

REVIEW ARTICLE



ISSN: 2321-7758

REVIEW ON: OFFLINE SIGNATURE VERIFICATION IN PUNJABI

Ms. RAJPAL KAUR, Ms. POOJA CHOUDHARY

Article Received: 23/10/2014

Article Revised on: 01/11/2014

Article Accepted on:03/11/2014



RAJPAL KAUR



POOJA CHOUDHARY

ABSTRACT

Biometrics, which refers to identifying an individual based on his or her physiological or behavioral uniqueness, reliably distinguishes between an authorized person and imposter. Signature can be verified in different parts as offline (static) and online (dynamic). This paper presents HMM with surf feature based recognition of offline signatures system that is trained with low-resolution scanned signature images. The signature of a person is an important biometric attribute of a human being which can be used to authenticate human identity. However human signatures is technique that can be handled as image and recognized using computer vision or operations and hidden Markov model(HMM) with surf feature techniques. With modern computers, there is need to develop fast algorithms for signature verification and recognition. There are many different approaches discussed to signature recognition and verification for research. In this paper, off-line signature verification using HMM and surf feature is proposed, where the signature is captured and presented to the user in the form of scanned image. Signatures verification can be perform based on different parameters extracted from the signature using various image processing techniques. The Off-line (static) Signature verification and recognition is implemented using Mat lab toolbox. This work has been tested (Analyzing) and found suitable for its purpose. For the implementation of this proposed work Mat lab software is used.

Keywords— Signature verification, signature recognition, signatures database, and HMM.

©KY Publications

INTRODUCTION

Biometrics is the act of science to verify and identify a human being. Biometrics confirmation crown or judge numerous improvements over conventional approaches. Biometrics can be categorized into two types: Behavioral and physiological. Behavioral biometrics including signature verification, keystrokes dynamics. Physiological biometrics including fingerprints and iris characteristics .The

signature verification and signature recognition are the behavioral biometrics. Signature is act of writing person's name that may contain many alphabets, characters and letters. In signature verification scan the signature of person, done some improvements and match it with the signature stored in database. In signature verification the test signatures is

compared with all signatures in database, it find out the test signature is forged or original.

Different Types of signature verification: The handwritten signature verification has two categories: Online signature verification and offline signature verification.

Dynamic or online signature verification: An online signature included the dynamic properties and works on signal processing and pattern recognition. The dynamic properties are as flow of pen tip , duration, velocity, pressure point and acceleration and acquisition done by stylus, touch screen, digitizer.

Static or online signature verification: In offline signature verification data acquisition done by scanner. It works on document authentication using in banks, performing financial transactions, boarding an aircraft and crossing international borders.

Types of forgery: The main objective of offline signature verification system is to discriminate between original and forgery .These types of forgeries explained as:

Random Forgery: The forger written the signature but who don't knows the shape of original signature.

Unskilled Forgery: The forger writes the signature in his own style without knowledge of spelling.

Skilled Forgery: The forger who have practice in coping the signatures.

Tracing: The forger has modelise the original signature, which he or she may contain beside a window, utilize carbon paper, or light box and square another sheet of paper over the tap, and literally trace the line.

Cut and paste: The original signature is cut from one document and paste on another document and after it photocopied. If the resolution is properly adjusted the document will appear genuine.

Error Rates: The many types of error rates for signature verification that will define the signature verification system that explained as below:

False Rejection Rate (FRR) : FRR is the ratio of total number of forger signatures accepted to the total number of forger signature submitted. It is also called type-1 error.

False Acceptance Rate (FAR): FAR is the ratio of total number of original test signature rejected to the total number of original test signatures submit. FAR is also call type-2 errors.

Average Error Rate (AER): The Average error rate is the average of FRR and FAR or average of type-1 and type-2 errors.

Mean square error (MSE): The MSE betokens error function which tries to minimize the errors between the network output and target value.

