Comparative Analysis of Off-line Signature Recognition

Ankit Arora[1], Aakanksha S. Choubey[2]

[1]M.E (CTA) Scholar, CSE Department, SSGI, Bhilai, India

[2]Senior Assistant. Professor, CSE Department, SSGI, Bhilai, India

Abstract: ***Biometrics (or biometric authentication) assigns to the confirmation of humans by their biological features.*** *In* ***Computer science,*** *biometrics* ***is used as an aspect of determination*** *and access control****. Signature is one of the most widely used biometric systems for authentication of person as well as document. Online and offline signature is existing in person identification and authentication problems. Offline signature categorizes the signature into two classes: genuine and forged. In this paper, we discuss various features of offline signature recognition and verification process. We review and compare existing techniques, their results and methods of feature extraction.***

Keywords: Offline signature, feature extraction, recognition, biometrics, neural network.

1. Introduction

Biometric determination, or biometrics, accredits to the automatic recognition of a person based on his/her anatomical (e.g., fingerprint, iris) or behavioral (e.g., signature) properties or traits. Biometric confirmation awards numerous improvements over conventional approaches. A biometric system is a pattern recognition system which determines a user by assuring the legitimacy of a specific feature or behavioral characteristic possessed by the user. Numerous significant consequences must be considered in designing a realistic biometric system. First, a user necessity is registered in the system so that his biometric feature can be acquired into the system. This template is steadily stored in a vital record or a smart card issued to the user. The template is employed for comparing when an individual desires to be recognized. Depending on the situation, a biometric system can operate either in verification (authentication) or an identification mode [1]. Signature of a person is an important biometric trait of a human being and is used for confirmation for decades. Signature recognition is the process of writer's verifying by sample signature that is compared with the database records.

Signatures are composed of special character therefore usually they are not readable. The objective of signature recognition is to recognize the writer [2] [3]. The field of automatic signature verification and recognition are subdivided into two classes, online signature and offline signature. Offline signature recognition systems are more difficult than online recognition systems because the information like duration, flow, velocity is lost, in case of offline signatures. But, offline systems have a special advantage that they do not require access to special processing device like signature pad, digital tablet, etc.

In online approach we acquire more information about the signature which includes dynamic properties like duration, flow of pen-tip, velocity, pressure points, acceleration. The system performance improves because the dynamic features are difficult to imitate [4].

In off-line signature recognition, we have a template images which were acquired by optical scanner, hence we have only static characteristics of the signatures. The presence of person is not required at the time of verification. Thus offline signature is convenient in various places like document verification, banking transaction, etc [5] [6]

2. Offline Signature Recognition Approaches

A lot of research has been done in off-line signature recognition and verification. Kaewkongka T and his colleague used Hough transform as a basic approach for this task. They applied Hough transform to detect stroke lines from the signature image. The Hough transform is used to extract the parameterized Hough space from the thinning signature as unique feature of signature. They applied the straight line Hough transforms to signature image to map Cartesian coordinates into polar coordinates of radius and angle. The unique feature is extracted by finding the vote's value in the accumulator from the Hough space. The BPNN is used in the last stage to classify the tested signatures. They achieved the recognition rate 95.24% [7].

Bharadi and Kekre proposed global as well as grouping based features, for determining information in pixel of the signature. They use Walsh transform to the horizontal pixel distribution and vertical pixel distribution [8], this transform is fast to calculate. They achieved FAR of 2.5%, EER of 3.29%, with accuracy of 95.08%.

Bansal, Gard, and Gupta [9] proposed a contour matching algorithm, which is used to track the basic pattern in a sample signature and verify it. A contour can be best described as the outline of the signature. They use vector quantization method to extract critical point and then apply the matching algorithm. FAR was found to be 0.08% in case of random forgery and 13.02% in case of simple and skilled forgery.

Karki, Indira and selvi [10] used a Back Propagation Neural Network as the basic scheme in the signature recognition and verification. They consider the global features and grid information features as the unique characteristics. For global

feature they divide the information into two different level and for grid information features, they segmented the image into 96 rectangular regions. A FRR of less than 0.1 and FAR of 0.2 were achieved in this system.

