A SURVEY ON AUTOMATIC SIGNATURE VERIFICATION TECHNIQUES

[1]Varun.P.Sarvade , [2]Supriya.P.Sarvade
[1]Assistant Professor , Department of Computer Science & Engineering
Biluru Gurubasava Mahaswamiji Institute of Technology Mudhol, District Bagalkot, Karnataka, India
[2]Department of Electronics & Communication Engineering , Basaveshwar Engineering College Bagalkot, Karnataka, India
E-mail: [1]varunpsarvade@gmail.com, [2]supriyasarvade@gmail.com

Abstract— Signature is one of the most important and widely accepted form of identity verification. It is largely used in bank checks, stamp paper documents, agreement documents, bonds etc. It is also one of the most easily forgeable biometric identity when compared to other biometric features like thumb impression, face recognition etc. Hence Signature verification is very much important to differentiate between original and forged. Several attempts are being made to automate the process of signature verification and this paper intends to provide comparison of these processes.

Keywords—Signature Recognition, forgery, FAR, FRR, neural network, HMM, Fuzzy model.

I. INTRODUCTION

The signature of an individual is a significant biometric aspect which can be used to validate his/her identity**.** Human signatures provide safe way of confirmation and authorization in most of the legal documents; hence the need for signature authentication system becomes an important factor. Even though many modern techniques such as thumb impression, face recognition etc. are available for authenticity of a person, the handwritten signature is still a widely accepted way of authentication. Signature verification problem is concerned with the purpose of checking whether the given signature belongs to the person as claimed. Manual method for signature validation is very difficult and tedious especially when large numbers of documents are to be authenticated. Several attempts are being made to automate the process of signature verification and this paper intends to provide comparison of these processes.

Automatic Signature verification processes are broadly classified as On-line and Off-line methods.

1. **On-line Signature Verification System** [1][2]: In this system signature is captured and analyzed in real time. Here dynamic properties of the signature like pen pressure, signature trajectory, velocity, acceleration, location, time stamping and other factors are taken into consideration for signature verification. Devices like Digital Pen/Stylus based Tablet/Device are used to capture signature in real time. This verification system is better than offline signature verification because forging an On-line signature is very difficult due its dynamic properties.

2. Off-line Signature Verification System [1][2]: In this system image of the signature is captured by scanning it from a piece of writing paper. This system is useful for the verification of signatures found on paper documents like

bank checks, Stamp papers, bonds etc. Here static properties of the signature like slant angle, centroid, size etc are taken into consideration for signature verification. In this method it is not possible to capture dynamic characteristics because of the non-repetitive nature. The variation in signatures is caused by factors like age, illness, geographic location, emotional state of the person etc. Hence the off-line signature recognition method is complex.

II. SOME COMMON TERMS USED IN SIGNATURE VERIFICATION

A. *Types of Forgeries[3][4]:*

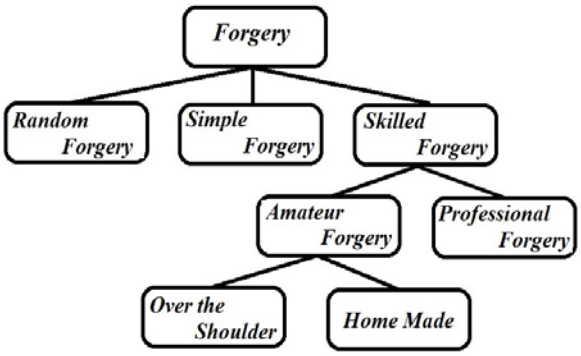

Figure 1.1 Classification of Forgery

As shown in Fig.1.1 forgeries can be classified into three main types:

1. **Random Forgery**: In such cases the forger doesn‘t know the writer‘s signature but comes up with his/her own. Here the forger may derive this from the writer‘s name. This forgery accounts for majority of forgery cases though it‘s easy to detect with naked eyes.
2. **Simple Forgery:** The forger imitates the signature in his own style by observing the signature closely for a while. Here the forger tries to imitate the signature without much practice.
3. **Skilled Forgery:** This type of forgery is possible only when the forger has unrestricted access to genuine signature. The skilled forgery category has been classified further as

i. **Amateur Forgery:** The amateur forgeries are again categorized as home improved and over the shoulder forgeries. In home improved the forger has a paper copy of the signature and has sufficient time to practice at home and over the shoulder forgeries are produced when immediately the forger has witnessed the writer make a genuine signature.

ii. **Professional Forgery:** A professional forgery is done by a person with professional expertise in handwriting analysis and is able to come up with high quality forgeries which are very difficult to detect.

