A Study on Handwritten Signature

L B. Mahanta
Institute of Adv. Study in Science and Technology
Guwahati – 35, P.O- Gorchuk
Assam, India

Alpana Deka
Department of Statistics
Gauhati University
Guwahati-14, Assam, India

ABSTRACT
Handwritten signature verification is a behavioral biometric. Every day, we may face signature verification problem directly or indirectly whether it is in a banking transaction or signing a credit card transaction or authenticating a legal document. In order to solve this problem, during the last few decades, research has been going on with different approaches to introduce an efficient signature verification and identification system. This paper presents some basic concepts of signature and also explores on different approaches for verification.

General Terms
Pattern Recognition and Security.

Keywords
Biometric, Error Rate, Forgeries, offline signature verification.

INTRODUCTION
Handwritten Signature is a biometric measure. Biometric is the branch of science for identifying or verifying a person's identity and falls in the field of pattern recognition. Physical and behavioral characteristics of an individual are examined in the biometrics study. Physical characteristics include facial features, features of the eye (i.e. retina and iris), fingerprints, hand geometry. On the other hand, behavioral characteristics include handwritten signature, keystrokes or typing, voiceprint, gait, gesture [1]. Both verification and identification mode can be operated by a biometric system. In the verification mode, system database maintains a respective biometric template(s) for each person and then a person's identity is verified by comparing captured biometric data with the stored template which is a one-to-one comparison. The identification mode is a one-to-many comparison because the identification is performed by searching the templates of all the users in the database for a match [2]. The objective of the signature verification system is to distinguish the original from the forgery. Variations in signatures may arise in two ways which are related to intra and interpersonal variability. The variation among signatures of same person is called Intra Personal Variation. The variation between originals and forgeries is called Inter Personal Variation [3].

There are few key factors on which a signature depend [4]:

i) Physical and psychological state of the person – The shape and pattern of a signature may depend on factors of a person like illness, injuries, fears, heart rate, person's age, calmness, goodwill etc. These factors have influence to increase the fluctuation of shape of a signature. Experiments reveal that person's age is also an important factor. The nature of signature will vary with respect to young age, middle age and old age.

ii) Body position – While signing a document, body position may be one of the remarkable factors. The pressure applied with pen on paper will be different depending on whether a person is sitting or standing. It is important to notice whether a person's body is free from all perspectives or there is any burden on the signing hand.

iii) Writing surface and writing material (pen) – Signature will look different on papers of different quality. Since the way of handling a pen or pencil is different to some extent, hence writing material may impact on signature.

iv) Purpose of signing – signature is usually significantly different if taken in formal environment than in informal. Since in informal environment, a person does not have any mental pressure, therefore purpose of writing may be considered as a factor on which handwritten signature depend.

v) Environmental factors – environment and people that surround the signatory. This includes noise, luminance, temperature, humidity, etc.

2. PERFORMANCE EVALUATION
Since the main objective of signature verification system is to identify whether a given signature is genuine or not, therefore we need to measure the performance of the system. The efficiency of a signature verification and recognition system, is expressed in terms of two error rates: the Type I error rate and Type II error rate, which are also known as the False Reject Rate (FRR) and False Acceptance Rate (FAR), respectively. False reject rate or type I error is the percentage of genuine signatures that are incorrectly rejected by the system and false accept rate or type II error is the percentage of incorrectly accepted forgeries. Depending on the security requirements of the application, the two types of errors usually have different costs related with them. Equal Error Rate is the point where the false accept rate and the false reject rate are the same and the performance of a system is often measured by this. It has been proved that a more meaningful performance measure is the Error Tradeoff Curve (receiver operating characteristic curve), which shows how one error changes with respect to the other [5].

Performance evaluation is a vital measurement done on forgeries related with signature. Signature forgery means copying, altering or falsifying written matter for the purpose of defrauding others. Signature forgery is done for diverse applications like cashing a check, signing a credit card transaction or authenticating a legal document. Depending on the degree of similarity with the original signature forgery can be divided into three types: Random, Unskilled and Skilled forgery as shown (Figure 1) below [6].

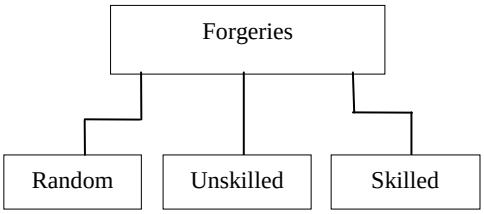


Fig 1: Types of Forgeries

1. Random Forgery: Here the term 'random' indicates that the signer writes the name of the owner in random style. He knows the name of the victim and produces the signature in his own style. This forgery is easily detected by visual analysis.