Equal Error rate (EER): The EER is simply a point or location in ROC where the FRR and FAR are equal.

STEPS OF SIGNATURE VERIFICATION

In signature verification following steps are discussed:

Data acquisition: In the offline signature image data acquisition done by scanner and digital camera.

Preprocessing: The preprocessing is process to prepare the signatures for feature extraction and make signature image better or enhance after scanning image.

- i. **Noise Removal:** Image is containing salt and pepper noise, that noise is detected using many morphological filters or operation.
- ii. **Binarization:** It is process of transformation of gray scale image into binary image.
- iii. **Cropping:** Crop the particular part of image for more improvements and enhancement.
- iv. **Thinning:** In thinning eliminate the thickness of the image using morphological operations.
- v. **Resizing:** After cropping the image is zoom in and zoom out then to the bounding rectangle of the signature.

Feature Extraction: Feature extraction is process of extracting the characteristics and attributes from image which is most useful for classification part. Mostly the exactness of verification system depends on feature extraction process. Feature extraction process is divided into two parts:

- i. **Global Features:** Features which are extracted whole characteristics or attributes of whole signature or image. The Global features extracted block codes, Fourier series and wavelet, width, edge points, length, baseline of signature and density, kurtosis, occupancy ratio, vertical and horizontal projection, center of gravity, normalized area of black pixels. The Global feature declares limited information for signature verification but it extracted comfortably and without any difficulty.
- ii. **Local Features:** Local features are extracted from finite area of signatures and extract information in more detail. So, it is more accurate than global. It extracts both statistical and geometrical features. Statistical Features are extracted from pixel distribution of signature image and geometrical features included the location, tangent track, curvature.

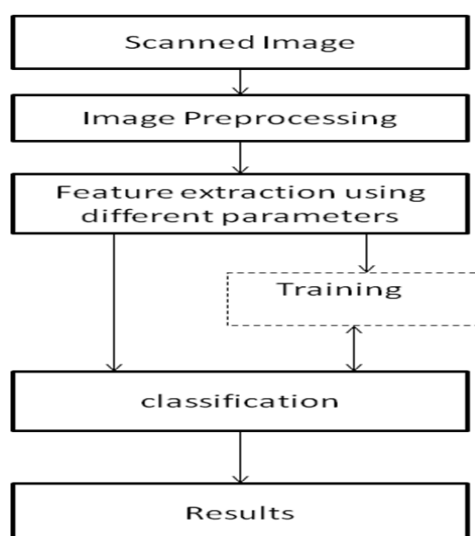


Figure 1: Signature verification Steps

CLASSIFICATION

There are many methods or techniques used for offline signature verification and recognition some of them discussed below:

Neural Network: To train the extracted features the neural network is most widely used. The neural network is consisting of small processing unit which is modeled on human nerves system. The NN have more than a few types of architecture; two main are feed forward and recurrent NN. Artificial Neural network is also known as NN. The NN including no. of input layers, hidden layers and output layers. The output layer will get binary decision based on predefined threshold. Many neural network topologies are tested and their correctness is compared. The input is received the magnitude of the output is greater than threshold otherwise input is rejected. NN most useful in signature verification for the purpose of handwritten signatures and verify its authenticity. Two steps included are Training and Learning. In the primary Training phase, training with the help of extract a feature set representing the signature with several samples from conflict signers. In second phase the learning is for the NN to learn the relationship between a signature and its class.

Hidden Markov Model: Hidden markov Model is most useful model for both offline and online signature verification. HMM is arithmetical, geometrical and algebraic learning model that assume both variableness and characteristics of variables and resemblance or relation of sharing properties between patterns. HMM is based on simple induction principles that are Empirical Risk Minimization principle. HMM is depends upon grid segmentation scheme because it extracts three

features: Pixel density feature, pixel distribution features and an axial slant features for density forgery. Handwritten signature is series of vector of values relative to each point of signature in its trajectory. A well chosen set of features vector for HMM could lead to design of a better signature verification system.

