ISSN: 2321-7782 (Online)
Volume 3, Issue 1, January 2015
International Journal of Advance Research in Computer Science and Management Studies
Research Article / Survey Paper / Case Study
Available online at: www.ijarcsms.com

A Survey on Handwritten Signature Verification Techniques

Patel Bhumika A[1]
Computer Science & Engineering Department
Parul Institute of Engineering and Technology
Vadodra, India

Shashwat Kumar[2]
Computer Science & Engineering Department
Parul Institute of Engineering and Technology
Vadodra, India

Abstract: Signature verification is the process used to recognize an individual's handwritten signature. Signatures are used in many documents like bank cheques, academic certificates; attendance registers monitoring, legal transactions, etc. Due to large number of documents signature verification is sometimes difficult and time consuming process. Based on data acquisition this system can be online or offline. Online system use electronic tablet and stylus to extract dynamic information about signature where as in offline system camera and scanner are used for extracting static information about signature. This paper represents the survey of various approaches being used in signature verification system.

Keywords: Biometrics, Signature Verification, Feature Extraction, FAR, FRR, RR.

I. INTRODUCTION

Biometrics is technology used for measuring and analysing a person's unique characteristics. Biometrics can be classified into two broad categories, behavioural (signature verification, keystroke dynamics, etc.) and physiological (iris, hand geometry, fingerprint, etc.). Handwritten Signatures are one of the most widely used behavioral biometrics for personal identification and Verification. Even with the introduction of new technologies handwritten signature is continuously used as a means of communication in day to day life like, in a formal agreements, financial systems, government use, marketing documents or paintings etc. The main difficulty observed in a signature verification is individual's signature are not consistent, variation may appear due to signing position, pen width, weight, stress, mood, time etc [7]. Depending on data acquisition method it can be classified in two different ways:

A. On-line (Dynamic mode)

In this technique system obtain the data directly from user through stylus, touch screen, or a digitizer that can generate dynamic values, such as coordinate values, pressure, time, or speed of signature. This technique achieves high accuracy due to its dynamic characteristics.

B. Off-line (static mode)

In the offline signature verification techniques, images of the signatures written on a piece of paper are obtained using a scanner or a camera. Processing of off-line signature is complex due to the absence of stable dynamic characteristics. It contains the lots of noise as compared to on-line signature.

II. GENERAL METHODOLOGY OF SIGNATURE VERIFICATION

The first approach on how to support query operations on encrypted data with bucketization, after the data is encrypted, the

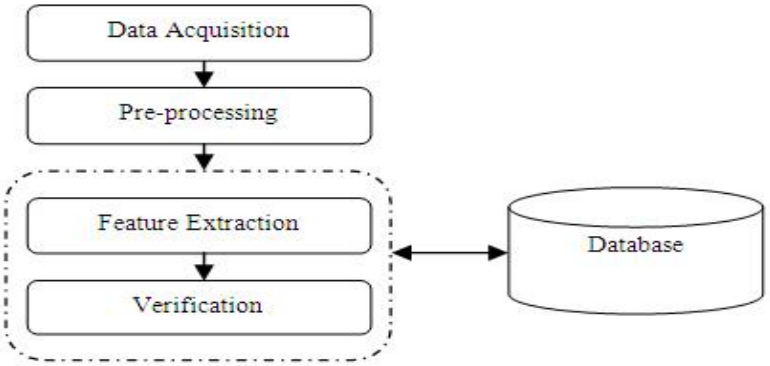

Fig. 1 General overview of signature verification

General methodology of signature verification include following steps:

A. Data Acquisition

This phase obtain the signature from the user through cameras, mobile phone and scanned using the scanners, so that Data is available in digital format for further processing.

B. Pre-processing

Pre-processing is necessary step to improve the accuracy and reduce the Computational needs of Feature extraction and Classification phase. Its main purpose is to make the signature standard and ready for the feature extraction. It primarily include following steps.

Noise Removal: Various noise filtering techniques (Like, Mean, Median, Gaussian filters, Average filter etc.) are applied to reduce noise encounter during a scanning process.

Conversion of color image to Gray image: It converts the color image of signature to a gray scale image. Grey scale images only contain brightness information. Compared with binary images, they contain richer information. Gray scale images contain 8 bits data.

Resizing: The image is cropped, to the bounding rectangle of the signature. So it should be resized to a standard size.

Thinning: The goal of the thinning is to eliminate the thickness difference at each image pixel. After performing the thinning, image data of the offline signature has almost same quality of image data as online signature.

Smoothing: It is often used to reduce noise within an image or to produce a less pixilated image. Excellent smoothing algorithm can both remove various noises and preserve details. It preserves high frequency components.

C. Feature Extraction

The Success of signature verification step is depends mainly on the choice of the powerful sets of features extracted. Feature extraction technique extract attributes and characteristics from the given image and recorded it for further purpose [1]. Feature Extraction is broadly divided into three main categories:

1. Global Features

2. Local features

3. Geometric Features

Global Features: Here, signature is viewed as a whole and features are extracted from the entire pixel confining the signature image. This features are like Signature area, height, width, Aspect ratio, Edge point, Horizontal and vertical center of the signature, Horizontal/ Vertical projection peaks, Number of closed loops, Local slant angle Number of edge points, Number

of cross points, Global slant angle, Baseline shift etc. Global features are suitable for random forgery but it not gives a high accuracy for skilled forgery.

Local features: These features are extracted from a portion or a limited area of the signature image [10]. They are more accurate as compared to global features. Some of the local features are the slant angle of an element, number of black pixels, length ratio of two consecutive parts, central line features, corner line features, position relation between the global and local baseline, stroke elements, local shape descriptors, pressure and slant features and critical points etc.