2. Unskilled Forgery: Without having any previous experience, the signer tries to copy the signature in his own style instead of the victim's signature style. By knowing the name of the signer but without having any knowledge of spelling of signer's signature, unskilled forgery is created.

3. Skilled Forgery: This type of forgery is produced by looking at the original signature or by having idea about the signature of the victim. Professional persons who have experience in copying the signature, performs this type of forgery to create a duplicate copy of the original signature. In skilled forgery, the signature is trying to copy in such a way that, in some of the cases, visual inspection may fail to identify whether a given signature is genuine or not. It has been observed that such forgeries are done by using very clever tricks, like copying from a signature stored in a mobile. The paper kept on top of the mobile shows a very clear impression of the signature below, due to the light source from the mobile.

On comparison, it is obvious that random and unskilled forgeries are easy to verify than the detection of skilled forgery since professional person is employed here to create duplicate copy of the original signature.

3. A COMPARATIVE STUDY ON FEATURES OF ONLINE AND OFFLINE SIGNATURE VERIFICATION

Depending on the data capturing method and captured characteristics, signature verification and recognition are of two kinds: online signature and offline signature verification. In online verification, a specialized hardware called stylus and digitizing tablet is used.

For online signature verification system, following features can be considered [7]:

i) Time: Total time taken to complete the signature.

ii) Distance: Total distance traveled by the pen while writing the signature.

iii) Pen-up: During signing process (including or excluding the final pen-up) total number of pen-ups is counted which is taken as an important feature. The time for which the pen was up is considered as the total pen-up time.

iv) Pressure: The number of times the pressure goes above an upper threshold and pressure falls below a lower threshold (thresholds can be a certain percentage of the peak value) are another dynamic features of an online signature verification system.

v) The number of zeros in the velocity in X and Y direction.

vi) The number of zero crossings in the acceleration in X and Y direction.

Since analysis is performed on the basis of dynamic features, hence, the online verification is also known as dynamic verification system.

In offline (static) signature verification, people write the signature on a paper and then it is collected with the help of a scanner or digital camera, therefore only static biometric characteristics can be extracted, which are as follows[8]:

i) Global Features: The term 'global' indicates that features are globally extracted from a signature image i.e. features are extracted by considering the input image as a whole. These features include transformations, series expansions, image gradient analysis etc. instead of local, geometrical, or topological properties of the signature. Global features can be easily extracted and insensitive to noise, they depend on the position alignment and highly sensitive to distortion and style variations.

(ii) Statistical Feature: From the distribution of pixels of a signature, features like statistics of high gray-level pixels are derived to identify pseudo-dynamic characteristics of signatures and are known as statistical features. This method includes the extraction of high pressure factors with respect to vertically segmented zones (for example, upper, middle and lower zones) and the ratio of signature width to short- or long-stroke height. Since statistical features take some topological and dynamic information into explanation it can consequently tolerate minor distortions and style variations in its methodology.

(iii) Geometrical and topological features: This features deals with global and local properties of a signature to describe the geometrical and topological characteristic of a signature. The degree of tolerance to distortion and style variations in geometrical and topological is higher than that of statistical feature. It can also tolerate a certain degree of translation and rotation variations.

Comparatively the off-line signature verification is more difficult than online one, since only static information of a signature image can be extracted, and all the dynamic information during the writing process disappears almost completely.

4. DIFFERENT SIGNATURE VERIFICATION APPROACHES

During the last few decades, it is observed that by employing various approaches, researchers have made great effort to find out an offline signature verification system which can detect genuine and forgery signature accurately.

4.1 Statistical approach

This approach is related with statistical concepts like mean, standard deviation, correlation coefficient, bayes theorem and used to measure the performance of a system.

P. Metri, A.Kaur [9] proposed a method on the basis of correlation coefficient. Here Instance Based Learning algorithm is used in order to take the advantage of small database storage. Features are extracted from different projection profiles like horizontal, vertical and diagonal projection. Features of all sample signatures are correlated for each person. From this correlation value, a mean value is obtained. Finally, deviation value verifies the signature.

H. Srinivasan, S.N. Srihari, M. J Beal [10] developed a signature verification system using Kolmogorov-Smirnov statistic. Here in the feature extraction stage, gradient, structural and concavity (or GSC) features are extracted. To determine the GSC features from a sample, a signature is segmented with 4*8 grids as shown in Figure 2. The probability of similarity is measured

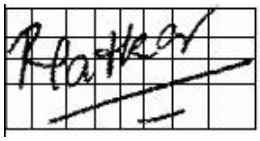


Fig 2: Grid segmentation with signature

by Kolmogorov-Smirnov test. From the experimental result, it is shown that the overall accuracy increases as the number of samples taking for learning increases.

