A Novel Approach for Signature Verification using Artificial Neural Network

Vibha Pandey, Sanjivani Shantaiya

Abstract:- This paper presents a new technique for off-line signature verification and recognition. The proposed system is based on morphological features (Shape features).Feature extraction stage is the most essential and difficult stage of any off-line signature verification system. The accuracy of the system depends mainly on the effectiveness of the signature features use in the system. The present research work incorporates a novel feature extraction technique for off-line signature verification system. There are nine features extracted from a static image of signatures using this technique. From the experimental results, the new features proved to be more robust than other related features used in the earlier systems. This approach is implemented in MATLAB and it verifies signatures taking into consideration several novel features and success rate achieved is 99.5%.

Index Terms - Signature, Morphological, Feed Forward Neural Network, Feature Extraction, offline- signature recognition & verification.

I. INTRODUCTION

As available computing power eventually increases and computer algorithms become smarter, tasks that a few years ago seamed completely unfeasible, now come again to focus. This partly explains why a considerable amount of research effort is being recently devoted in designing algorithms and techniques associated with the problems like human handwritten signature recognition and verification.A signature recognition and verification system is a system capable of efficiently addressing two individual but strongly related tasks: (a) identification of the signature owner, and, (b) decision whether the signature is genuine or forger. Within the field of human classification, the procedure of biometrics is emergent because of its distinctive properties such as hand geometry, iris scan, fingerprints or DNA.The use of signatures has been one of the more opportune methods for the recognition and verification of human beings. A signature may be termed a behavioural biometric, as it can modify depending on many essentials such as: frame of mind, exhaustion, etc. The exigent aspects of automated signature recognition and verification have been, for a long time, a true impetus for researchers. Research into signature verification has been energetically pursued for a number of years [1] and is still being explored (especially in the off-line mode) [2]. On-line verification must be differentiated from off-line verification, as the number of features, which may be extracted from on-line mediums, surpass those obtained from off-line verification i.e. time, pressure and velocity can be extracted from on-line modes of verification [3].

Prior approaches, such as that based on fuzzy modeling and the employment of the Takagi-Sugeno model, have been projected using angle features extracted. From a box approach to verify and identify signatures [4]. Also, The GSC (Gradient, Structural and Concavity) trait extractor provided outcome as high as: 78% for verification and 93% for identification [5]. Various classifiers, such as Support Vector Machines (SVMs) and Hidden Markov Models (HMMs), have also been successful in off-line signature verification; SVMs providing an overall enhanced outcome than the HMM-based approach [6]. Study into person identification/verification, including physical character, fingerprint and signature examination has also been investigated [7].In the field of pattern recognition, choosing a dominant set of features is crucial for both the application and the classifier. They uses the direction distribution, moment feature, stroke width distribution and grey distribution to carry out signature verification [8].

Prior work using the Modified Direction Feature (MDF) generated encouraging results, reaching an precision of 81.58% for cursive handwritten character identification [9]. A problem of personal verification and identification is an actively growing area of research. The methods are numerous and are based on different personal characteristics; voice, lip movement, hand geometry, face, odor, gait, iris, retina and fingerprint are the most commonly used authentication methods. All these psychological and behavioral characteristics are called biometrics. The driving force of the progress in this field is above all, the growing role of the internet and electronic transfers in modern society. Therefore considerable number of applications is concentrated in the area of electronic commerce and electronic banking systems [10]. The method of signature verification reviewed in this paper benefits the advantage of being highly accepted by potential customers. The use of the signature has a long history which goes back to the appearance of writing itself [11]. Utilization of the signature as an authentication method has already become a tradition in the western civilization and is respected among the others. The signature is an accepted proof of identity of the person in a transaction taken on his or her behalf. Thus the users are more likely to approve this kind of computerized authentication method [12]. Signature verification systems differ in both their feature selection and their decision methodologies. More than 40 different feature types have been used for signature verification [13] Signature recognition and verification involves two separate but strongly related tasks: one of them is identification of the signature owner, and the other is the decision about whether the signature is genuine or forged. Also, depending on the need, signature recognition and verification problem is put into two major classes: (i) On-line signature recognition and verification systems (SRVS) and (ii) Off-line SRVS. On-line SRVS requires some special peripheral units for measuring hand speed and pressure on the human hand when it creates the signature. On the other hand, almost all Off-line SRVS systems

Manuscript received on August, 2012.