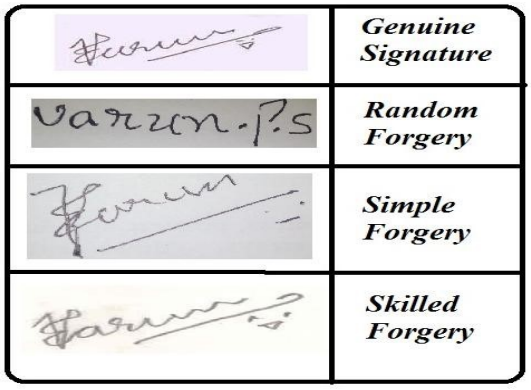

Figure 1.2 Sample Signature Forgery

B. *Measure of Error*

Any signature verification systems accuracy is measured based on the following parameters [1] [6]:

1. **False Rejection Rate (FRR):** It is the measure of genuine signatures rejected as forged and is usually expressed in percentage. It is also known as Type-I error.

$$FRR = \frac{\text{No. of Original Signatures Rejected}}{\text{No. of Signatures Tested}} * 100$$

2. **False Acceptance Rate (FAR):** It is the measure of forged signatures accepted as genuine and is usually expressed in percentage. It is also known as Type-II error.

$$FAR = \frac{\text{No. of Forged Signatures Accepted}}{\text{No. of Signatures Tested}} * 100$$

III. GENERAL STEPS IN OFF-LINE SIGNATURE VERIFICATION

An Off-line signature verification system consists of the following steps:

1. Signature Acquisition
2. Pre-processing
3. Feature Extraction
4. Verification

Figure 3.1 shows the general steps involved in a off-line signature verification system [7].

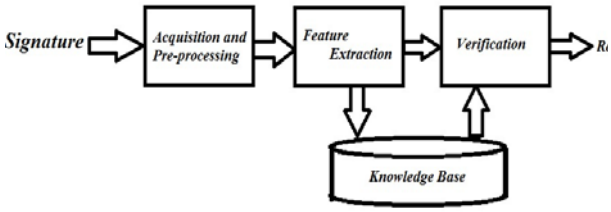

Figure3.1 : Steps in Signature Verification System

1. Signature Acquisition: *In this step the signature on the document is scanned using a scanner to obtain a digital image of the signature.*

2.Pre-processing[1][8]: In this stage operations like Resizing, Gray Conversion, Background elimination, Noise reduction, Edge enhancement, Binarization are performed on each signature. In Gray Conversion colour image is converted into black and white image. The purpose of edge enhancement is to highlight the detail in an image or to restore, at least partially, detail that has been blurred (either in error or as a consequence of a particular method of image acquisition). Binarization converts a gray scale image to a binary image i.e., value ‗1' for white and value ‗0' for black is assigned, which can be easily processed.

3. Feature Extraction [1][9]: In this stage we extract some features of signature image. Here different algorithms can be used to extract these features which will be used as input for training and verification. The features can be classified as global, local and transition features. Global features like width, height, aspect ratio are obtained from entire signature image. Local features are obtained from specific parts of the signature image. Transition features are obtained by counting the transition black to white pixel or vice versa in the binary signature image. The set of features are selected for verification based on the requirement of the application. 4. **Verification:** The features of the test siganature extracted in the previous step are compared with those already present in the database. If the features match then the test signature is genuine or else forged.

IV.METHODS OF OFFLINE SIGNATURE VERIFICATION

Madasu Hanmandlua, Mohd. Hafizuddin Mohd.Yusofb,Vamsi Krishna Madasuc [3] have proposed a system based on fuzzy modeling. This fuzzy modeling employs the Takagi–Sugeno (TS) model. Here the input signature image is divided into eight sections and each section is resized. Then in each section angle and distance features are extracted. These extracted features are provided to the TS Model for forgery detection. For a TS model with consequent coefficients fixed the FRR is 37.5% and FAR(for Skilled Forgery) is 34% and for a TS model with adapted consequent coefficients the FRR is 46.5% and FAR(for Skilled Forgery) is 42%.