D. Jena, B. Majhi, S.K. Jena [11] proposed a signature verification system based on geometric feature. Horizontal and vertical splitting are performed on the signature to retrieve sixty geometric centers. Classification is performed on statistical parameters like mean, variance and Euclidean distance. Experiment is done on all the three types of forgeries.

4.2 Fuzzy logic based approach

R.Zakaria, A.F.Wahab , J. M. Ali [12] proposed an approach for offline handwriting signature verification where confidence fuzzy interval by alpha-cut of triangular fuzzy number is used. In order to achieve defuzzification signature, defuzzification method was used. This offline handwriting signature is modeled by using fuzzy interpolation rational cubic Bezier curve. The confidence of fuzzy interval which comprises of left (lower bound) and right (upper bound) fuzzy signature are determined by the value alpha cut .Acceptance of signatures and value of standard error depend on range of the confidence fuzzy interval. For the value of alpha cut, confidence fuzzy number and standard error, they depend on the verification of the offline handwriting signature.

S.Maheswaran[13] implemented a fuzzy logic based signature verification and detection system on angular features.

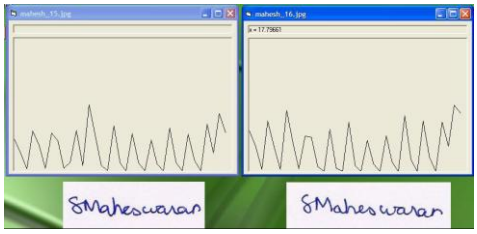


Fig 3: Extracted angle features for two samples of the same person's signature

Depending on various factors, signature of the same person can be varied as shown as Figure 3. Here, angular feature efficiently detects the difference between the two signatures of same person. A total of 60 features are collected from each signature. Here Takagi-Sugeno Fuzzy Modeling approach is applied.

M.Nasiri, S.Bayati and F.Safi[14] described a system based on fuzzy approach. Here, after extracting the boundaries and control points from the preprocessed signature, four local features on the control points are collected. To classify the signatures, zero-order Takagi-Sugeno Fuzzy Inference System is used.

4.3 Neural network approach

From the study of offline handwritten signature, it is found that Neural Network is the most extensively used approach for this verification.

S.Patil, S.Dewangan [15] presented a method for verifying handwritten signatures by using NN architecture. Other than the other features like horizontal length, maximum height, aspect ratio, number of pen-ups, they also considered Hu's Moment Invariant Feature. Here, Hu's moment invariant is analyzed on image scaling and rotation. The EER for skilled forgery is 25.1% and for random forgeries is 5.5% The main advantage of this method is that it reduces memory overhead and results in faster comparisons of the data to be verified.

I.A.B. Abdelghani, N.E. B. Amara [16] proposed a neural planner model for handwritten signature. Here geometric and textural Features are extracted. Each signature image is

Fig 4: Signature with Horizontal Segmentation

divided horizontally into three parts as shown in Figure 4. Each segmented signature band is characterized by the textural and geometric features. Here neural network approach is used.

K.Sisodia , S.M.Anand [17] evaluated the performance of an Error Back Propagation (EBP) Artificial Neural Network (ANN) for authentication. A verification rate is found to be 94.27% with database size 240. Here features are extracted on the basis of centroid, length and width of the signature, quadrant areas, global slant angle etc.

4.4 Wavelet-based approach

I.A.Ismail, M.A.Ramadan, T. S.El danaf, A.H.Samak [18] developed a novel off-line signature recognition method based on multi scale Fourier Descriptor and wavelet transform. Average error rate was found to reach 1%. They compared different distance measures (like Minkowski distance, Manhattan distance, Euclidean distance, Angle – based distance, Correlation coefficient- based distance etc.) between feature vectors with respect to the recognition performance. Recognition experiments were performed on 840 images.

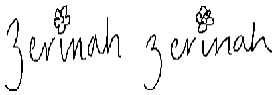
M.H.Sigari, M.R.Pourshahabi, H.R.Pourreza [19] designed new method for offline (static) handwritten signature identification and verification based on Gabor wavelet transform. Here, after pre-processing stage, Gabor wavelet is used to extract the features. For signature verification, Mahalonobis Distance is used. Experiment was performed on four signature dataset with different nationalities including Iranian, Turkish, South African and Spanish signatures. Since, the system is dealing with four different nationalities, so identification and verification of same system with more than one nationalities is one of the main advantage of this system.