Vibha Pandey, M.tech.(Information Security) Scholar from DIMAT,Raipur (C.G.), India.

Sanjivani Shantaiya, Assistant professor in dept of Computer Science & Engineering at Disha Institute of Management & Technology, Raipur (C.G.) India.

rely on image processing and feature extraction techniques [14].

A.Types of Signature Verification

Based on the definitions of signature, it can lead to two different approaches of signature verification.

1) Off-Line or Static Signature Verification Technique: This approach is based on static characteristics of the signature which are invariant [15]. In this sense signature verification, becomes a typical pattern recognition task knowing that variations in signature pattern are inevitable; the task of signature authentication can be narrowed to drawing the threshold of the range of genuine variation. In the offline signature verification techniques, images of the signatures written on a paper are obtained using a scanner or a camera.
2) On-line or Dynamic Signature Verification Technique: This is the second type of signature verification technique. This approach is based on dynamic characteristics of the process of signing. This verification uses signatures that are captured by pressure sensitive tablets that extract dynamic properties of a signature in addition to its shape. Dynamic features include the number of order of the strokes, the overall speed of the signature and the pen pressure at each point that make the signature more unique and more difficult to forge. Application areas of Online Signature Verification include protection of small personal devices (e.g. PDA, laptop), authorization of computer users for accessing sensitive data or programs and authentication of individuals for access to physical devices or buildings [16].

B. Nature of Human Signature

It is supposed that the features of the process of signing originate from the intrinsic properties of human neuromuscular system which produces the aforementioned rapid movements. Knowing that this system is constituted by a very large number of neurons and muscle, fibers is possible to declare based on the central limit theorem that a rapid and habitual movement velocity profile tends toward a delta-log normal equation [12]. This statement explains stability of the characteristics of the signature. Thus, the signature can be treated as an output of a system obscured in a certain time interval necessary to make the signature. This system models the person making the signature [17].

C. Types of Forgeries

The main task of any signature verification system is to detect whether the signature is genuine or counterfeit. Forgery is a crime that aims at deceiving people. Since actual forgeries are difficult to obtain, the instrument and the results of the verification depend on the type of the forgery [11]. Basically there are three types that have been defined: Random forgery: this can normally be represented by a signature sample that belongs to a different writer i.e. the forger has no information whatsoever about the signature style and the name of the person. Simple forgery: this is a signature with the same shape or the genuine writer's name. Skilled forgery: this is signed by a person who has had access to a genuine signature for practice [16].

II. RELATED WORK

As signatures continue to play an important role in financial, commercial and legal transactions, truly secured authentication becomes more and more crucial. This section presents the current approaches for verification of signatures in offline mode. To perform verification or identification of a signature, several steps must be performed. After preprocessing all signatures from the database by converting them to a portable bitmap format, their boundaries are extracted to facilitate the extraction of features using MDF. Verification experiments are performed with neural-based classifiers. Experiments have been performed with the "Grupo de Procesado Digital de Senales" (GPDS) signature database [10].

The next approach presents a set of geometric signature features for offline automatic signature verification based on the description of the signature envelope and the interior stroke distribution in polar and Cartesian coordinates. The features have been calculated using 16 bits fixed-point arithmetic and tested with different classifiers, such as hidden Markov models, support vector machines, and Euclidean distance classifier. The experiments have shown promising results in the task of discriminating random and simple forgeries. The geometrical features proposed by this method is based on two vectors which represent the envelope description and the interior stroke distribution in polar and Cartesian coordinates [18].

