ISSN:0975-9646

Priyank Jain et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (1) , 2014, 211-216

Online Signature Verification Using Energy, Angle and Directional Gradient Feature with Neural Network

Priyank Jain , Jayesh Gangrade

Computer Science, RGPV Bhopal
IES IPS ACADEMY INDORE (M.P.)INDIA

Abstract— Signature used as a biometric is implemented in various systems as well as every signature signed by each person is distinct at the same time. It is very important to have an online computerized signature Verification system differentiate digital signature. Hand written signature used every day at various places (Bank, Office etc.) for the authentication of a person, but a signature of a person may not be same at different time or it may be generated by some fraud way. So the robust system is required for verification of the signature. The signature verification can be done either online or offline, here we are using online signature verification network. In the proposed system the signatures is taking as a image by the signature pad and apply image processing technique before the feature extraction to make the system effective. It is pattern recognition process identifies the similarity of two patterns. This process also governs the fact that no two individual exhibits similar signature or handwriting genuinely. The angle, energy and chain code features are used in this paper to differentiate the signature. Neural network is used as a classifier for this system. The studies of online signature verification are given in this paper.

Keywords— Directional Feature, Energy Density, Chain Code, Neural Network, Neuron, pad and pen.

I. INTRODUCTION

For human identification, the usage of biometrics is important in daily routine. Signature may be used as a biometrics as every signature is distinct. The problem occur in signature verification system is hard to decide whether the two different signature signed by the genuine signer is identical or not because the signature signed by the person may vary according to its mood, health, etc. As signature has already used and accepted as an identification of the person who signed in so many systems, it is important to keenly observe the signature because it may be forgery before having any conclusion about the signee. This gives rise to a computerized signature verification system. Signature verification is quite important in different sectors like financial organizations, business sector and governments to authorize confidential documents and transactions. With spread of internet and its frequent use, signature verification has become very important
in need since forgery and fraud may cost lot of damage including money, repute and time. Signature verification environment requires Fast, reliable, real-time authentication high-volume, transaction-oriented environments. Out of all, available solutions for automatic signature verification techniques, there are specific features that need to be identified and resolved and if any attribute is to be addressed, the corresponding data value must be fetched. Before modelling the computerized signature verification system, better we should know about different type of forgeries

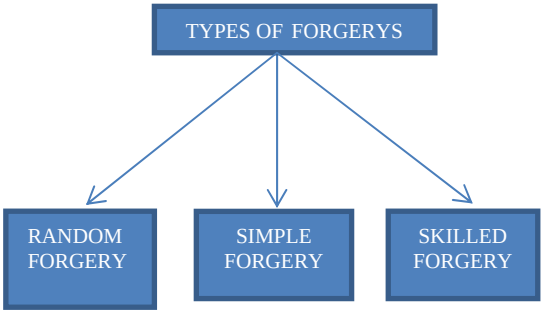

Fig. 1: Types of forgery

- Random forgery: It produced without any knowledge of signature shape or even the signer's name.
- Simple forgery: It is produced by knowing only the name of the signer's but without having any examples of signer's signature style.
- Skilled forgery: It is produced by looking at an original signature sample, attempting to imitate it as closely as possible.

The random & simple forgery is easily detecting but skilled forgery required efforts. So our proposed work is based on skilled forgery.
Types of signature verification system
a) On-Line or Dynamic Signature Verification system.
b) Off-Line or Static Signature Verification system.
Off-line verification system requires less hardware and depends upon the static features of signature image. Where as in the On-line system dynamic feature are taken into consideration, which include the time when stylus is in and out of the contact with the paper, the total time taken to make signature and the position where the stylus is raised from and lowered onto the paper, number of break points, maximum/minimum pressure of stylus contact, speed etc. The main problem is that a signature of a person may vary according to his/her mood, health etc. even the genuine signer may not copy his/her signature as it is. There will always a change observed. Then it seems somewhat difficult to distinguish between genuine signature and a forgery.

Signature Characteristics

The system used for analysis of signature must use the concepts of image processing. Most probable, it is possible that the signature of a signer varied for every sign but there must be some unique characteristic to identify the signature so that it can be used as biometrics. Some essential characteristics are listed below:

a) Invariant: It should be constant over a long period of time.

b) Singular: It must be unique to the individual.

c) Imitable: It must be irreproducible by other means.

d) Reducible and comparable: It should be capable of being reduced to a format that is easy to handle and digitally comparable to others.

