mean square error. It was found that while ANN base system had an overall accuracy of 90% the accuracy of SVM – RBF kernel was significantly higher at 95%.**

Keywords: **- Signature Verification, Radial Basis Function, neural network, SVM etc.**

I. INTRODUCTION

A huge number of customers are influenced consistently by fraud. While a large number of these robberies happen essentially in the virtual world nowadays, there are still numerous crooks who attempt to pass themselves off as another person by fashioning a mark. Whether they are marking checks or different archives, these people are more often than not in it for the cash. You don't need to be a master to have the capacity to tell regardless of whether a mark is manufactured. Everything you need is a little learning and the readiness to be attentive.

Interesting as it is to accept, the lion's share of individuals over and over sign their name utilizing absolutely the same measure of line space. Give this a test by get-together a few illustrations of your signature and measuring them with a conventional ruler. Indeed, even a mark you made quite a while prior will most likely be the same length as one you marked today. On the off chance that you have a known authentic signature and one that makes you suspicious, measure them both with a ruler. Any noteworthy contrast long recommends that one of the marks is a phony or fake.

To overcome this problem, computer algorithms can come to aid, especially algorithms that involved machine learning, this paper proposes a novel method of finding fake signatures using machine learning algorithms, after the section of literature survey. The paper also discusses the outcomes of the proposed method with respect to the neural network algorithm approach with comparative charts and last but not lest, the paper give future directions after the discussion section.

II. LITERATURE SURVEY

Impedovo Donato and Pirlo Giuseppe. "Automatic Signature Verification: The State of the Art". IEEE Transactions on Systems, Man, and Cybernetics—Part C: Applications and Reviews, Vol. 38, No. 5, September 2008.

A systematic review of literature has been carried out in the study concluding that research need not be focused almost exclusively on accuracy improvements, as it has mostly been in the past. Instead, it should address a multitude of issues related to various scenarios of the application themselves.

Pu Danjun, Ball Gregory R , Srihari Sargur N "A Machine Learning Approach to Off-Line Signature Verification Using Bayesian Inference" Computational Forensics Lecture Notes in Computer Science Volume 5718, 2009, pp 125-136.

In this research work the machine learning approach to off-line signature verification has been presented. The prior distributions were determined from genuine and forged signatures of several individuals. The task of signature verification is a problem of determining genuine-class membership of a questioned (test) signature. 3-steps were taken writer independent approach: 1) Determine the prior parameter distributions for means of both “genuine vs. genuine” and “forgery vs. known” classes using a distance metric. 2) Enroll n genuine and m forgery signatures for a particular writer and calculate both the posterior class probabilities for both classes. 3) When evaluating a questioned signature, determine the probabilities for each class and choose the class with bigger probability. By using this approach, performance over other approaches to the same problem was dramatically improved, especially when the number of available signatures for enrollment is small. On the NISDCC dataset, when enrolling 4 genuine signatures, the new method yielded a 12.1% average error rate, a significant improvement over a previously described Bayesian method.

Karouni A. Daya B. Bahlak S. “Offline Signature Recognition Using Neural Network Approach”. Procedia Computer Science, 3 (2011) pp 155-16.

The researchers have presented a method for offline verification of signatures using a set of simple shape based geometric features. The features that have been used were area, centroid, skewness, kurtosis, eccentricity. Artificial neural network was used to classify the signatures as exact or forged and a classification ratio of 93% was obtained under a threshold of 90%

Patil Sandeep, DewanganShailendra. “Neural Network-based Offline Handwritten Signature Verification System using Hu’s Moment Invariant Analysis”. International Journal of Engineering and Advanced Technology (IJEAT), ISSN: 2249 – 8958, Volume-1, Issue-1, October 2011

