ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 6, June 2014

A Review on Offline Signature Recognition and Verification Techniques

Sameera Khan[1], Avinash Dhole[2]

M-Tech Scholar, Department of Computer Science and Engineering, RITEE, Raipur, India[1]

Associate Professor, Department of Computer Science and Engineering, RITEE, Raipur, India[2]

Abstract: As signatures are widely accepted bio-metric for authentication and identification of a person because every person has a distinct signature with its specific behavioural property, so it is very much necessary to prove the authenticity of signature itself. A huge increase in forgery cases relative to signatures induced a need of efficient "Signature Verification System". These systems can be online or offline based on type of input taken by the system. This paper represents a brief review on various approaches used in signature verification systems.

Keywords: Signature, Biometric, Neural Networks, Off-line Signature Recognition and Verification.

I. INTRODUCTION

Biometrics are technologies used for measuring and analysing a person's unique characteristics. There are two types of biometrics: behavioural and physical. Behavioural biometrics are generally used for verification while physical biometrics can be used for either identification or verification. Among the different forms of biometric recognition systems such as fingerprint, iris, DNA, face, voice, vein structure palm etc., signature is widely used bio-metric. On the basis of signature acquisition method in the computer system, signatures are classified as online and offline signatures.

II. TERMINOLOGIES IN SIGNATURE VERIFICATION

A. *Types of Forgeries*

- **Simulation**-the forger has access to a model of the genuine signature from which he practices making copies
- **Tracing**-the forger has a model of the genuine signature, which he may hold against a window, or use carbon paper or a light box, and place another sheet of paper over the top, and literally trace the line.
- **Cut-and-paste**-A genuine signature is cut from one document and placed on the spurious document, then photocopied. If the lighting and resolution is properly adjusted, the document will appear genuine.
- **Electronic forgery**-The forger simply digitizes a genuine signature by scanning at a high resolution, then inserts it into the spurious document and prints it.
- **Freehand signature**-The forger simply writes the victim's name without making any attempt to copy.

B. *Types of Signatures*

Based on the definitions of signature, it can lead to two different approaches of signature verification viz Off-Line or Static Signature Verification Technique and On-line or Dynamic Signature Verification Technique.

- **Off-Line or Static Signature Verification Technique**-This approach is based on static characteristics of the signature which are invariant In this sense signature verification, becomes a typical pattern recognition task knowing that variations in signature pattern are inevitable; the task of signature authentication can be narrowed to drawing the threshold of the range of genuine variation. In the offline signature verification techniques, images of the signatures written on a paper are obtained using a scanner or a camera.
- **On-line or Dynamic Signature Verification Technique**-This is the second type of signature verification technique. This approach is based on dynamic characteristics of the process of signing. This verification uses signatures that are captured by pressure sensitive tablets that extract dynamic properties of a signature in addition to its shape. Dynamic features include the number of order of the strokes, the overall speed of the signature and the pen pressure at each point that make the signature more unique and more difficult to forge.

C. *Error Rates*

False rejection rate (FRR) is one of the most important specifications in any biometric system. The FRR is defined as the percentage of identification instances in which false rejection occurs. It is also known as Type- I error

- **False acceptance rate (FAR**) is the measure of the likelihood that the biometric security system will incorrectly accept an access attempt by an unauthorized user. A system's FAR typically is stated as the ratio of the number of false acceptances divided by the number of identification attempts. It is also known as Type- II error
- **Average Error Rate (AER**) is the average of type 1 and type 2 errors.
- **Equal Error Rate (EER)** is the location on a ROC or Detection Error Trade-off curve where the FAR and FRR are equal. Smaller the value of EER, better is the performance of the system.

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 6, June 2014

III. STEPS IN OFFLINE SIGNATURE VERIFICATION

An offline signature verification scheme basically uses some network or mechanism as a classifier and a database in which some specimen signatures are stored. Features are extracted for each stored signature and when a new signature is employed it is matched using the classifier which classify it as genuine or forgery. Steps involved in Signature verification process can be summarized as-

- Acquire the Signature images to create a database.
- Perform image pre-processing to remove noise and blurring.
- Extract the various features of stored images.
- Use these features to train the classifier
- Employ unknown Signature image and extract its features.
- Perform the pattern matching with data set
- Do the classification and classify as genuine or forge.