II. METHODOLOGY

2.1 Data acquisition

Online signature verification system used pad and pen for capture the signature image .Signature pattern has been captured firstly while the user doing signature. Then it is transformed into frames. On the other hand, the series of patterns can also be captured out of which static patterns are then retrieved out. The static patterns are attained by hardware while a signature being done that tracks the position of pen moment. For data acquisition, we have taken a hardware device. Below is the figure of that.

Fig.2: Hardware Device for data acquisition

2.2 Data pre-processing

The Input signature database is pre-processed, which provides required input set for the further learning. For data pre-processing noise reduction, skew removal and segmentation is to be done.

Binarization is performed on input image for converting the image into black and white image and we consider black partition as 0 and white partition as 1.

Skew removal is used for inclining the signature to normal position.

Thinning is performed over the binary image to obtain a single pixel thick skeleton of the signature instance. This image is used to obtain a number of features later. The standard thinning algorithm using morphological operation is used for this purpose.

Segmentation means dividing the signature image into small parts. Segmentation is done using the sub-matrix access.

There are three-feature extraction method are used in our proposed system Angle, Chain-Code and Energy Density method, which are discussed as follows.

2.3 Angle Feature Method

In Angle method first the Pre-processing image is resized and partitioned into 4 equal segment using the equal horizontal method after that each segment are divided in to 3 row and 3 column of equal size so we have total nine minor segment of each segment. After that consider taking each part of minor segment 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 the entire minor segment. Once the value of angles for each minor segment is found then calculate the mean value from that to determine the value of angle for that cell or partition. This process is repeated for the remaining 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.

Fig. 3: Resize original image after preprocessing

Fig. 4: After Resizing original image partition into four equal part

Fig. 5: Image is partitioned into nine equal parts

Fig. 6: Finding the angle of each white pixel and calculate the mean value

2.4 Chain-Code Method

Chain-code method is based on the direction of the connecting pixels. Each pixel is observed for next pixel for connectivity and their direction changes mapped by giving a numerical value to every possible direction. To obtain chain-code top left corner is considered as origin and scanning is done left to right, top to bottom. Each pixel has observed separately and direction vector for that pixel is noted down. This process is repeat until the last pixel has connected.

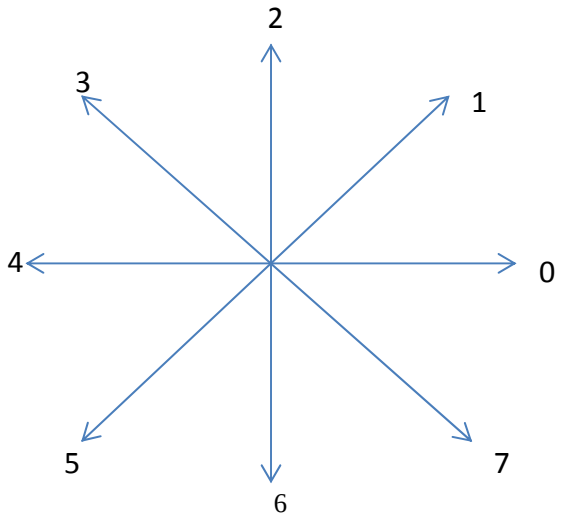

Fig. 7: 8 Connectivity of a pixel

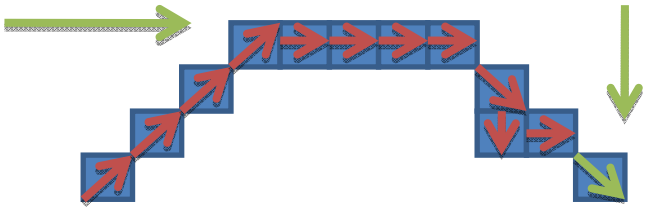

Fig. 8: Direction Changes in a Part of a signature

2.5 Energy Density

Online signature verification system the input signature image is segmented in to the 4 equal segment and calculating the number of ones in each segment. In addition, we are considering the Aspect ratio, which is used as a global feature, but here we normalize it for all segments. Aspect ratio is the ratio of height (maximum vertical distance) to length (maximum horizontal distance) of the signature. We have calculated it after segmentation. Thus, we have a feature vector of size 1*4 for a single signature image and it is used as a final database in an energy density method. For 300-signature image, we have feature vector of size 300*4. This final database is fed to the neural network to perform the desired function i.e. training or classification. The white portion of image is considered as 1 and black portion is considered as 0.

Fig. 9: Image partitioned into four parts

2.6 Artificial Neural Networks

Neural Network (NN) is a mathematical model or Computational model based on biological neural networks. Neural networks are named after the cells in the human brain that perform intelligent operations. The brain is made up of billions of neuron cells. Each of these cells is like a tiny computer with extremely limited capabilities; however, connected together, these cells form the most intelligent system known. Neural networks are formed from hundreds or thousands of simulated neurons connected together in much the same way as the brain's neurons. Just like people, neural networks learn from experience, not from programming. ANN are composed of a large number of highly interconnected processing elements (neurons) working in unison to solve specific problems.