Although the verification process can be thought to as a monolith component, it is recommended to divide it into loosely coupled phases (like preprocessing, feature extraction, feature matching, feature comparison and classification) allowing us to gain a better control over the precision of different components. This paper focuses on classification, the last phase [machine learning] in the process, covering some of the most important general approaches in the field. Each approach is evaluated for applicability in signature verification, identifying their strength and weaknesses. It is shown, that some of these weak points are common between the different approaches and can partially be eliminated with our proposed solutions. To demonstrate this, several local features were introduced and compared using different classification approaches. Handwritten signatures are considered as the most natural method of authenticating a person’s identity (compared to other biometric and cryptographic forms of authentication).The learning process inherent in Neural Networks (NN) can be applied to the process of verifying handwritten signatures that are electronically captured via a stylus. This paper presented a method for verifying handwritten signatures by using NN architecture. Various static (e.g., area covered, number of elements, height, slant, etc.) , dynamic (e.g., velocity, pen tip pressure, etc.) signature features are extracted and used to train the neural network. Several Network topologies were tested as per this paper and their accuracies compared.

PansereAshwini, Bhatia Shalini “Handwritten Signature Verification using Neural Network”. Volume 1– No.2, January 2012.

As per this paper a number of biometric techniques have been proposed for personal identification in the past. Among the vision-based ones are face recognition, fingerprint recognition, iris scanning and retina scanning. Voice recognition or signature verification are the most widely known among the non-vision based ones. As signatures continue to play an important role in financial, commercial and legal transactions, truly secured authentication becomes more and more crucial. A signature by an authorized person is considered to be the “seal of approval” and remains the most preferred means of authentication. Therefore, the method presented in this paper consists of image prepossessing, geometric feature extraction, neural network training with extracted features and verification. A verification stage includes applying the extracted features of test signature to a trained neural network which will classify it as a genuine or forged.

Dewan Upasana, Ashraf Javed “Offline Signature Verification Using Neural Network Offline Signature Verification Using Neural Networks”. IJCEM International Journal of Computational Engineering & Management, Vol. 15 Issue 4, July 2012.

As per this paper, even today an increasing number of transactions, especially financial, are being authorized via signatures; hence methods of automatic signature verification must be developed if authenticity is to be verified on a regular basis. Verification can be performed either Offline or Online based on the application. Online systems use dynamic information of a signature like velocity, acceleration and pressure captured at the time the signature is made. Offline systems work on the scanned image of a signature. In this paper we present a method for Offline Verification of signatures using a set of simple geometric features. The features that are used are Token length, Average values, Trend Coefficients and Standard Deviations of observation components. Before extracting the features, pre-processing of a scanned image is necessary to isolate the signature part and to remove any spurious noise present. The system in this paper was based on back propagation neural network and is initially trained using a database of signatures obtained from the individual whose signatures have to be authenticated by the system. Then another set of test signatures of the same person are input to the system to check whether they are genuine or forgery. We either accept or reject the test signatures by using a suitable threshold. If the magnitude of the output of the neural network is less than a pre-defined threshold (corresponding to minimum acceptable degree of similarity), the test signature is verified to be genuine else detected as a forgery.

III. RESEARCH GAP

Problem Formulation: After conducting systematic literature survey and associated material related to this research problem, it was found that the most used algorithm used in machine learning for identification forged signatures is neural network. Since, off-Line signature verification systems take as input the 2-D image of a signature. Offline systems are useful in automatic verification of signatures found on bank checks and documents. A concrete system has to be developed which should not only be able to consider these factors but also detect various types of forgeries. The present study focuses on detection of these forgeries using Support Vector Machine with Radial Basis Function (SVM – RBF) kernel.

IV. IMPLEMENTATION STEPS

Signature Data Acquisition

Since our research work is driven mainly based on the observations we got from the samples of signatures we tried to find the nature of the dataset and from the figure 4.1 clearly depicts that it is non linear in nature and it has data points distribution in such a manner that it is will be difficult to find the hyperplane.