Gady Agam in 2007 propose another scheme of offline signature recognition which is warping based. They present a new approach for reducing the variation in signature based on curve warping. The input signature image is pre-processed in first stage to convert the signature into curves. The resulting curves are then warped and compared using a derived metric to determine their similarity. The conversion of signature into curve has done using curve normalization, structural graph representation. In this scheme, a particle system is formed by insetting particles at curve vertices. An attraction force field is induced by the target curve, thus forming extrinsic warping constraints [11].

Daramola and Ibiyemi used a Hidden Markov Model for offline signature recognition. The technique is based on Discrete Cosine transform and Hidden Markov Model. In the feature extraction phase signature images are segmented into equal number of HMM states despite the length of the signatures. The application of DCT features coupled with well defined HMM topology framework contributed greatly to the generation of robust signature models.

Prasad and Amaresh proposed a system based on the Euclidean distance, Euclidean distance between the claimed signature and the template is proposed. The performance of the system is measured in terms of the False Rejection Rate (FRR), for the original signature - 8.57% and the False Acceptance Rate (FAR), for forged signatures - 13.33% [12].

The Support Vector Machine (SVM) method is used to verify and classify the signatures of different persons in [13], with a classification ratio of 0.95. The features used to describe the signatures are of three types: global, directional and grid features, making a total set of 77 features. As the recognition of signatures represents a multiclass problem, SVM's one-against-all method is used.

Sabourin [14] use granulo-metric size distributions for the definition of local shape descriptors in an attempt to characterize the amount of signal activity exciting each retina on the focus of a superimposed grid. He then used a nearest neighbor and threshold-based classifier to detect random forgeries. A total error rate of 0.02% and 1.0% was reported for the respective classifiers.

Fang [15] developed a system that is based on the assumption that the cursive segments of forged signatures are generally less smooth than that of genuine ones. Two approaches are proposed to extract the smoothness feature: a crossing method and a fractal dimension method. The smoothness feature is then combined with global shape features. Verification is based on a minimum distance classifier. An iterative leave-one-out method is used for training and for testing genuine test signatures. A database with 55 writers is used with 24 training signatures and 24 skilled forgeries per writer. A AER of 17.3% is obtained.

Zhang have proposed a Kernel Principle Component Self-regression (KPCSR) model for off-line signature verification and recognition problems. Developed from the Kernel Principle Component Regression (KPCR), the self-regression model selected a subset of the principle components from the kernel space for the input variables to characterize accurately each person's signature, thus offering good verification and recognition performance. The model directly worked on bitmap images in the preliminary experiments, showing satisfactory performance. A modular scheme with subject-specific KPCSR structure proved to be very efficient, from which each person was assigned an independent KPCSR model for coding the corresponding visual information. He reported FRR 92% and FAR .5% [16].

Baltzakis [17] developed a neural network-based system for the detection of random forgeries. The system uses global features, grid features (pixel densities), and texture features (co occurrence matrices) to represent each signature. For each one of these feature sets, a special two-stage perceptron one-class-one-network (OCON) classification structure is built. In the first stage, the classifier combines the decision results of the neural networks and the Euclidean distance obtained using the three feature sets. The results of the first stage classifier feed a second-stage radial basis function (RBF) neural network structure, which makes the final decision. A database is used which contains the signatures of 115 writers, with among 15 and 20 genuine signatures per writer. An average FRR and FAR of 3%and 9.8%, respectively is obtained.

In [18] Armand, Blumenstein and Muthukkumarasamy used combination of the Modified Direction Feature (MDF) in conjunction with additional distinguishing features to train and test two Neural Network-based classifiers. A Resilient Back Propagation neural network and a Radial Basis Function neural network were compared. Using a publicly available database of 2106 signatures containing 936 genuine and 1170 forgeries, they obtained a verification rate of 91.12%.

Justino [19] used a discrete observation HMM to detect random, casual, and skilled forgeries. A grid segmentation scheme was used to extract three features: a pixel density feature, a pixel distribution feature (extended-shadow-code), and an axial slant feature. A cross-validation procedure was used to define dynamically the best number of states for each model (writer). Two data set are used. The first data set contains the signatures of 40 writers with 40 genuine signatures per writer. This data set was used to determine the best codebook size for detecting random forgeries. This optimized system was then used to detect random, casual, and skilled forgeries in a second data set. The second data set contains the signatures of 60 writers with 40 training signatures, 10 genuine test signatures, 10 casual forgeries, and 10 skilled forgeries per writer. A FRR of 2.83%and an FAR of 1.44%, 2.50%, and 22.67% are reported for random, casual, and skilled forgeries, respectively.