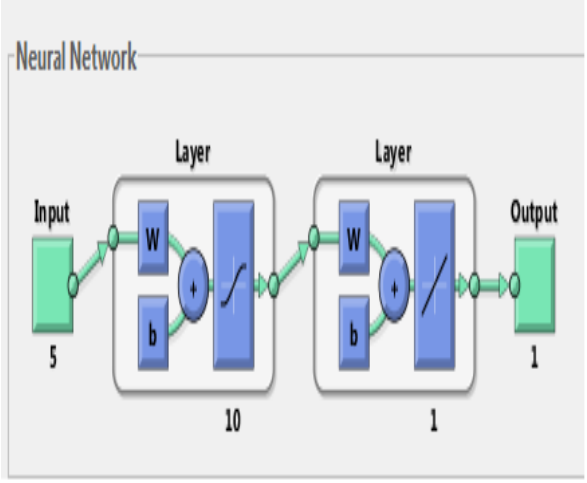

Fig. 10: Artificial Neural Networks

III. RESULT

The proposed system is tested on generated real signature database to show the effectiveness of the proposed system. Raw Signature Database is gathered from 6 people in which 50 Genuine from each individual is collected (i.e. 300 Signature Samples) using digitized paid. For comparison and performance evaluation of the proposed methodology, we have training and classification. A comparison for all the three methods has done based on above-mentioned parameters. Now the result obtained from the proposed technique (mix of Angle, Chain Code with Energy Density) is compared with Angle Feature Method, Chain-Code and Energy Density Method.

Training: Training process refers to preparing and training of neural network for doing the classification work with an optimum accuracy for online signature verification.

Classification: In classification phase, system under test takes an image of the signature as input and verifies whether the input image matches with the genuine training signature image available in the database or not. This is identifying the authenticity of the signature.

Online Classifier: In online classification phase, system under verification phase and after verification system generate result that the person is authorize or not or unidentified.

If signature of a person is similar to another person in that case online classifier, generate the name of another person at output or result of online classifier.

3.1 Result Tables and Graphs of Training and Classification

Table 1: Is the part of train with 240 signatures and tested with 60 signatures

TRAIN WITH 240 SIGNATURE AND TEST WITH 60 SIGNATURE				
MEAN SQUARE ERROR	**TIME**	**FEATURE**	**ACCURACY (%)**	**CORRECT IDENTIFICATION**
0.052213	O.17315	ENERGY	80	48
0.69721	0.51713	ANGLE	18.4	11
0.004473	2.0416	DIRECTION	71.7	43
0.00991	4.5645	MIXED	78	47

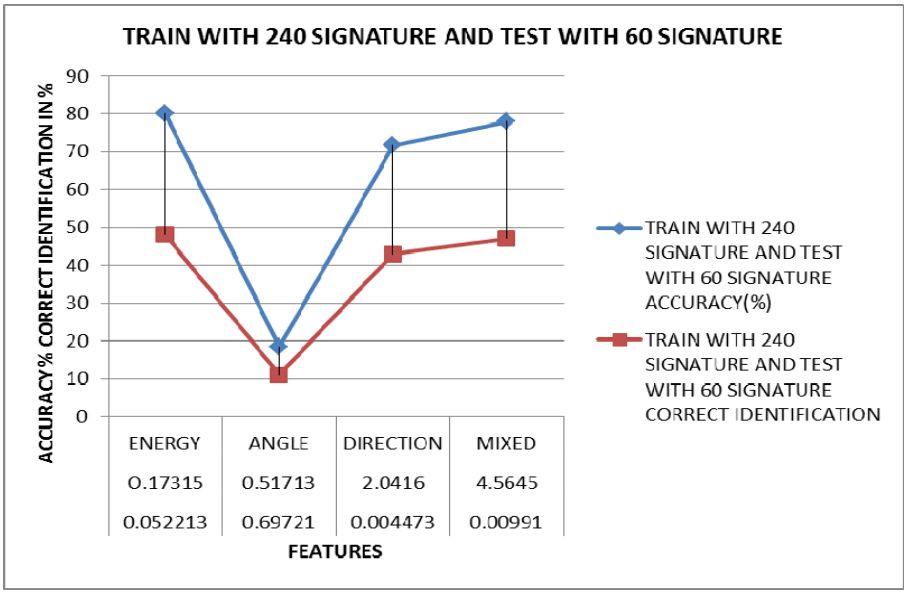

Figure 11: Graph comparison of training and testing within 240 & 60 signatures

Table 2: Is the part of train with 180 signatures and tested with 120 signatures.

