Performance Evaluation of Energy, Angle, Chain Code and Their Mixed Method over Different Training Subsets

Imran Hussain
M.Tech
I.T
I.T.M. Bhilwara
imran.hussain1983@gmail.com

Vikash Shrivastava
Sr. Technical Architect
I- GATE Global
Limited, Noida (U.P.)
vikash_shrivastava@yahoo.com

Rajesh Jatoliya
Sr. Lecturer
C.S. Department
ITM,Bhilwara
raj.pearl7@gmail.com

Vivek Kr. Shrivastava
Asst. Prof. & HOD-IT
ITM, Bhiwara
Rajasthan
viveks2001@gmail.com

Abstract:- For identification of a particular human being signatures prove to be an important biometric. The signature of a person is an important biometric attribute of a human being which can be used to authenticate human identity. However human signatures can be handled as an image and recognized using computer vision and neural network techniques. With modern computers, there is need to develop fast algorithms for signature recognition. There are various approaches to signature recognition with a lot of scope of research. In this paper, off-line signature recognition & verification using neural network is proposed, where the signature is captured and presented to the user in an image format. Signatures are verified based on parameters extracted from the signature using various image processing techniques. This paper evolutes the performance of signature verification technique based on the angle, energy and chain code feature of signature.

Keywords - Signature, Authentication, Feed Forward Neural Network, biometric, offline-signature recognition & verification.

I. INTRODUCTION

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. H. Lv *et al* used 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 type of 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 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 boundary of each signature must be extracted prior to the feature extraction process. The features extracted must be appropriate for both the application and the classifier used. MDF has been used to extract features for the signature verification problem. This technique employs a hybrid of two other feature extraction techniques, Direction Feature (DF) and the Transition Feature (TF). Another features like centroid, tri surface, length feature,sixfold surface feature, best fit feature were extracted by this method[9].

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].

The next approach is Neural Network based approach in which various approaches were done by various people to achieve highest accuracy as well as FAR & FRR. Till now the accuracy, FAR and FRR features were compared on the basis of Energy Density, Angle, Chain Code and mix of Energy Density with Angle and mix of Energy Density with Chain Code features. The details of these techniques are depicted below.

a. Energy Density

In this method, two features are used for training. Aspect ratio is used as a global feature and energy density is used as local feature. Aspect ratio is the ratio of Height (maximum vertical distance) to length (maximum horizontal distance) of the signature. It is calculated after skew removal. Energy density is defined as the total energy present in each segment. 100 segments of each signature is done and energy density is obtained by counting the total number of 1s in each segment (i.e. Total White Pixels). Thus, the feature vector of size 101X1 for energy density method as final database. This final database is fed to the neural network to perform the desired function i.e. training or classification.

b. Chain Code

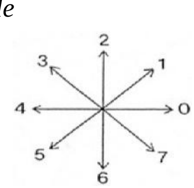

Fig. 1 Connectivity of a Pixel

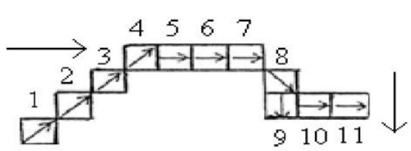

Fig. 2. Direction Changes in a Part of a Signature

Chain code is based on the direction of the connecting pixels. Each pixel is observed for next connected pixel and their direction changes mapped by giving a numerical value to every possible direction. There are generally 8 connectivity is taken into consideration as shown in the Fig. 1. But in this technique 4 connectivity i.e. 0, 1, 2 & 3 is used. As another 4 directions i.e. 4, 5, 6 & 7 are simply the negation of 0, 1, 2 & 3 directions. To obtain chain-code top left corner is considered as origin and scanning is done left to right, top to bottom (refer Fig. 2). Each pixel has observed separately and direction vector for that pixel is noted down. This process is carried out until the last pixel has scanned. Now, the frequency of occurrence in a particular direction is calculated for each segment and the histogram for each segment is used it to train the neural network.

c. Angle

In this method first the Pre-processing image is resized and partitioned into four portion or cell using the equal horizontal method after that each partition(cell) are divided in to 3 row and 3 column of equal size so we have total nine sub cell of each cell. After that consider the sub cell one by one and calculate the angle of each with pixels by considering the bottom left corner after that calculate the mean value of the angles this process is repeat for all the sub cells. Once the value of angle for each sub cell is found then calculating the mean value from that to determine the value of angle for that cell or partition. This process is repeat for the reaming three partitions, so at the end we have the angle vector of size 1*4. This is given as an input to the neural network. For example the data base used consist 100 signature samples. For one sample we have angle vector of size 1*4 so for all 100 sample we have feature vector of size 100 *4 which is used as a final data base for training the neural network and also for classification.

III.PROPOSED EVALUATION OF NEURAL NETWORK BASED TECHNIQUE

The signature is verified using various technique, in this paper we want to concentrate on offline signature verification technique based on the neural network. Till now the signature is verified by the help of neural network by analysis the various features of signature like energy, angle and chain code. But the problem is that no one till now compares these techniques on a single platform to tell which technique is better? So in this paper we want to give the answer of this question by comparing various features like angle, energy, chain code and mix of energy with chain code and mix of energy with angle features based techniques by taking eleven combination of original and forgery signature. These combinations are (0o,100f), (10o,90f), (20o,80f), (30o,70f), (40o,60f), (50o,50f), (60o,40f), (70o,30f), (80o,20f), (90o,10f), (100o,0f) in which 'o' represents original and 'f' represents forgery. As we know that in neural network firstly training has to be given to the neural network after that classification has been carried out. So here we first trained the neural network with one of the above specified combination and after that classification has been performed on all eleven samples. The table 1. below shows the outcome of the verification process.

Table 1.

TRAINING	**CLASSIFICATION (AVERAGE VALUES)**				
(Original, Forgery)	**ENERGY**	**ANGLE**	**CHAIN CODE**	**MIXED EA**	**MIXED EC**
(0o,100f)	50%	50%	50%	50%	**51%**
(10o,90f)	65%	58%	83%	82%	**85%**
(20o,80f)	77%	75%	97%	85%	**98%**
(30o,70f)	81%	82%	95%	89%	**99%**
(40o,60f)	82%	86%	98%	88%	**99%**
(50o,50f)	75%	54%	94%	82%	**95%**
(60o,40f)	81%	83%	95%	89%	**99%**
(70o,30f)	79%	80%	73%	88%	**98%**
(80o,20f)	72%	73%	95%	83%	**97%**
(90o,10f)	65%	64%	96%	77%	**98%**

IV. CONCLUSION AND FUTURE WORK

This paper focused on the offline signature verification based on the various features like angle, energy, chain code and mix of energy with chain code (**MIXED EC**) and mix of energy with angle (**MIXED EA**) features. As per the above specified results we can conclude that in offline signature verification based on features of the signature the mixed energy with chain code feature gives better result. But the individual values in some case of chain code and some cases of energy with angle gives considerable results. So this can be taken for future studies to more elaborate this area.

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 Experimentales y TecnologíaUniversidad 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.