Ferrer, Alonso, and Travieso [20], used Offline Geometric Parameters for Automatic Signature Verification Using Fixed-Point Arithmetic. They used set of geometric signature features for offline automatic signature

verification based on the description of the signature envelopes and the interior stroke distribution in polar and Cartesian coordinates. FRR reported was 2.12% and FAR was 3.13%.

Deng [21] developed a system that used a closed contour tracing algorithm to represent the edges of each signature with several closed contours. The curvature data of the traced closed contours were decomposed into multi-resolution signals using wavelets transforms. The zero crossings corresponding with the curvature data were extracted as features for matching. When only the skilled forgeries are considered, AERs of 13.4% and 9.8% are reported for the respective data sets. When only the casual forgeries are considered, AERs of 2.8% and 3.0% are reported.

Table 1: Performance comparison of offline signature recognition system

S. No	*Approach*	*FAR*	*Accuracy*
1	Parameterized Hough Transform [7]		95.24%
2	Signature recognition using clustering technique [8]	2.5%	95.08%
3	Contour based approach [9]	0.08%	-
4	Euclidian distance based approach [12]	13.33%	-
5	Support Vector Machine based approach [13]	-	95.0%
6	Exterior Contours and Shape Features [22]	06.90%	93.80%
7	Back-PropagationNeural Network Prototype [23]	10.00%	-
8	Geometric Centres [24]	09.00%	-
9	Hidden Markov Model and Cross-Validation [19]	11.70%	-
10	Smoothness Index Based Approach [25]	3.13%	79.00%
11	Geometric based on Fixed-Point Arithmetic [20]	4.90%	-
12	Wavelet–based Verification [21]	10.98%	-
13	Virtual Support Vector Machine [26]	13.00%	
14	Genetic Algorithm [27]	01.80%	86.00%

3. Steps in Signature Recognition

In signature recognition system, there is a need to pre-process the data. The chief ladders are as follows

3.1 Data Acquisition

The signature to be processed by the system should be in proper digital image format. We need to scan the signature through optical scanner from the document for the verification purpose.

3.2 Pre-processing

Image capturing devices causes the need to normalize an input image of signature (so called: pre-processing). This stage is farther sub-divided into following stages [2]:– Normalization, – Image Binarization, – Data Area Cropping, – Thinning.

3.2.1 Normalization:

Before any further processing takes place; a noise reduction filter is applied to the binary scanned image. The aim is to eradicate single white pixels on black back ground and single black pixels on white background. In order to accomplish this, we apply a 3 X 3 mask to the image with a simple decision, basic principle is this if the number of the 8 neighbours of a pixel that have the same colour with the central pixel is less than two, and then reverse the colour of the central pixel. Figure 1 and Figure 2 shows this stage.

Figure 1: Original Image

Figure 2: Normalized Image

3.2.2 Image Binarization: It allows us to reduce the amount of image information (removing colour and background), so the output image is black-white. The black-white type of the image is much more easily to further processing

Figure 3: Binarized Image

3.2.3 Data Area Cropping: The signature area is alienated from the background by using the well known segmentation methods of vertical and horizontal projection. Thus, the white space surrounding the signature is discarded [28]. Morphological operation Erosion and Dilation applied to perform this step.

Figure 4: Erodated and Dilated Image

3.2.4 Thinning: Size of the image is abridged. In this procedure unnecessary signature areas are removed [29].

Step 1: Mark all the points of the signatures that are candidates for removing (black pixels that have at least one white 8-neighbor and at least two black 8-neighbors pixels).

Step 2: Examine one by one all them, following the contour lines of the signature image, and remove these as their removal will not cause a break in the resulting pattern.

Step 3: If at least one point was deleted go again to Step 1 and repeat the process once more.