TRAIN WITH 180 SIGNATURE AND TEST WITH 120 SIGNATURE				
MEAN SQUARE ERROR	**TIME**	**FEATURE**	**ACCURACY(%)**	**CORRECT IDENTIFICATION**
0.08368	0.1377	ENERGY	73.3	88
0.55288	0.42095	ANGLE	8	10
0.00881	1.3308	DIRECTION	75	90
0.00975	2.9179	MIXED	73.4	88

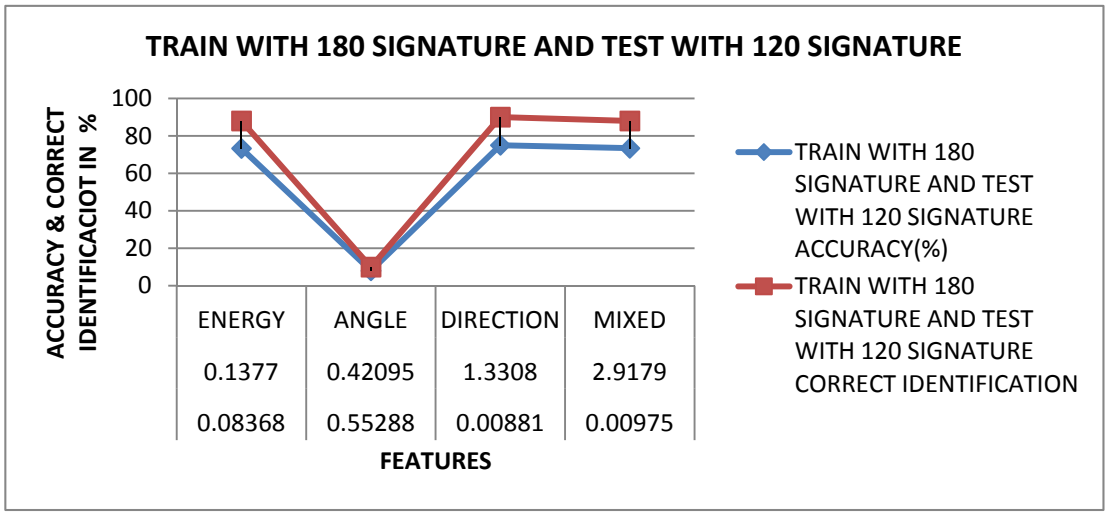

Figure 12: Graph comparison of training and testing within 1800 & 120

3.2 Result Tables of Online Classifier

Table 3: Generated result table by using (Monika signature)

monika	Energy	angle	chain code	mixed feature
1	Unidentified	unidentified	unidentified	unidentified
2	Unidentified	unidentified	sheela	monika
3	Unidentified	unidentified	milind	unidentified
4	Unidentified	arvind	monika	monika
5	Sheela	unidentified	unidentified	unidentified
6	Unidentified	unidentified	monika	monika
7	Unidentified	unidentified	sheela	monika
8	Unidentified	unidentified	unidentified	unidentified
9	sheela	priyank	unidentified	monika
10	sheela	unidentified	unidentified	monika

Table 4: Generated result table by using (milind signature)

priyank	energy	angle	chain code	mixed feature
1	unidentified	unidentified	milind	milind
2	milind	priyank	unidentified	priyank
3	unidentified	unidentified	unidentified	milind
4	unidentified	unidentified	milind	milind
5	milind	priyank	monica	priyank
6	unidentified	priyank	monica	milind
7	milind	milind	milind	milind
8	unidentified	unidentified	unidentified	priyank
9	milind	milind	monika	milind
10	unidentified	unidentified	monika	priyank

Table 5: Generated result table by using (Priyank signature)

priyank	energy	angle	chain code	mixed feature
1	unidentified	unidentified	sheela	ratnesh
2	unidentified	priyank	unidentified	priyank
3	unidentified	unidentified	unidentified	milind
4	unidentified	unidentified	unidentified	priyank
5	unidentified	priyank	monica	priyank
6	unidentified	priyank	monica	priyank
7	unidentified	unidentified	unidentified	priyank
8	unidentified	unidentified	unidentified	priyank
9	priyank	unidentified	monika	arvind
10	unidentified	unidentified	monika	priyank

In the above table signature of priyank is verified by with its own signature, with different parameter called energy, angel, chain code and mixed feature, result of each parameter is shown in above table. The accuracy of the mixed feature of priyank signature in table is 70% and this accuracy can be given by this formula:

$$\text{Accuracy} = \frac{\text{Current Identification of Signature}}{\text{Input Signature}}$$

The percentages of accuracy can vary from person to person according to the style of signature.