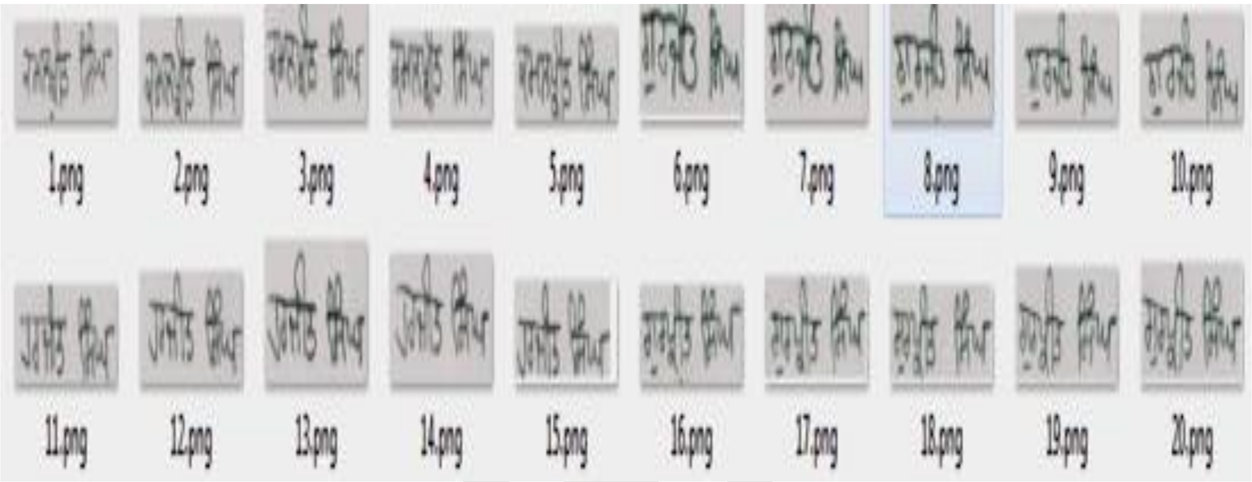

Figure 4.1 Partial lists of images

Table 4.1 Dataset Characteristics

Sr No	Dataset Characteristics:	Multivariate
A	Attribute Characteristic	Real Valued
B	Missing Values	None
C	Number of Instances of Observations:	20
D	Number of Attributes :	05

Table 4.2 Attributes of Observations

Sr No	Attribute	Description	Mathematical Expressions
1	Area	Actual number of pixels in the image	$A_i = \sum_{r=0}^{height-1} \sum_{c=0}^{width-1} I_i(r,c)$
2	Centroid	Horizontal and vertical centers of gravity of signatures	C $_x$= $\frac{\sum C_{ix} A_i}{\sum A_i}, C_y = \frac{\sum C_{iy} A_i}{\sum A_i}$
3	Eccentricity	Ratio of the distance between the foci of the ellipse and its major axis length	Aspect Ratio = $\frac{C_{\max} - C_{\min} + 1}{r_{\max} - r_{\min} - 1}$
4	Skewness	Measure of asymmetry of distribution	S = 1/MN $\sum_{i=1}^{M} \sum_{j=1}^{N} \left[p(i,j) - \mu / \sigma \right]^3$

5	Kurtosis	Measure of flatness of distribution	$K = \left\{ 1/MN \sum_{i=1}^{M} \sum_{j=1}^{N} \left[p(i,j) - \mu/\sigma \right]^4 \right\} - 3$

Step 2: (Signature data pre-processing and feature extraction for signature verification)

1. Read Image Instance from the images file database.
2. Proceed, if image gray type, else convert it to gray.
3. Get all the labeled regions of the image and run region props function.
4. For each labeled region: Calculate numeric values for Area, Centroid, Eccentricity, Skewness and Kurtosis.
5. For each Image instance, get the Path, title and description.
6. Insert each calculated value in step 4, and store in output table.

From the classification matrix as shown in Figure 4.1 and Table 5.1 (SVM – RBF performance matrix) it can be seen that the lower triangular matrix shows the number of misclassifications, while the upper triangular matrix shows the correctly classified signatures. In fact, for calculating the true positive rate we sum up the total number of observations that fall diagonally along this matrix. Output class here represents the output produced by the Artificial Neural Network and Target class represents the actual data (correct signatures). As is visible in the confusion matrix, the proposed algorithm is able to detect forgery 90% of the time.