The next approach for Off-line Signature Verification is based on Fusion of Grid and Global Features Using Neural Networks. The global and grid features are fused to generate set of features for the verification of signature. The test signature is compared with data base signatures based on the set of features and match/non match of signatures is decided with the help of Neural Network. The performance analysis is conducted on random, unskilled and skilled signature forgeries along with genuine signatures [19].

This approach is based on compression neural networks; It is a novel robust technique for the off-line signature verification problem in practical real conditions is presented. The technique is based on the use of compression neural networks, and in the automatic generation of the training set from only one signature for each writer. This methods incorporates a new kind of acceptance/rejection rule, which is based on the similarity between subimages or positional cuttings of a test signature and the corresponding representation stored in the class compression network [20].

This approach uses principle component analysis for off-line signature identification method based on Fourier Descriptor (FDs) and Chain Codes features. Signature identification classified into two different problems: recognition and verification. In recognition process Principle Component Analysis was used. In verification process multilayer feed forward artificial neural network was used [21].

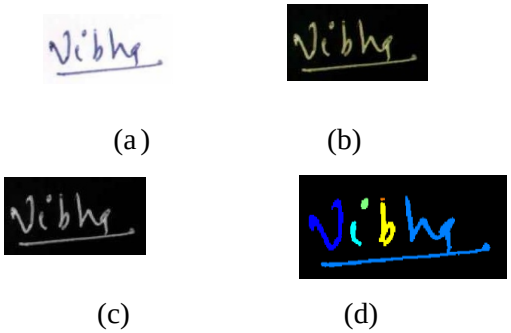
III. METHODOLOGY

To perform verification or identification of a signature, several steps must be performed. After preprocessing all signatures from the database, then by enhancing the image various features has been extracted. Verification experiments are performed with neural-based classifiers.

The present work has been carried out in two steps. Initially a set of signatures are obtained from the subject and fed to the system. These signatures and preprocessed then the preprocessed images are used to extract relevant features like Extent, Solidity, Number of objects, Majoraxislength, Equivdiameter, Area, Convex area, Orientation and Euler number that can distinguish signatures of different persons. These are used to train the system. The proposed methodology or procedure for classification of signature image are as follows:

A. Preprocessing

In the preprocessing phase, first image is acquired, after that it has been converted into gray image then enhanced for the removal of noise.The following are the results obtained in this phase:-



(a) (b)

(c) (d)

Fig. 1: a) Original Image b) Complemented Image c) Gray Image d)Rgb Image based on number of objects

B. Feature Extraction

Feature extraction stage is the most vital and difficult stage of any off-line signature verification system. The accuracy of the system depends mainly on the effectiveness of the signature features used in the system.

Calculation of various features:-

1) Total Area(TA) :- It specifies the actual number of pixels in the region .It can be calculated by the formula

   TA= Number of pixels/region covered

2) Convex Area(CA) :- It specifies the number of pixels in convex image.It can be calculated by the formula

   CA= No. of pixels/convex image

3) Equivdiameter(ED):-It specifies the diameter of circle with the same area as the region. It can be calculated by the formula

   ED = sqrt(4*area/pi)

4) Euler Number (EN)=It specifies the number of regions in the objects-Number of holes in those objects. It can be calculated by the formula

   EN= (No. of regions – No. of holes)in the object

5) Extent (ET):-It specifies ratio of pixels in the region to pixels in total bounding box. It can be calculated by the formula

   ET= Area/Total area of bounding box

6) Major Axis Length (MAL):-It specifies the length of major axis of the ellipse.

7) MeanOrientation(MO):-It specifies the angle between x-axis and major axis of the ellipse.

8) Solidity (SD):- It specifies the proportion of the pixel in the convex hull that are also in the region. It can be calculated by the formula

   SD = Area/Convex Area.

9) Number of objects (NOB):-It counts each character of the signature called as objects.

The below table shows the values obtained in the feature extraction phase.Here SS represent the signature samples ,GS represent the genuine sample and FS represent the forge samples.These values are the input for the next phase.