IV. Conclusion

The proposed mixed approach for signature verification based on Angle feature, Chain-Code and Energy Density feature extraction method, and gradient descent back propagation learning technique minimizes the mean square error and improves the accuracy. The proposed approach gives 70 to 80% accuracy with less forgery acceptance and less genuine rejection. If Angle feature, Chain-Code and Energy Density method used separately. The performance of proposed system reduces significantly when we using large signature database. If large number of people uses the online signature, verification system for signature verification the accuracy of
the proposed signature verification system reduces. The online signature verification system gives in depth review of handwritten signature recognition systems and special consideration is given to the analysis of Dynamic Signature Recognition Systems. The performance metrics of typical systems are compared along with their feature extraction mechanisms.

We have discussed an online Signature Recognition Systems based on energy, angle and direction feature set as well as mixed global features using artificial neural network. This is a multi-algorithmic system such systems combine the advantages of individual feature sets and improve the Recognition rates. The proposed method was successfully made the online signature verification with improve the efficiency and accuracy and easily can detect these killed forgeries.

V. Future Work

Only the local features were considered for verification and evaluated independently. Combining these features with global can improve the accuracy. Global features also can be extracted from the signatures obtained by using a signature pad. Combining the local features and global features can improve the accuracy. Interesting future work will be to incorporate a multimodal technique combining other biometric data acquired from webcams or combing the signature data obtained from signature pads placed at different positions. The selection of good learning technique is an important research topic in the study of any type signature recognition either online or offline. The proposed systems only reduce the unauthorized acceptance and improve the accuracy. The accuracy of the proposed system can further be improved by adding other techniques like velocity, pen pressure and time of contact between pads etc. on the signature verification system. Use of Innovative Data Acquisition Devices like Acceleration Sensor Pen that consists of two sensors integrated in a pen producing three signals. The acceleration sensor—accelerometer placed near the pen nib produces two signals corresponding to the horizontal and vertical movements of the pen.

VI. Acknowledgment

We are very thankful to the Prof. Namrata Tapaswi HOD and prof. Jayesh Gangrade (Computer Science & Engineering) IES, IPS Academy Indore for their constant support and Motivation.

VI. References

[1] A.V. D. Silva, D. S. D.Freitas, “Wavelet-based Compared to Function-based On-line Signature Verification”, IEEE, 2002, 1530-1834/02

[2] R. Sharma, M.Shrivastav, “An Offline Signature Verification System Using Neural Network Based on Angle Feature and Energy Density ”,International Journal on Emerging Technologies 2(2): 84-89(2011), 2011, ISSN No. (Online): 2249-3255

[3] M. Tomar, P. Singh, “A Directional Feature with Energy based Offline Signature Verification Network”, International Journal on Soft Computing (IJSC), 2011, Vol.2, No.1, 10.5121/ijsc.

[4] B. Li, K. Q. Wang, D. Zhang, “On-line Signature Verification for E-finance and E-commerce Security System ”, IEEE Proceedings of the Second International Conference on Machine Learning and Cybernetics, Wan, 2-5November 2003, 0-7803-7865-Z03

[5] D. Muramatsu, K. Yasuda, T. Matsumoto, “Biometric Person Authentication Method Using Camera-Based Online Signature Acquisition”, IEEE 10th International Conference on Document Analysis and Recognition, 2009, 978-0-7695-3725-2/09

[6] D.S. Guru, H.N. Prakash, “Online Signature Verification and Recognition An Approach Based on Symbolic Representation ”, IEEE transactions on pattern analysis and machine intelligence, June 2009, VOL. 31, NO. 6, 0162-8828

[7] D.S. Guru, H.N. Prakash, “Symbolic Representation of On-line Signatures”,IEEE International Conference on Computational Intelligence and Multimedia Applications, 2007, 0-7695-3050-8/07

[8] F. FA, F. J, G.A, G. J, O-G J. “Spain robustness of signature verification systems to imitators with increasing skills”.In: 10th international conference on document analysis and recognition, 2009.

[9] J.Guo, J.Zheng, B. Lu, “Research of Online Signature Recognition Based on Energy Feature”, IEEE Workshop on Power Electronics and Intelligent Transportation System, 2008, 978-0-7695-3342-1/08

[10] L. L. Lee, T.Berger,E. Aviczer, “Reliable On-Line Human Signature Verification System”, IEEE Transactions on pattern analysis and machine intelligence, June 1996, vol. 18, no. 6