4.5 Combination of approaches

Since most of the time, signature is found as a highly stylish, so it may be difficult to identify a signature with the help of

only one approach. To efficiently recognize the signature, we are required to combine two or more approaches.

A. McCabe, J.Trevathan [20] described a system for performing handwritten signature verification using complementary statistical models. Here static features of a signature like shape, slant, size are extracted. Dynamic features like velocity, pen-tip pressure and timing are also collected to efficiently judge the identity of a signer with both the features. The nature of a signature captured with stylus for extracting static features as well as without using stylus to capture dynamic features is shown (Figure 5) below.



(a) (b)

Fig 5: With and without stylus capturing signature

Here, both the approaches Neural Network and Hidden Markov Model are combined to increase the accuracy of the system performance rather than using any specific approach alone. The system performed reasonably well and achieved an overall error rate of 2.1% in the best case.

M.Mehta, R.Sanchati, A.Marchya [21] proposed a signature verification system. Here recognition is performed on a particular banking cheque fields like name, amount. Samples are collected at the same time. Two feature types namely Sum graph and HMM are combined for automatic cheque processing with detection of skilled forgery and classified them with knowledge based classifier and probability neural network.

4.6 Other Approaches

Apart from the above approaches, Clustering Technique, Support Vector Machine are other approaches.

S.Biswas, T.H.Kim, D.Bhattacharyya [7] used K-Nearest Neighbors' (KNN) as a clustering technique enabling to handle clusters of different sizes and shapes. Here the extracted features are signature height width ratio, signature occupancy ratio, distance ratio calculation at boundary, number of spatial symbol within a signature taken for

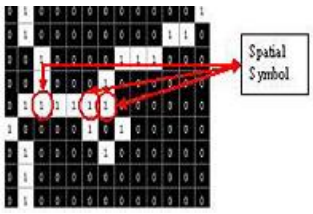


Fig 6: Number of spatial symbol

verifying the signature. Spatial symbol means pixels having more than two neighbors with value 1 as shown in Figure 6. From both the sample and test signatures, features are extracted. Then a decision will be made based on the clustering results between the computed feature of Sample signature image and Test Signature Image.

V. kiani, R. Pourreza, H.R. Pourezza [22] described a signature verification system with support vector machine. Experiments are done on two databases: English and Persian. To verify the signature, Randon Transform and Support Vector Machine are used as feature extractor and classifier respectively.

Table 1: Comparison of Different Approaches

Approach	Author	Data-base size	Features	Verification rate (%)
Statistical Approach	D. Jena et al.	-	Geometric Features	FAR-2.08 FRR-20.83 (AER-11.46)
Fuzzy Based Approach	M.Nasiri et al.	300	Geometric Features	FRR-10.3 FAR-8.105 (AER–9.2)
Neural Network Approach	K.Sisodia et al.	240	Global Features	FRR-7.2917 FAR-4.1667 (AER-5.8)
Wavelet-Based Approach	I.A.Ismail et al.	840	Discrete Wavelet Transform	AER-1
Combination of Approaches	A. McCabe	-	Static, Dynamic Features	OER-2.1 (AER) - 1
Other Approaches	Support Vector Machine	924	Local Features	FRR – 19 FAR – 2 (AER-10.5)

5. CONCLUSION

Here we have given some preliminary concept about signature analysis. A comparative study of offline and online signature is also discussed. Lastly we try to focus on some of the available approaches for offline signature verification. The efficiency of a signature verification system depends on each and every stage like preprocessing, feature extraction and selection of classifier. A well preprocessed image should be fed to the system in order to extract features. Features that are to be extracted depend on nature and pattern of signature. The same set of features may not be preferable to both simple as well as cursive letters, to attain an efficient result. Since among the three types of forgeries, detection of skilled forgery is a crucial task, hence selection of classifier(s) is also an important job. A signature may not be readable for all the time due to presence of flourishes. Since the pattern of a signature may vary from person to person from normal signature to cursive-ness, hence finally we can conclude that depending on the demand of the pattern of the signature, an efficient pattern recognition system can be implemented with suitable classifier(s) to recognize the signature.

The main objective of handwritten signature verification is nothing but to reduce the fraud cases. In most of the cases, verification is done by manually, say for example in banking sector, when we go to deposit or withdraw money, our identification is verified just by visual inspection of the written signature. Hence to increase the security, an automatic signature verification system can be applied.