Sayantan Roy, Sushila Maheshkar[10] have proposed a system using Grid based and centroid based approach. In grid based approach the pre-processed image is divided into 240 cells with each cell containing 100 pixels. Then information related to signature is extracted and stored in an array and using Column Matching Score signature verification is done. In case of Centroid based approach the pre-processed signature image is divided into three sections and centroid of each section is calculated. After finding these centroids they are connected to each other. Then the area enclosed by these centroids connecting lines is calculated. Then the ratio between this area and the bounding box area is calculated. The FAR (for skilled forgery) is 20%.

Prashanth C. R. and K. B. Raja [12] have proposed a system based on Angular features. In this system the angular features from pre-processed signature are extracted in two phases. The angular features are compared with a threshold for comparison between database and test signatures. The number of differences greater than the threshold is counted and if the number is greater than 133 out of 168, then test signature is considered as genuine signature or else forged. For this method the FAR is 4.995% and FRR is 8.5%.

M.K. Kalera. S. Srihari and Aihua Xu [13] proposed a system based on distance statistics. This system uses a combination of Gradient, Structural and Concavity (GSC) features at the local, intermediate and large scales for object recognition. These features capture the global, statistical and geometrical features of the signature. In the identification model, a binary feature vector is associated with each signature sample and then the proximity of a sample to all other samples is calculated using the similarity measure, whereas, in the verification model, a real-valued distance vector (where each component represents the distance between two signature samples) is used to describe the difference between a pair of signature samples. The weighted Euclidean distance measure

(weighted by the standard deviations of features) is used to measure the distance between any two distance vectors. This system has achieved accuracy as high as 78.1% for verification and 93.18% for identification on a pure offline database using GSC word features. For set 1, the FAR is 34.91% while the FRR is 28.33%. The average error rate of the system is 31.62%. For set 2, the FAR is 33.8% while the FRR is 30.93%. The average error rate of the system is 32.37%.

Hetal V. Davda, Sima K. Gonsai [14] have proposed a system based on Energy on Grid Level. In this proposed feature extraction method we derived features from the total energy a writer uses to create their signature. It is hypothesized that the planned execution of the signature uses the same amount of energy whereas original writer uses different energy for signatures. In the identification mode, the system recognizes an individual by comparing the extracted features with those stored in the database. Here the Euclidean distance gives moderate FAR and FRR values and time taken for calculation also more compare to Cityblock distance. Hellinger distance gives good FRR and FAR values and time taken for calculation is more compared to all distances. Whereas Cityblock and Squareeuclidean give good FAR and FRR values for energy features and both have low calculation time. Cityblock is good for energy features.

E. Justino, E. Bortolozzi, R Saburin [15] have proposed an off-line signature verification system based on Hidden Markov Models (HMMs) to detect random, casual, and skilled forgeries. Three features: a pixel density feature, a pixel distribution feature and an axial slant feature are extracted from a grid segmentation scheme. The FAR of 2.83% is obtained and a FRR of 1.44%, 2.50%, and 22.67% are obtained for random, casual, and skilled forgeries, respectively.

Ashwini Pansare, Shalini Bhatia [16] proposed a model in which neural network classifier is used for verification. The geometric features are extracted from pre-processed signature image. These extracted features are then used to train a neural network. In verification stage, on test signatures preprocessing and feature extraction is performed. These extracted features are then applied as input to a trained neural network which will classify it as a genuine or forged signature. The neural network when presented with 150 genuine signatures from 30 different persons classified 125 signatures out of 150 as genuine and 25 signatures as forgeries. Thus FRR of the system is 16.7% .When 150 forged signatures were given as input to neural network, it classified 18 signatures as genuine and 132 as forgeries. Thus FAR of the system is 12%.