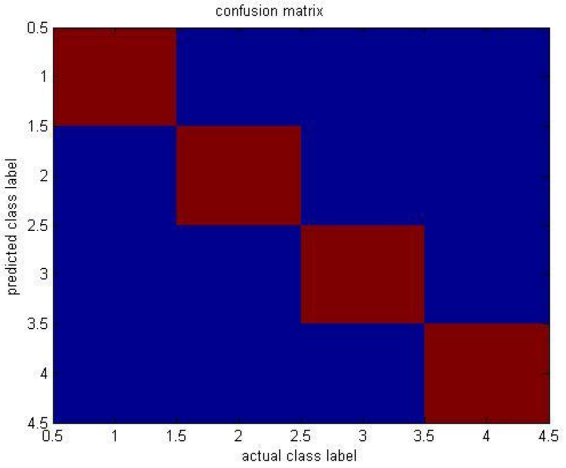

Fig 4.1 (classification matrix)

Since in our study we have taken 4 persons and obtained 5 different signatures from them, with only one being the correct while other four are incorrect. The predicted class represents the extent to which the algorithm is able to detect the correct signatures; while the actual class represents the repository of correct genuine signature.

Table 5.2 **SVM –RBF accuracy**

Fold	Accuracy
Fold 1	75%
Fold 2	77%
Fold 3	86%
Fold 4	93%
Fold 5	95%

V. INTERPRETATION OF RESULTS

The strength of our algorithm is that it identifies genuineness of the signatures so that the round truth is properly matched with the dedicated results. Therefore after designing multiple classifiers with various possible parameters of input observations, hidden layers and fixed number of output classes. We have tried to build a low computational resource intensive as well as less time consuming framework to detect the forgery using radial basis function based SVM algorithm. The selection of parameters for the design of classifier has been meticulously and empirically found after many experiments. The appropriate selection of initial weights for the learning function was found by using Twister Random Algorithm. So that the coverage is maximum and it occurs rapidly (-0.5 and +0.5). For deciding the training and testing patterns. We developed disjoint sets of training and testing datasets and got these validated using K4 cross validation method.

VI. CONCLUSION

It was found that the feature extraction by Color and texture features gives the best performance and more number of features can be extracted using methods explained in methodology section. Data Normalization must be used to reduce the number of samples and the complexity of the neural network and the computation time of the neural network. .For the classification schemes, it was found that training the model with a large number of test data and with fast training algorithm would greatly enhance the accuracy and hence the reliability of the system. The design of our classifier was done by running the neural network with different number of hidden layers and it was apparent from the bar graphs that it affected the accuracy. It was found that as we increase the number of hidden layers there was also an increase in computation time but high order of accuracy is also achieved until we have reached the maximum of hidden layers. Therefore , the use of SVM proved better as it was more accurate also did not had hidden layer concept , thus had low complexity and overhead in process .

VII. FUTURE SCOPE

We can explore more unsupervised machine learning algorithms which would offer more versatile method of identifying forgery by image processing. These methods may be based on some computational clustering technique and which can be evaluated on the basis of recall and precision values. We can further improve the system by reducing the complexity. The accuracy of classifier can also be enhanced by using more and equal number of training patterns. The present study uses ordinary camera (5 mega pixel) and an ordinary scanner (300dpi). Improvement in results can further be obtained by using high resolution camera and scanner. These high resolution devices not only provide enhanced clarity but also lead to considerable reduction in red eye. Besides the features we have used some other parameters like aspect ratio, perimeter, circumference etc. can also be used for correlating the results. As the number of input devices and techniques for handwriting acquisition increases, device interoperability will become an area of greater relevance and need specific investigation. The result of these developments is that signature capture will be feasible in many daily environments by means of fixed and mobile devices, and automatic signature verification will be used in even more applications. "Soft biometrics," the deployment of metadata-based systems for large-scale applications, which can expect both multiethnic and multilingual users, is very important and needs specific consideration.