IV. CLASSIFICATION

Major techniques used for offline signature verification system are based on Template Matching, Statistical Approach, Structural Analysis Approach , Spectrum Analysis Approach, Neural Network Approach[1]

- **Template Matching Approach** – The template matching is the simplest and earliest but rigid approach to pattern recognition in which instances of pre-stored patterns are sought in an image. It is performed at the pixel level and also on higher level. This approach has a number of disadvantages due to its rigidity. It may fail if the patterns are distorted due to the imaging process, viewpoint change etc as in the case of signatures. It can detect casual forgeries from genuine signatures But cant verify between the genuine signature and skilled ones. The template matching method can be categorized into several forms such as graphics matching, stroke analysis and geometric feature extraction, depending on different features.
- **Statistical Approach** – In this approach, each pattern is represented in terms of features and is viewed as a point in a d-dimensional space. Each pattern vector belonging to different categories occupy compact and disjoint regions in a d-dimensional feature space. Decision boundaries are set in feature space to separate different classes. The effectiveness of the feature set is determined by how well patterns from different classes can be separated. Hidden Markov Model (HMM), Bayesian these are some statistical approach commonly used in pattern recognition. They can detect causal forgeries as well as skilled and traced forgeries from the genuine ones.
- **Structural Approach** - It is related to graph, string and tree matching techniques and is used in combination with other techniques. It shows good performance detecting genuine signatures and forgeries. Its major disadvantage is that it uses large dataset for greater accuracy.
- **Spectrum Analysis Approach**-In this method the first stage of the procedure is the transformation of the data into another matrix which is a version of the trajectory matrix in Spectrum Analysis. Than a square window is placed in all possible places of image.[2] It basically decomposes a curvature-based signature into a multi-resolution format. This approach is used for long scripted signatures
- **Neural Network Approach**- The main characteristics of neural networks are that they have the ability to learn complex nonlinear input-output relationships, use sequential training procedures, and adapt themselves to the data. The most commonly used family of neural networks for pattern classification tasks is the feed-forward network, which includes multilayer perceptron, Radial-Basis Function (RBF) networks Self-Organizing Map (SOM), or Kohonen-Network.

V. PROPOSED METHODOLOGY

Working of an offline signature verification system can be sub divided into following stages-

- Data Acquisition
- Image pre-processing
- Feature Extraction
- Training the network
- Classification

- **Data Acquisition**-Signatures are collected using black or blue ink enclosed in a rectangular box of size 5cm×3cm.Each person provides at least 10 specimens of his signature with maximum possible variation. These signatures are then scanned and converted into gray image and are stored in a database.
- **Image pre-processing**- In this stage we will perform binarization ,background elimination, noise reduction ,size normalization and skeletonization on each signature image[3]. In binarization a color image is converted into black and white image so as to make feature extraction more easier. Background elimination and noise reduction is performed in those images which are extracted from some other documents. Skeletonization gives a skeleton of 2-D binary image which can be easily processed.
- **Feature Extraction**- The choice of a powerful set of features is crucial in signature verification systems. In this system, three groups of features are used such as grid features, local features and global features. In addition to these features SURF and MSER features are also used. Grid information concerned with the overall appearance information of the signature. The skeleton image is divided into 96 rectangular segments, (12 X 8), for each segment the area (sum of foreground pixels) is calculated. The result is normalized so that the lowest value (for the rectangular with smallest number of black pixels) will be zero and highest value (for the rectangular with highest number of black pixels) will be one. The result is 96 values for each signature image. Global features describe the entire signature image such as width, height, aspect ratio. These features are used in combination with other features. These features are less sensitive to noise. Local features describe the properties of signature image in specific parts. They are calculated by partitioning the signature image into

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 6, June 2014

parts by help of geometric centre or some other means.

- **Training the network**-Training a RBFN is the most crucial task of the system and is performed by using PSO. Three signatures from each individual is used in the training. After taking each input signature, it is pre-processed and is fed to the feature extraction module. Input matrices for the training of the first three ANNs are prepared after getting all the input signature features. The classifier which will be used in this system will use a radial basis function network. Training a neural network includes setting many tuneable parameters like-
  - The type of radial function to be used in the hidden units.
  - The distance type.
  - The centre of the radial functions (location of the hidden units).
  - The spread or radius of the radial functions.
  - As for the hidden units, Gaussian function is often used as the radial function and Euclidean distance as the distance type. In this case, the output of the i-th hidden unit with centre μi and spread σi is given as follows:

$$\phi_i(\mathrm{x}) = \phi\left(\|\mathrm{x}-\mu_i\|;\sigma_i\right) = e^{\left(-\frac{\|\mathrm{x}-\mu_i\|^2}{2\sigma_i^2}\right)}, \forall i$$

- Training an RBF network consists of finding the values for these parameters, such that the overall approximation or classification error is reduced. The values chosen for the centres and the spread of the radial functions have a great effect on the generalization abilities of the network. Many algorithms have been proposed for finding the centres of an RBF network
- **Classification**-When a new signature is employed, its features are extracted and matched with those already store in the database. If the features are matched than it is classified as genuine otherwise forge.