The matching is done by step of probability distribution of features involved in the signatures. If the result shows a higher or better probability than the test signature probability then it means signature is of original person otherwise signatures are rejected.

Support Vector Machine: SVM is kernel based technique that is very useful in signatures verification procedure. The Three major kernels have been used polynomial kernel, radial kernel, and linear kernel Verification process. SVM are machine learning algorithm that can be used to find the solution of multiclass problems. SVM is also used for appraise difference between classes of given data to generalize unseen data and high dimensional feature space. SVM is based on Structural Risk Minimization principle. SVM becomes very popular because of it is very successful in handwritten digit recognition. It is consist of two classes Linear Separable and classification difficulty. The linear separable establish the hyper plane with maximum Euclidean distance from the training set.

Template Matching: A process of pattern comparison is frequently or usually called template matching. Most widely used dynamic time wrapping method for matching, in this method test signatures are matched with templates of genuine signatures stored in knowledge base. System uses a closed contour tracing algorithm to exhibit the edge of

each signature with separate closed contour. The curvature facts of the traced closed contour are break down into multiresolution signals using wavelet transformation, zero-crossing equivalent to the curvature data are extracted as features for matching based on the correctness of the feature extraction process is calculated.

I. PROPOSED METHODOLOGY

The offline signatures verification system are divided into following Stages:

- Data Acquisition
- Preprocessing
- Feature Extraction
- Matching

- Classification
- Results or error rates

Firstly collect the Punjabi signature database with blue and red ink pen. After collecting the data scan the signature data using scanner or camera. Then perform the preprocessing and extract the features using Gabor filter. To locate the signatures are forgers or original we purpose the SURF Features matching and critical point matching for signature matching and the use of hidden markov model classifier for better accuracy. The results obtain using the error rates false acceptance rate, mean square error and false rejection rate.

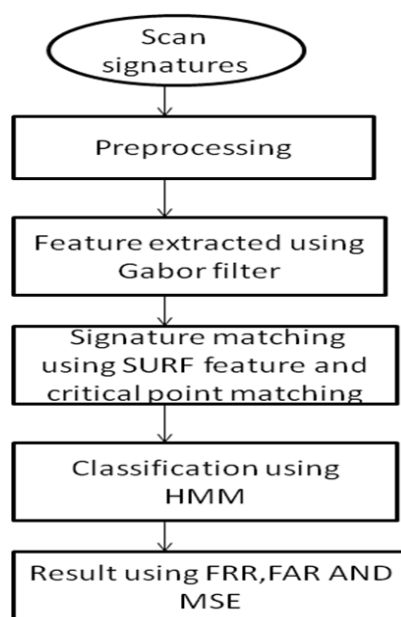


Figure2: Proposed methodology steps

LITERATURE SURVEY

The offline signature verification is one most challenging area of pattern recognition. An individual signature seize a property that it is not always consistent. It varies to a certain extent even done by a single person in that order. A number of such researchers and preceding work are summarized below:

Vahid Malekian, Alireza Aghaei, Mahdie Rezaeian and Mahmood Alian [2] introduce the rapid offline signature verification base on signature envelope and density partitioning using artificial neural network and support vector machine. The FAR achieved is 5.3% and FRR is 4.0. Ali Karouni, Bassam Daya, samia Bahlak [3] introduces the offline signature recognition using neural network approach. The geometrical features extracted and classification using ANN. Obtain the threshold 90%, FAR of 1.6% and FRR of 3% and classification ratio is 93%. Vu Nguyen, Midheal Blumenstein graham Leedham [4]

proposed a global feature for offline signature verification problem. The global features based on the boundary of a signature and its projections. The SVM is classifier is used for better accuracy and classification. The first global feature is derived from the total 'energy' a writer that uses to create the signature. The second features hire information from the horizontal and vertical projections of signature. FRR is 17.25% and FAR for random and targeted forgeries are 0.08 and 17.25.