REFERENCES

[1] A.Piyush Shanker, A.N. Rajagopalan, "Off-line signature verification using DTW", Pattern Recognition Letters 28 (2007) 1407–1414

[2] Alessandro Zimmer and Lee Luan Ling, "Offline Signature Verification SystemBased on the Online Data", EURASIP Journal on Advances in Signal Processing Volume 2008, Article ID 492910, 16 pages.

[3] Alisher Kholmatov, Berrin Yanikoglu. "Identity authentication using improved online signature verification method". Pattern Recognition Letters 26 (2005) 2400–2408

[4] Anil K. Jain, Friederike D. Griess, Scott D. Connell. "On-line signature veri!cation". Pattern Recognition 35 (2002) 2963 – 2972;

[5] Ashwini Pansare, Shalini Bhatia "Handwritten Signature Verification using Neural Network". Volume 1– No.2, January 2012

[6] Bajaj R, Chaudhary S. "Signature Verification Using Multiple Neural Classifiers".

[7] D. Bertolinia, L.S.Oliveirab, E.Justinoa, R.Sabourinc, "Reducing forgeries in writer-independent off-line signature verification through ensemble of classifiers", Pattern Recognition (2009), doi:10.1016/j.patcog.2009.05.009.

[8] Danjun Pu, Gregory R. Ball, Sargur N. Srihari "A Machine Learning Approach to Off-Line Signature Verification Using Bayesian Inference" Computational Forensics Lecture Notes in Computer Science Volume 5718, 2009, pp 125-136,

[9] Donato Impedovo and Giuseppe Pirlo. "Automatic Signature Verification: The State of the Art". IEEE Transactions on Systems, Man, and Cybernetics—Part C: Applications and Reviews, Vol.38,No. 5, September 2008.

[10] H. Baltzakis, N. Papamarkos. "A new signature veri®cation technique based on a two-stage neural network classifier". Engineering Applications of Artificial Intelligence 14 (2001) 95-103

[11] Hao Feng, Chan Choong Wah. "Online Signature Verification Using a New Extreme Points Warping Technique".

[12] J. Coetzer, B. M. Herbst and J. A. du Preez. "Offline Signature Verification Using the Discrete Radon Transform and a Hidden Markov Model". EURASIP Journal on Applied Signal Processing 2004:4, 559–571.

[13] K.R. Radhika, M.K. Venkatesha and G.N. Sekhar, "Off-Line Signature Authentication Based on Moment Invariants Using Support Vector Machine", Journal of Computer Science 6 (3): 305-311, 2010.

[14] Karouni A., Daya B., Bahlak S. "Offline Signature Recognition Using Neural Network Approach". Procedia Computer Science, 3 (2011) pp 155-16;

[15] Luan L. Lee, Toby Berger, and Erez Aviczer. "Reliable On-Line Human Signature Verification Systems". IEEE TRANSACTIONS ON PATTERN ANALYSIS AND MACHINE INTELLIGENCE, VOL. 16, NO. 6, JUNE 1996.

[16] Madasu Hanmandlu, Mohd. Hafizuddin Mohd. Yusof, Vamsi Krishna Madasu. "Off-line signature verification and forgery detection using fuzzy modeling".

[17] Ramachandra A C, Ravi J, K B Raja, Venugopal K R and L M Patnaik, "Signature Verification using Graph Matching and Cross-Validation Principle", International Journal of Recent Trends in Engineering, Vol 1, No. 1, May 2009.

[18] Reza Ebrahimpour, Ali Amiri, Masoom Nazari and Alireza Hajiany, "Robust Model for Signature Recognition Based on Biological Inspired Features", International JournalofComputerandElectrical Engineering, Vol. 2, No. 4, August, 2010.

[19] Sandeep Patil, Shailendra Dewangan. "Neural Network-based Offline Handwritten Signature Verification System using Hu's Moment Invariant Analysis". International Journal of Engineering and Advanced Technology (IJEAT),ISSN: 2249 – 8958, Volume-1, Issue-1, October 2011.

[20] Upasana Dewan, Javed Ashraf "Offline Signature Verification Using Neural NetworkOffline Signature Verification Using Neural Networks". IJCEM International Journal of Computational Engineering & Management, Vol. 15 Issue 4, July 2012