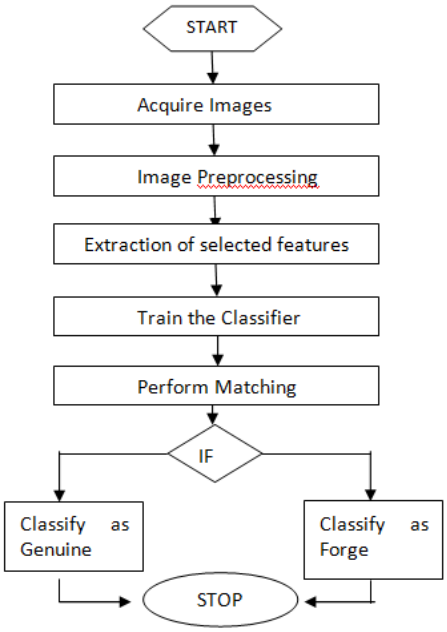

Fig. 1. Flowchart of SRVS

VI. LITERATURE SURVEY

An individual's signature possesses a property that it is not always consistent. It varies to a certain extent even when done by a single person repetitively. Offline signature verification is one of most challenging area of pattern recognition. Being a behavioural biometric trait which can be imitated, the researcher faces a challenge in designing such a system to counter intrapersonal and interpersonal variations. Several such researches and previous works are summarized below. H. Baltzakis and N. Papamarkos used two stage neural network classifier for offline signature verification[5]. This system was based on global, grid and texture features. For each one of these feature sets a special two stage Perceptron OCON (one-class-one-network) classification structure has been implemented. 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 second-stage radial base function (RBF) neural network structure, which makes the final decision. System was based on total 160 features grouped in three subsets. Observed FAR and FRR are 9.81% and 3% respectively.

Shashi Kumar D R, K B Raja, R. K Chhotaray, Sabyasachi Pattanaik4 [6] introduced Off-line Signature Verification Based on Fusion of Grid and Global Features Using Neural Networks. Fusion of global and grid features are used to generate powerful featurte set and neural networks are used as classifier.FAR achieved was 4.16% whereas FRR was 7.51%

L.Basavaraj and R.D Sudhaker Samuel [7] introduced offline signature verification technique based on four speed stroke angle. It extracts dynamic features of static signature image. It is based on the idea that intensity is directly proportional to the speed of the stroke. This method achieved FAR of 13.78% and FRR of 14.25%.

Prashanth C. R. and K. B. Raja [8] proposed Off-line Signature Verification based on Angular Features (OSVAF). The scanned signature image is skeletonized and exact signature area is obtained by preprocessing. In the first phase, the signature is divided into 128 blocks using the centre of signature by counting the number of black pixels and the angular feature in each block is determined to generate 128 angular features. In the second phase the signature is divided into 40 blocks from each of the four corners of the signature to generate 40 angular features. Totally 168 angular features are considered from phase one and two to verify the signature. A threshold value is set to compare difference of the original and forge signature. FAR is found to be 4.995 and FRR is found to be 8.5

Mohammed A. Abdala & Noor Ayad Yousif [9]proposed a system based on two neural networks classifier and three powerful features sets(global, texture and grid features).It consists of three stages: the first is preprocessing stage, second is feature extraction stage and the last is neural network (classifiers) stage which consists of two classifiers, the first classifier consists of three Back Propagation Neural Network and the second classifier consists of two Radial Basis Function Neural Network.

The system recognize the signature if two BP neural network of the first classifier recognize it and the identification rate is 95.955%.

Offline Signature Verification Based on Pseudo-Cepstral Coefficients proposed by Jesus F. Vargas and Mioguel A.Ferrer [10]. In this technique From gray-scale images, its histogram is calculated and used as "spectrum" for calculation of pseudo-cepstral coefficients. Finally, the unique minimum-phase sequence is estimated and used as feature vector for signature verification. The optimal number of pseudo-coefficients is estimated for best system performance. FAR and FRR are observed to be 7.35 and 5.05. J. B. Fasquel and M. Bruynooghe [11] proposed one offline signature verification system combining some statistical classifiers. The signature verification system consisted of three steps – the first step is to transform the original signatures using the identity and four Gabor transforms, the second step is to intercorrelate the analysed signature with the similarly transformed signatures of the learning database and then in the third step verification of the authenticity of signatures by fusing the decisions related to each transform. The proposed system allowed the rejection of 62.4% of the forgeries used for the experiments when 99% of genuine signatures were correctly recognized. FAR and FRR are 2.56 and 1.43 respectively.