Mohammed A. Abdala and Noor Ayad yousif [5] introduce a system based on two neural network classifier and three feature sets including global, texture and grid features. There are three phases performed. Firstly preprocessing second is feature extraction and last is classification using neural network and second classifier consisting of Radial Basis function neural network. The first classifiers recognize the signature and the identification rate is 95.955%. L.Basavaraj and R.D sudhakar Samuel [6]

proposed offline signature verification technique based on four speed stroke angle. The dynamic features extract of static signature image. The idea is used in it which is the intensity is directly propositional to speed of the stroke. In this method achieved FRR of 14.25% and FAR of 13.78%. H.Baltzakis and N. Papamarkos used two stages neural network classifier for offline signature verification [7] three features describe Grid, global and feature features. For each feature sets a special two stage preceptors OCON (one – class- one-network) classification structure has been implemented. The FRR is 3% and FAR is 9.81 % acquire. Offline signature verification based on Pseudo- cepstral coefficients proposed by Jesus F. Vargas and Mioguel A.Ferrer [8]. In this method from gray scale images, its histogram is calculated and used a “spectrum” for calculation of Pseudo – Cepstral coefficients. As the result the unique minimum phase sequence is estimated and used as feature vector for signature verification. The FAR is 7.35% and FRR is 5.05% obtained. Ashwini Pansara and Shalini Bhatia [9] introduce another approach using neural network with different set of extracted features. They extracted the geometric features of signature image including area of signature, center of mass, six fold surface feature and trisurface feature etc. The FAR is 14.66 and FRR is 20% in that order. Offline signature verification systems combine some statistical classification proposed by J.B Fasquel and M. Bruynooghe [10]. The signature verification system consists of three phases. First phase is to transform the original signature using identity and four Gabor transforms. Second part is to intercorrelate the analyze signature with the help of similarly transformed signature of learning database and third phase verification of authenticity of signature by fusing the decision related to each transform. FRR is 1.43 % and FAR is 2.56% obtained respectively. Online signature verification based on optimal feature is introduced by Julio Martinez – R and Rogelio Alcantraras [11]. the classification of signatures using neural network driven fuzzy reasoning. In this paper they create a reference signing model and a person extract set of shape features and dynamic features from set of original signatures. For each distinctive feature, an averaged prototype and a consistency function are calculated using genetic optimization. The FAR is 0.27% and FRR is 1.05%.

Prashanth C.R and K.B raja [12] proposed offline signature verification based on angular features. Firstly scanned the signature and perform preprocessing. Then feature extracted, firstly

signature is divided into 128 blocks using center of signature by counting number of black pixels and angular feature in each block is determined to generate 128 angular features. In second part the signature is separated into 40 blocks from each of 4 corners of signature generate 40 angular features. Totally 168 angular features are considered from phase one and phase two to verify signature. FAR is 4.995% and FRR is 8.5%. Shashi Kumar DR, KB Raja, RK Chattaroy Sabyasachi Pattanaik[13] propose offline signature verification based on fusion of global and grid features using neural network classifier. The FAR is achieved 4.16% and FRR is 7.51%.

CONCLUSION

A problem of personal verification and identification is an actively growing area of research. The methods are based on different individual characteristics; movement, lips voice, hand geometry, face, gait, iris, fingerprint and retina are the most commonly used authentication methods. Therefore considerable number of applications is concentrated in the area of electronic commerce and electronic banking system. A lot of signature verification techniques have been proposed earlier but they were not secure enough and can be temporarily tampered with, so the task was not fulfilled. Signature Verification using Surf Feature alone could not provide better results. We use Signature Verification Technique using HMM with surf feature. The results of matching are improved as we use HMM with surf feature technique for matching. Better improved quality of signature and matching results are obtained.