Table I: Results of Extracted Features

SS	NOB	EN	TA	MO	ED	ET	SD	CA	MAL
GS	6	5	2154.00	2.16	107.79	2.83	3.86	7566.00	288.14
	8	5	2415.00	2.16	133.71	3.30	5.58	5155.00	446.27
	6	4	2204.00	-16.83	123.88	2.13	3.45	4534.00	389.57
	6	2	2144.00	-14.32	121.11	1.86	3.49	4681.00	342.09
	6	3	2198.00	-2.63	116.15	1.22	2.53	5245.00	370.71
FS	8	5	2641.00	-24.85	137.67	3.29	5.34	5985.00	435.81
	8	5	2590.00	17.27	137.71	3.99	5.30	6232.00	453.70
	7	5	2235.00	-6.94	127.53	2.93	4.50	4638.00	405.51
	7	3	2606.00	-5.99	127.24	3.36	4.53	6049.00	466.53
	5	4	2417.00	-12.28	109.76	1.64	3.03	6043.00	352.11

C. Neural Network Classifier

For the training of dataset ANN has been used. The features that have been extracted from signature images are fed as an input to an Artificial Neural Network using feed forward back propagation. In this network, the information moves in only one direction, forward, from the input nodes, through the hidden nodes and to the output nodes. Feed forward neural network begins with an input layer. The input layer may be connected to a hidden layer or directly to the output layer. In order to train the neural network, a set of training signature images were required, and the varieties were predefined. During training, the connection weights of the neural network were initialized with some random values. The training samples in the training set were input to the neural network classifier in random order and the connection weights were adjusted according to the error back-propagation learning rule. Feed forward back propagation neural network classifier is used to verify the signatures. Database has been split into two parts, to perform the training and testing components. From the genuine set, 8 samples of each signature were used for training, and 2 for testing. We used 8 samples of each signature for training the forged signatures and 2 for testing purposes.

IV. RESULTS AND DISCUSSION

In the present research work a database of about 200 genuine and 200 forgery signatures of different individuals had been taken.The research work has been carried out using following procedure. First the input images are acquired then the images are preprocessed by complement, gray scale, background subtraction and binary image conversion. Then feature extraction is done and the system is trained using feed forward neural network. Then the unknown images are been tested against the trained network to obtain the classification process. The results are obtained in the form of 0 & 1, where 0 represents false or forge signature and 1 represents true or genuine signature.

Table II: Results Using Feed Forward Neural Network

Signature samples	Decision
Genuine	0.99(approx 1)
Forged	0.02(approx 0)

V.CONCLUSION

This paper proposed a novel approach for feature extraction of a signature for offline verification. The results obtained from this research work shows the following conclusion:-

- Using novel features verification of signature have been achieved.
- Accuracy of about 99.5% has been achieved In future research, a larger signature database will be collected, including multilingual signatures, to investigate the techniques proposed in this paper. This technique will be used as a further references for many classification technique and it can be extended for online signature verification system.