REFERENCES

[1] D. Zhang, "Automated Biometrics: Technologies and systems", Kluwer Academic Publishers, 2000.

[2] A. K. Jain, Patrick lynn, A. A. Ross, "Handbook of biometrics", publication: Springer, 2008.

[3] B. Majhi, Y. S. Reddy, D. P. Babu, "Novel Features for Off-line Signature Verification", International Journal of

Computers, Communications & Control Vol. I(2006), No. 1, pp. 17- 24.

[4] T. Fotak, M. Bača, P. Koruga, "Handwritten Signature Identification using Basic Concepts of Graph Theory", Wseas Transactions on Signal Processing, Issue 4, Vol. 7, pp. 117-129, October 2011.

[5] A. K. Jain, F. D. Griess, S. D. Connell, "On-line signature verification", Pattern Recognition, The Journal of the Pattern Recognition Society, pp. 2963-2972, 2002.

[6] U. Dewan, J. Ashraf, "Offline signature verification using neural network", International Journal Of Computational Engineering & Management (IJCEM), Vol. 15, Issue 4, July 2012, pp: 50-54.

[7] S. Biswas, T.H. Kim, D. Bhattacharyya, "Features Extraction and Verification of Signature Image Using Clustering Technique", International Journal of Smart Home, Vol.4, No.3, July 2010.

[8] M.K. Kalera, S. Srihari, A. XU, "Offline Signature verification and identification using distance statistics", International Journal of Pattern Recognition and Artificial Intelligence, Vol. 18,No. 7, pp.1339-1360, 2004.

[9] P. Metri, A. Kaur, "Handwritten Signature Verification using Instance Based Learning", International Journal of Computer Trends and Technology- March to April Issue 2011, pp: 1-3.

[10] H. Srinivasan, S.N. Srihari, M. J Beal,"Signature verification using Kolmogorov – Smirnov statistic",January 9, 2005.

[11] D. Jena, B. Majhi, S.K. Jena,"Improved Offline Signature Verification System Using Feature Point Extraction Method",Journal of Computer Science 4(2), 2008, pp: 111-116.

[12] R. Zakaria, A. F. Wahab, J. M. Ali, "Confidence Fuzzy Interval in Verification of offline Handwriting Signature", European Journal of Scientific Research, Vol. 47, No.3 (2010), pp.455-463, EuroJournals Publishing, Inc.2010.

[13] S.Maheswaran, "Fuzzy Logic Based Off-line Signature Verification and Forgery Detection System".

[14] M.Nasiri, S.Bayati and F.Safi, "A fuzzy Approach for the Automatic Off-line Signature Verification Problem Based on Geometric Features", 2012.

[15] S. Patil, S. Dewangan, "Neural Network-based Offline Handwritten Signature Verification System using Hu's Moment Invariant Analysis", International Journal of Engineering and Advanced Technology (IJEAT), Vol.1, Issue 1, October 2011, pp:73-79.

[16] I.A.B. Abdelghani, N.E. B. Amara, "A Neural Planar Modeling for Handwritten Signature based on Automatic Segmentation", International Journal of Computer applications, Vol. 49,No. 8, 2012.

[17] K. Sisodia , S.M. Anand, "Off-line Handwritten Signature Verification using Artificial Neural Network Classifier", International Journal of Recent Trends in Engineering, Vol. 2, No. 2, November 2009, pp: 205-207.

[18] I.A. Ismail, M.A. Ramadan, T. S. El danaf, A.H. Samak, "Signature Recognition Using Multi Scale Fourier Descriptor And Wavelet Transform", International Journal of Computer Science and Information Security (IJCSIS), Vol.7, No.3, 2010,pp: 14-19.

[19] M.H. Sigari, M.R. Pourshahabi, H.R. Pourreza, "Offline Handwritten Signature Identification and Verification Using Multi-Resolution Gabor Wavelet", International Journal of Biometrics and Bioinformatics (IJBB),Vol. 5, Issue 4, 2011, pp: 234-248.

[20] A. McCabe, J.Trevathan, "Handwritten Signature Verification Using Complementary Statistical Models", Journal of Computers, Vol. 4, No. 7, July 2009, pp: 670-680.

[21] M. Mehta, R. Sanchati, A. Marchya, "Automatic Cheque Processing System", International Journal of Computer and Electrical Engineering, Vol. 2, No. 4, August, 2010, pp: 761-765.

[22] V. kiani, R. Pourreza, H.R. Pourezza, "Offline Signature Verification Using Local Random Transform and Support Vector Machines", International Journal of Image Processing (IJIP), Vol. 3, Issue 5, pp. 184-194.