Julio Martínez-R and Rogelio Alcántara-S[12] introduced On-line signature verification based on optimal feature representation and neural-network-driven fuzzy reasoning. To create a reference signing model of a person, a set of shape features and dynamic features are extracted from a set of original signatures. Subsequently, for each distinctive feature, an averaged prototype and a consistency function are calculated using genetic optimization, this procedure derived from the concept of optimal feature representation in which FRR was 1.05% and FAR was 0.27% Another approach using neural network with different set of extracted features was introduced by Ashwini Pansare and Shalini Bhatia[13].They extracted set of geometric features from a signature image which includes center of mass, area of signature, trisurface features , six fold surface features etc. FAR and FRR are reported to be 14.66% and 20% respectively. Vu Nguyen, Michael Blumenstein Graham Leedham [14] proposed a signature verification system using SVM and features extracted are Global features based on the boundary of a signature and its projections. The first global feature is derived from the total 'energy' a writer uses to create their signature. The second feature employs information from the vertical and horizontal projections of a signature, focusing on the proportion of the distance between keystrokes in the image, and the height/width of the signature. The combination of these features with the Modified Direction Feature (MDF) resulted in significant improvement in signature verification. FAR for random and targeted forgeries are 0.08% and 17.25% whereas FRR is found to be 17.25%.

VII. CONCLUSION

There are several approaches for offline signature verification, Each technique has its different advantages and disadvantages, depending on feature set selected for different techniques can be used to get optimum results.

REFERENCES

[1] Hemanta Saikia, Kanak Chandra Sarma, Approaches and Issues in Offline Signature Verification System International Journal of Computer Applications (0975 – 8887)Volume 42– No.16, March 2012.

[2] Hossein Hassani, A Brief Introduction to Singular Spectrum Analysis

[3] Kanawade M. V., Katariya S. S. ,Review of Offline Signature Verification and Recognition System, International Journal of Emerging Technology and Advanced Engineering,Volume 3, Issue 7, July 2013

[4] Madhuri Yadav, Alok Kumar, Tushar Patnaik, Bhupendra Kumar, A Survey on Offline Signature Verification International Journal of Engineering and Innovative Technology (IJEIT), Volume 2, Issue 7, January 2013

[5] 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

[6] Shashi Kumar D R, K B Raja, R. K Chhotaray, Sabyasachi Pattanaik, Off-line 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

[7] L.Basavaraj and R.D Sudhaker Samuel, Offline-line Signature Verification and Recognition: An Approach Based on Four Speed Stroke Angle, International Journal of Recent Trends in Engineering, Vol 2, No. 3, November 2009

[8] Prashanth C. R. and K. B. Raja, Off-line Signature Verification Based on Angular Features, International Journal of Modeling and Optimization, Vol. 2, No. 4, August 2012

[9] Mohammed A. Abdala & Noor Ayad Yousif, Offline Signature Recognition and Verification Based on Artifical Neural Network, Eng & Tech. Journal, Vol.27, No.7,2009.

[10] 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.

[11] 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.

[12] Julio Martínez-R.,Rogelio Alcántara-S.,On-line signature verification based on optimal feature representation and neural-network-driven fuzzy reasoning

[13] Vu Nguyen, Michael Blumenstein , Graham Leedham, Global Features for the Off-Line Signature Verification Problem 10th International Conference on Document Analysis and Recognition, 2009.

[14] Ashwini Pansare, Shalini Bhatia,Handwritten Signature Verification using Neural Network, International Journal of Applied Information Systems (IJAIS) – ISSN : 2249-0868 Foundation of Computer Science FCS, New York, USA Volume 1– No.2, January 2012

BIOGRAPHIES

Sameera Khan is a P. G Student (M. Tech) in the Department of Computer Science and Engineering, Raipur Institute of Technology, Raipur(C.G). She received her Bachelor of Engineering (CSE) in 2008 from Raipur Institute of Technology, Raipur affilated to Pt.Ravishankar University,Raipur (C.G).Her research interest are Image Processing and neural network.

Avinash Dhole is an Associate Professor and Head in Computer Science and Engineering Department, in Raipur Institute Of Technology, Raipur, (C.G.) . His research interests include Digital Image Processing, Compilers, Automata Theory, Neural Network, Artificial Intelligence, Information and Network Security.