N.P.Narayan, Dr.S.V.Bonde, Dr.D.D.Doye [17] have proposed a system using shape dissimilarities. Here novel approach for verification of signatures based on curve matching using shape descriptor and Euclidian distance is used. In this approach ,the measurement of similarities are proceeded by finding correspondences between signatures, attaching shape descriptor (shape context) with Euclidian distance between the sample points of one signature and the sample point of other signature for better results, estimate aligning transforms by using this correspondences between signatures, classify the signatures using linear discriminant analysis and measures of shape dissimilarity between signatures based on shape context distance ,bending energy , registration residual, anisotropic scaling. FRR for genuine signature is 0.1011 and FAR for skilled forgery is 0.0421 and for random forgeries 0.0867.

V. PERFORMANCE EVALUATION OF VARIOUS APPROACHES

Sl no.	Methodology	FAR	FRR
1	Fuzzy Modeling [3]	34%	37.5%
2	Grid and centroid based approach [10]	20%	19%
3	Angular features [12]	4.995%	8.5%
4	distance statistics [13]	34.91%	28.33%
5	Hidden Markov Models (HMMs) [15]	2.83	1.44(random) 2.50(casual)

			22.67(skilled)
6	Geometric features [16]	12%	16.7%
7	Shape dissimilarities [17]	0.0421 (skilled) 0.0867 (random)	0.1011
8	Geometric features using Neural network [22]	14.66 %	20%
9	Novel feature extraction [23]	1	0.5
10	Support Vector Machine [25]	0.11	0.02
11	Dynamic Time Warping (DTW) [26]	20%	25%
12	Wavelet-based verification [27]	10.98%	5.60 %
13	Back-propagation Neural Network Prototype [28]	10%	6%
14	Signature Envelope and Adaptive Density Partitioning[29]	5.3%	4%

VI. CONCLUSION

This paper presents a brief survey on automatic signature verification techniques. An attempt is made to analyze various methods for signature verification like neural network, fuzzy model, HMM, DTW etc. Here various methods are compared along with their FAR and FRR. Each signature verification technique has its own advantages and disadvantages, based on selected set of features optimum results are obtained.

References

[1] *M.R. Deore, S.M. Handore,* ―A Survey on Offline Signature Recognition and Verification Schemes,‖ International Conference on Industrial Instrumentation and Control, IEEE**,** pp. 165-169, May 2015.

[2] *U.A. Jain,N.N. Patil,* ―A Comparative Study of Various Methods for Offline Signature Verification,‖ Internationai Conference on Issues and Challenges in Intelligent Computing Techniques, IEEE**,** pp. 760-764, 2014.

[3] *Madasu Hanmandlua, Mohd. Hafizuddin Mohd.Yusofb,Vamsi Krishna Madasuc,* ―Off-line signature verification and forgery detection using fuzzy modeling,‖ The Journal of Pattern Recognition Society,Elsevier**,** pp. 341 – 356, 2005.

[4] *S. Garhawal, N. Shukla,* ―A Study on Handwritten Signature Verification Approaches,‖ International Journal of Advanced Research in Computer Engineering & Technology, *Volume 2, Issue 8,* pp. 24972503, *August 2013*.

[5] *Yogesh V.G., Abhijit Patil,* ―Offline and Online signature Verification Systems: A Survey,‖ International Journal of Research in Engineering and Technology, *Volume 3,* pp. 328-332, *May* 2014.

[6] *Pooja, Ranjan Goyal,* ―Offline Signature Verification System – A Review‖ International Journal of Computer Application and Engineering Technology, Volume 3, Issue 2, pp. 188-192, Apr 2014.

[7] D. Impedovo and G. Pirlo, "Automatic Signature Verification: The State of the Art", IEEE transactions on systems, man, and cybernetics, vol.38, pp. 609-635,2008

[8] *Sameera Khan, Avinash Dhole,* ―A Review on Offline Signature lRecognition and Verification Techniques‖, International Journal of Advanced Research in Computer and Communication Engineering, Vol.3, Issue 6,pp.6879-6882 June 2014

[9] *Madhuri Yadav, Alok Kumar, Tushar Patnaik, Bhupendra Kumar,* ―A Survey on Offline Signature Verification‖, International Journal of Engineering and Innovative Technology, Volume 2, Issue 7,pp. 337-340 January 2013

[10] *Sayantan Roy, Sushila Maheshkar,* ―Offline Signature Verification using Grid based and Centroid based Approach‖, International Journal of Computer Applications Volume 86 – No 8,pp.35-39, Jan 2014.