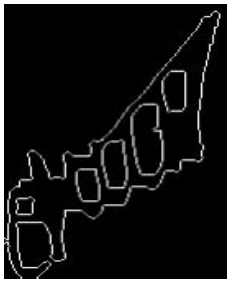

Figure 5: Edge detected image

4. Feature Extraction for Offline Signature

During this step a gathering of characteristic data take place. The output result is a set of the unique information about the signature. The choice of a powerful set of features is crucial in optical recognition systems. The features used must be suitable for the application and for the applied classifier. Global features provide information about specific cases concerning the structure of the signature, grid information and texture features are intended to provide overall signature appearance information in two different levels of detail. For grid information features, the image is segmented in 96 rectangular regions. Only the area (the number of signature points) in each region is used to form the grid information feature group. For the texture feature group to be formed, a coarser segmentation scheme is adopted. The signature image is segmented in only six rectangular areas, while, for each area, information about the transition of black and white pixels in the four deferent directions are used.

a) Image area: The number of black (foreground) pixels in the image. In skeletonised signature images, it represents a measure of the density of the signature traces.
b) Vertical centre of the signature: The vertical centre Cy
c) Horizontal centre of the signature: The horizontal centre Cx
d) D. Maximum vertical projection: The vertical projection of the skeletonised signature image is calculated. The highest value of the projection histogram is taken as the maximum vertical projection.
e) Maximum horizontal projection: As above, the horizontal projection histogram is calculated and the highest value of it is considered as the maximum horizontal projection.
f) Vertical projection peeks: The number of the local maxima of the vertical projection histogram.
g) Horizontal projection peeks: The number of the local maxima of the horizontal projection histogram.
h) Number of edge points: An edge point is a signature point that has only one 8-neighbor.
i) Number of cross points: Cross point is a signature point that has at least three 8-neighbors.

5. Performance Measure

The performance of the system depends on how precisely the system can classifies the genuine and forged signatures [9]. The forgery involved in offline signature verification is classified into three types:

5.1 Random forgery

The signer uses the name of the victim in his own style to create a forgery known as the simple forgery or random forgery. This forgery accounts for most of the forgery cases although they are very easy to detect even by the naked eye.

5.2 Unskilled forgery

The signer imitates the signature in his own style without any knowledge of the spelling and does not have any prior experience. The imitation is preceded by observing the signature closely for a while.

5.3 Skilled forgery

Undoubtedly the most difficult of all forgeries are created by professional impostors or persons who have experience in copying the signature. For achieving this one could either trace or imitate the signature by hard way. Signature recognition and verification system is designed for detecting these levels of forgeries. The main metrics for performance measure of these systems are:

1. False Acceptance Ratio (FAR)
2. False Rejection Ratio (FRR)
3. Equal Error Rate (EER)

6. Conclusion and Future Work

This paper gives the depth review of available approaches of offline signature recognition. The performance metrics of available schemes are compared and we found that between all the available methods offline signature recognition system which is based on parameterized Hough transform is giving the best result and accuracy. The major contribution of this work is to give the detailed description about offline signature recognition and verification methodology currently adapted. Apart from this review we can explore more details about handwriting analysis, as the signature is considered as a small part of handwriting so the approaches discussed above can be best used in this way.

References

[1] An overview of biometric recognition. Available: http://biometrics.cse.msu.edu/info.html.
[2] M. Radmehr, S.M.Anisheh, M.Nikpour, A.Yaseri, “Designing an offline method for signature recognition”, world Applied Science Journal 13 (3): 438-443, 2011.
[3] E.Ozgunduz, T.Senturk, M.E.Karshgil, “Offline signature verification and recognition by support vector machine”, in Proc. EUSICPO, 2005,
[4] R.Plamondon, “The design of an on-line signature verification system”, Theory to practice, International journal of Pattern recognition and Artificial Intelligence,