REFERENCES

1. K. Han, and I.K. Sethi, "Handwritten Signature Retrieval and Identification", Pattern Recognition 17, 1996, pp. 83-90.
2. S. Chen, and S. Srihari, "Use of Exterior Contour and Shape Features in Off-line Signature Verification", 8th International Conference on Document Analysis and Recognition (ICDAR '05), 2005, pp. 1280-1284.
3. A. Kholmatov, and B. Yanikoglu, "Identity Authentication using improved online signature verification method", Pattern Recognition Letters, 2005, in press.
4. M. Hanmandlu, M.H.M. Yusof, and V.K. Madasu, "Off-line Signature Verification using Fuzzy Modeling", Pattern Recognition 38, 2005, pp. 341-356.
5. M.K. Kalera, S. Srihari, and A. Xu, "Off-line signature verification and identification using distance statistics", International Journal of Patern Recognition and Artificial Intelligence 18(7), 2004, pp. 1339-1360.
6. E.J.R. Justino, F. Bortolozzi, and R. Sabourin. "A comparison of SVM and HMM classifiers in the off-line signature verification", Pattern Recognition Letters 26, 2005, pp. 1377-1385.
7. H. Srinisvasan, M. J. Beal and S.N. Srihari, "Machine Learning approaches for Person Identification and Verification", SPIE Conference on Homeland Security, 2005, pp. 574-586.
8. H, Lv, W. Wang, C. Wang and Q. Zhuo, "Off-line Chinese Signature Verification based on Suppor Vector Machines", Pattern Recohnition Letters 26, 2005, pp. 2390-2399.
9. M. Blumenstein, X.Y. Liu, and B. Verma, "A Modified Direction Feature for Cursive Character Recognition", International Joint Conference on Neural Networks (IJCNN '04), 2004, pp. 2983-2987.
10. L.E. Martinez, C.M. Travieso, J.B. Alonso, and M. Ferrer, "Parametrization of a forgery Handwritten Signature Verification using SVM", IEEE 38th Annual 2004 International Carnahan Conference on Security Technology, 2004, pp. 193-196.
11. Kalenova," Personal Authentication using Signature Recognition", D.2005.
12. Plamondon, "The Handwritten Signature as a Biometric Identifier: Psychophysical Model & System Design" IEE Conference Publications, R.1995,Issue CP408, 23-27.
13. Jain, A., Griess, F., and Connel1, S. "Online Signature Recognition", Pattern Recognition, vol.35,2002, pp 2963-2972.
14. OZ, C. Ercal, F. and Demir, Z. Signature Recognition and Verification with ANN.
15. Ozgunduz, E., Karsligil, E., and Senturk,,"Off-line Signature Verification and Recognition by Support Vector Machine", T. 2005 .Paper presented at the European Signal processing Conference.
16. Aykanat C. et. al ,(Eds). 2004. Proceedings of the 19th International Symposium on Computer and Information Sciences, ISCIS 2004. Springer-Verlag Berlin Heidelberg New York. pp. 373-380.
17. Pacut, A. and Czaja,"Recognition of Human Signatures. Neural Network", A. 2001,in proceedings of the International Conference on Neural Network, IJCNN'01, vol.2, pp 1560-1564.
18. 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, June 2005.
19. Shashi kumar , K.B.raja, R.K. Chhotary, Sabyasachi Pattanaik, "Off-line Signature Verification Based on Fusion of Grid and Global Features Using Neural Networks", Shashi Kumar et. al. / International Journal of Engineering Science and Technology Vol. 2(12), 2010, 7035-704
20. José F. Vélez, Ángel Sánchez and A. Belén Moreno," Robust Offline Signature Verification using compression networks and positional cuttings", Escuela Superior de Ciencias Exper imentalesy Tecnología Universidad Rey Juan Carlosc/ Tulipán, s/n 28933- Móstoles (Madrid), SPAIN.
21. Ismail A. Ismail 1, Mohamed A. Ramadan 2, Talaat S. El- Danaf 3 And Ahmed H. Samak ,"An Efficient Off-line Signature Identification Method Based On Fourier Descriptor and Chain Codes", IJCSNS International Journal of Computer Science and Network Security, Vol.10 No.5, May 2010.

AUTHORS PROFILE

Vibha Pandey, obtained her Master of Computer Application (MCA) from SSCET, Bhilai, C.G. in 2007. She is an M.tech.(Information Security) Scholar from DIMAT,Raipur, India. Her research area includes Cryptography and Biometric based application development.

Sanjivani Shantaiya, obtained her B.E. (Computer Science & Engg.) in 1999 from VYWS college of Engineering ,Badnera,Amravati and M.Tech (Computer Science & Engg.) from RIT Raipur in 2010. She is Assistant professor in dept of Computer Science & Engineering at Disha Institute of Management & Technology, Raipur (C.G.) India. Her research area includes Cryptography; Biometric based application and Image processing.