[11] *G.S. Eskander, R. Sabourin, E. Granger,* ―A bio-cryptographic system based on offline signature images‖, Information Sciences, Elsevier pp.170 –191,2014.

[12] *Prashanth C. R. and K. B. Raja,* ―Off-line Signature Verification Based on Angular Features‖, International Journal of Modeling and Optimization, Volume 2, No. 4,pp.477-481 August 2012.

[13] *M.K. Kalera. S. Srihari and Aihua Xu,* ―Off-line Signature Verification and Identification using Distance Statistics‖, International Journal of Pattern Recognition and Artificial Intelligence, World Scientific, Vol. 18, No. 7, pp. 1339-1360, 2004

[14] *Hetal V. Davda, Sima K. Gonsai,* ―Offline Signature Verification System Using Energy on Grid Level‖, International Journal of Engineering Research, Volume No.3, Issue No.2, pp : 104-107, Feb. 2014

[15] *E. Justino, E. Bortolozzi, R Saburin*, ― Off-line Signature Verification Using HMM for Random, Simple and Skilled Forgeries,‖ ICDAR, vol.1, pp. 105-110,2001.

[16] *Ashwini Pansare, Shalini Bhatia,* ―Off-line Signature Verification Using Neural Network‖, International Journal of Scientific & Engineering Research, Volume 3, Issue 2, pp. 1-5, Feb-2012.

[17] *N.P.Narayan, Dr.S.V.Bonde, Dr.D.D.Doye,*―Offline Signature Verification Using Shape Dissimilarities‖, International Conference on Communication, Information & Computing Technology, IEEE, pp. 1-6, 2015.

[18] *Srikanta Pal,Michael Blumenstein,Umapada Pal,*― Off-Line Signature Verification Systems: A Survey‖, International Conference and workshop on Emerging Trends in Technology, 2011.

[19] *V A Bharadi, H B Kekre,*― Off-Line Signature Recognition Systems‖, International Journal of Computer Applications, Volume 1 – No. 27 pp.48-56,2010.

[20] *Meenakshi S Arya, Vandana S Inamdar,*― A Preliminary Study on Various Off-line Hand Written Signature Verification Approaches‖, International Journal of Computer Applications, Volume 1 – No. 9 pp.55-60,2010.

[21] *Yogesh V.G., Abhijit Patil,*― Offline and Online Signature Verification Systems: A Survey‖, International Journal of Research in Engineering and Technology, Volume: 03 Issue: 03 pp.328-332,May2014.

[22] *Ashwini Pansare, Shalini Bhatia* ,―Handwritten Signature Verification using Neural network‖, International Journal of Applied Information Systems (IJAIS), Volume 1– No.2 pp.44-49, January 2012.

[23] *Daramola Samuel, and Prof. Ibiyemi Samuel*, ―Novel feature extraction technique for off-line signature verification system,*"* International Journal of Engineering Science and Technology, vol. ED- 2(7), pp. 3137-3143, 2010.

[24] *G. Rigoli, A. Kosmala*, ―A Systematic Comparison Between on-line and off-line Methods for Signature Verification with Hidden Markov Models,‖ 14th International Conference on Pattern Recognition - vol. II, pp.1755—1757, Australia, 1998.

[25] *Özgündüz E, Şentürk T, and M. Karslıgil E.* ―Offline Signature Verification and Recognition by Support Vector Machine,‖ Eusipco, pp. 113-116, September 2005.

[26] *A. Piyush Shanker, A.N. Rajagopalan,*― Off-line signature verification using DTW‖, Pattern Recognition Letters, Elsevier, pp. 1407–1414, 2007.

[27] *P. Deng, H. Yuan Mark Liao & H. Tyan*, ―Wavelet Based Off-line Signature Recognition System‖, Proceedings 5th Conference on Optical Character Recognition and Document Analysis, 1996, Beijing, China.

[28] *R.Abbas*, ―Back propagation Neural Network Prototype for off line signature verification‖, thesis Submitted to RMIT, 2003

[29] *Malekian, V., Aghaei, A., Rezaeian, M., Alian, M.* "Rapid Off-line Signature Verification Based on Signature Envelope and Adaptive Density Partitioning", IEEE, 2013.