(1994)795-811.
[5] H.B.kekre, V.A.Bharadi, "Specialized global features for off-line signature recognition", 7th Annual National Conference on Biometrics RFID and Emerging Technologies for Automatic Identification, VPM Polytechnic, Thane, January 2009.
[6] H.B.Kekre, V.A.Bharadi, "Signature recognition using cluster based global features", IEEE International Conference (IACC 2009), Thapar University, Patiala-Punjab, India. March 2009.
[7] T. Kaewkongka, K. Chamnongthai, B. Thipakom, "Off-Line signature recognition using parameterized Hough Transform ", Proceedings of Fifth International Symposium on Signal Processing and its Applications, ISSPA '99, Brisbane, Australia, 22-25 August, 1999 Organized by the Signal Processing Research Centre, QUT, Brisbane, Australia.
[8] H. B. Kekre, V. A. Bharadi, "Off-line signature recognition Systems" International Journal of computer application, Vol 1, No.27, pp 48-56, 2010.
A. Bansal, D. Garg, A. Gupta, "A pattern matching classifier for offline signature verification", IEEE 2008, pp.1160-1163
[9] M. V. Karki, K. Indira, S. S. Selvi, "Offline signature recognition and verification using neural network", IEEE 2007, pp.307-312
[10] G. Agam, "Warping based offline signature recognition", Information forensic and security, Vol.2, issue 3 IEEE 2007, pp.430-437
A. G. Prasad & V. M. Amaresh, "An offline signature verification system".
[11] E. Ozgunduz, T. Sentnrk & M. Elif Karshgil, "Efficient off-Line verification and identification by multicast support vector machine".
[12] R. Sabourin, G. Genest, F.J. Preteux, "Off-line signature verification local granulometric size distributions", IEEE Trans. Pattern Anal. Mach. Intell. 19 (9) (1997) 976-988.
[13] B. Fang, C.H. Leung, Y. Y. Tang, P.C.K. Kwok, K.W. Tse, Y.K. Wong, "Offline signature verification with generated training samples", IEEE Proc, Image Signal Process. 149 (2) (2002) 85-90.
[14] Bai-ling Zhang, "Off-line signature recognition and verification by kernel principal component self-regression", Proceedings of the 5th International Conference on Machine Learning and Applications (ICMLA'06), 0-7695-2735- 3/06, 2006, 4 – 6.
[15] H. Baltzakis, N. Papamarkos, "A new signature verification technique based on a two-stage neural network classifier",
[16] Engineering Applications of Artificial Intelligence 14 (2001) 95±103, 0952-1976/01/$ - PII: S 0 9 5 2 - 1 9 7 6 (0 0) 0 0 0.
[17] S. Armand, M. Blumenstein and V. Muthukkumarasamy, "Off-line signature verification based on the modified direction feature", Engineering Applications of Artificial Intelligence 14 (2004), 0952-1976/04/$ - PII: S 0 9 5 2 6.
[18] J. Edson, R. Justino, F. Bortolozzi and R. Sabourin, "The interpersonal and intrapersonal variability influences on off-line signature verification using HMM", Proc. XV Brazilian Symp. Computer Graphics and Image Processing, 2002, pp. 197-202, Oct. 2002.
[19] M.A. Ferrer, Jesu´s, B. Alonso, and C.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.
[20] P. Deng, H. Y. M. Liao & H. Tyan, "Wavelet based off-line signature recognition system", Proceedings 5th Conference on Optical Character Recognition and Document Analysis, 1996, Beijing, China.
[21] S. Chen and S. Srihari, "Use of exterior contours and shape features in off-line signature verification", Proceedings of the 2005 Eight International Conference on Document Analysis and Recognition (ICDAR'05), 1520-5263/05.
[22] R. Abbas, "Back propagation neural network prototype for off line signature verification", thesis Submitted to RMIT, 2003.
[23] B. Majhi, Y. Reddy, D. Babu, "Novel features for off-line signature verification", International Journal of Computers, Communications & Control Vol. I (2006), No. 1, pp. 17-24.
[24] B. Fang, Y.Y. Wang, "A smoothness index based approach for off-line signature verification", Document Analysis and Recognition, 1999, ICDAR '99. Proceedings of the Fifth International Conference on 20-22 Sept.1999, PP 785 - 787, 10.1109/ICDAR. 1999.791905.
[25] S. Audet, P. Bansal, and S.Baskaran, "Off-line signature verification using virtual support vector machines", ECSE 526 - Artificial Intelligence, April 7, 2006
[26] Y. Xuhua, F. Takashi, K. Obata, Y. Uchikawa, "Constructing a high performance signature verification system using a GA method", IEEE Conf. ANNES, 20-23 Nov. 1995, PP: 170 - 173, 10.1109/ANNES.1995.499465.
[27] R. C. Gonzalez and R. E. Woods "Digital Image Processing", second edition, ISBN81-7808-629-8, 2003.
[28] T. Pavlidis"A thinning algorithm for discrete binary images. Computer graphics and image processing journal Vol.13, Issue 2 1980, 13:142-157.