REFERENCES

- [1] Anil K Jain, Arun Ross and Salil Prabhakar, “An Introduction to Biometric Recognition,” *IEEE Transactions on Circuits and Systems For Video Technology*, vol. 14, no.1, pp. 1-29, 2004.
- [2] Vahid Malekian, Alireza Aghaei, Mahdie Rezaeian and Mahmood Alian, “rapid offline signature verification base on signature envelope and density partitioning” *IEEE*, 2013.
- [3] Ali Karouni, Bassam Daya, samia Bahlak, “offline signature recognition Using neural network approach” *A. Karouni et al. /Procedia Computer Science 3 (2011) 155–161.*
- [4] Vn Nguyen, Michael Blumenstein Graham Leedham , “global feature for offline

- signature verification problems" 10th international Conference on document analysis and recognition, 2009 .
- [5] Mohammed A. Abdala & Noor Ayad Yousif, Offline Signature Recognition and Verification Based on Artificial Neural Network, Engineering & Technology Journal, Vol.27, No.7, 2009.
- [6] L. Basavaraj and R.D Sudhakar Samuel, Offline line Signature Verification and Recognition: An Approach Based on Four Speeds Stroke Angle, International Journal of Recent Trends in Engineering, Vol 2, No. 3, November 2009
- [7] H. Baltzakis, N. Papamarkos, A new signature verification technique based on a two stage neural network classifier, Engineering Applications of Artificial Intelligence 14 (2001) 95-103.
- [8] Jesus F. Vargas, Miguel A. Ferrer, Carlos M. Travieso, Jesus B. Alonso, Offline Signature Verification Based on Pseudo Cepstral Coefficients, 10th International Conference on Document Analysis And Recognition 2009.
- [9] Ashwini Pansare, Shalini Bhatia, Handwritten Signature Verification Using Neural Network, International Journal of Applied Information Systems (IJ AIS) ISSN: 2249 0868 Foundation of Computer Science FCS, New York, USA Volume 1 No.2, January 2012.
- [10] Jean Baptiste Fasquel and Michel Bruynooghe, A hybrid opto-Electronic method for real time automatic verification of handwritten Signatures, Digital Image Computing Techniques and Applications, 21, 22 January 2002, Melbourne, Australia.
- [11] Julio Martínez R., Rogelio Alcántara S., Online signature verification Based on optimal feature representation and neural Network driven Fuzzy reasoning.
- [12] Prashanth C. R. and K. B. Raja, Offline Signature Verification Based On Angular Features, International Journal of Modeling and Optimization, Vol. 2, No. 4, August 2012.
- [13] Shashi Kumar D R, K B Raja, R. K Chattaroy, Sabyasachi Pattanaik, Offline Signature Verification Based on Fusion of Grid and Global Features Using Neural Networks, International Journal of Engineering Science and Technology Vol. 2(12), 2010, 7035-7044.
- [14] J.F. Vargas, M.A. Ferrer, C.M. Travieso, and J. B. Alonso. Offline signature verification based on pseudo-cepstral coefficients. 10th IEEE Int Conf on Document Anal. & Recognition, 2009.
- [15] A.I. Al-Shoshan. Handwritten signature verification using image Invariants and dynamic features. Proc of the IEEE Int Conf on Computer Graphic, Imaging and Visualization (CGIV'06), 2006.
- [16] M. Piekarczyk. Hierarchical random graph model for off-line handwritten signatures recognition. IEEE Int Conf on Complex, Intelligent, Software Intensive Systems, 2010.
- [17] S.M.S. Ahmad, A. Shakil, M.A. Faudzi, R.M. Anwar. Analysis of Goat' within user population of an offline signature biometrics. 10th IEEE Int Conf on Information Science, Signal Processing and their applications (ISSPA 2010).
- [18] J.P. Drouhard, R. Sabourin, and M. Godbout. A neural network Approach to off-line signature verification using directional PDF. Pattern Recognition, 29(3), (1996), 415--424.