Geometrical features: These features describe the characteristic geometry and topology of a signature and preserve their global as well as local properties. It describes the geometric characteristic of the signature image. It has the ability to tolerate with distortion, style variations, rotation variations and certain degree of translation [8].

Choice of using global or local features depends mainly on style of the signature and the types of forgeries to be detected from the system. A suitable combination of global and local features has been improving a classifiers ability to recognize forgeries and to tolerate intrapersonal variances [8].

D. Verification

Verification is a decision making steps of the recognition system. Performance of the verification depends on the accuracy of the features. Various approaches used for the off-line signature verification systems are based on the Template Matching approach, Statistical approach, Structural or Syntactic approach, Spectrum Analysis approach and Neural Networks approach [5][6][7].

Template matching approach: Template matching approach is the process of matching the templates. It match the test signature with the training signature (genuine sig.) stored in a database. This approach is simple but rigid approach of pattern recognition.

Statistical approach: In a statistical approach each pattern is represented in the form of features and view as a point in a d-dimensional space. Features should be selected in such a way that the pattern vectors belonging to different categories occupy compact and disjoint regions in a d-dimensional feature space. This approach is used to perform some statistical concept likes the relation, deviation etc between two or more data item to find the specific relation between them.

Structural approach: In structural approach each pattern is represented in the term of symbolic data structure such as graphs, trees. To recognize any unknown pattern (forged sig.), its symbolic representation is compared with the prototype stored in a database. This approach is generally used in combination with other techniques. For greater accuracy this approach requires large data set and large computational efforts.

Spectrum Analysis approach: Spectrum Analysis approach is used to decompose curvature-based signature into multi-resolution format. This approach can be applied to different language like English, Chinese. It is most probably used for the long signatures like some of Indian script signature.

Neural network approach: Neural network (NN) is a network of small processing units is modelled on human nerve tissues [9].Neural Network approach is widely used in signature verification. 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.

III. TYPES OF FORGERIES

Generally three types of forgery occur in signature verification [2][4]. Random forgery, Simple Forgery and Skilled forgery.

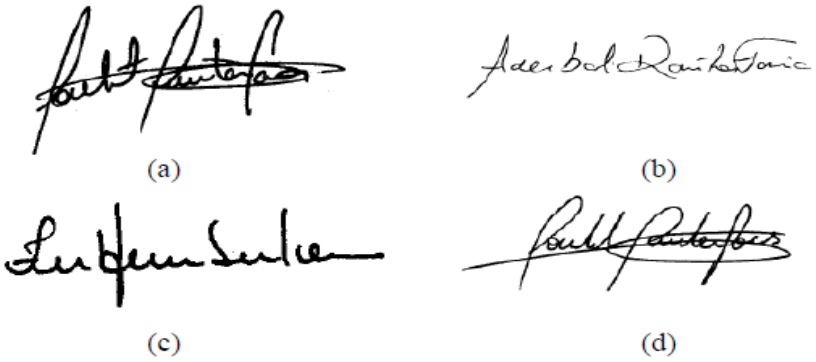

Fig. 2 Type of forgeries: (a) genuine signature; (b) random forgery; (c) simple forgery; and (d) skilled forgery.[5]

A. Random forgery

The forgers sign the signature without any information about signatory name and signature sample. Here, Forger reproduces a random signature so, it is easiest to detect.

B. Simple forgery

The forgers sign the signature without any prior sample of the signature but he/she knows the name of the signatory and then produces the signature in his/her own style.

C. Skilled forgery

The forger knows the name of the signatory and the samples of the genuine signature so he/she is able to reproduce it. It is hardest to detect.

IV. ERROR RATE

In a signature verification system performance is evaluated in term of error rate [2]. Different types of error rates are False Rejection Rate (FRR), False Acceptance Rate (FAR), and Recognition Rate (RR)

A. FAR (False Acceptance Ratio)

The false acceptance ratio is given by the number of forged signatures accepted by the system with respect to the total number of comparisons made.

$$\text{FAR} = \frac{\text{Number of Forgeries sig. accepted}}{\text{Number of Forgeries sig. tested}} * 100$$

B. FRR (False Rejection Ratio)

The false rejection ratio is the total number of genuine signatures rejected by the system with respect to the total number of Comparison made.

$$\text{FRR} = \frac{\text{Number of Genuine sig. rejected}}{\text{Number of Genuine sig. tested}} * 100$$

C. RR (Recognition Rate)

Recognition Rate is the number of signature identified from total number of signature stored.

$$\text{RR} = \frac{\text{Identified Signatures}}{\text{Total Signatures}} * 100$$

V. CONCLUSION

This paper presents a brief survey of the recent works done on signature verification. Different existing methods and approaches are discussed. Lots of work has been already done, still there are many challenges in this research field. First it is difficult to develop one general system to classify every style of signature. Another is it is not easy to make a signature dataset of real documents. Publicly available signature datasets of real documents would make it possible for researchers to achieve a better performance in this field. Most of the researchers have proposed or developed their systems for a limited type of signatures. So, Future work should be extended by fusion of different classifier for better verification results.

References

1. Sameera Khan, Avinash Dhole, "A Review on Offline Signature Recognition and Verification Techniques", International Journal of Advanced Research in Computer and Communication Engineering, June 2014.
2. Nitya Raj, Disha Dawani, Harshit Singhania & Utkarsh Mishra," Signature Verification – A Biometric Authentication System" ISSN 2013.
3. Dr. H.B.Kekre, Dr. Dhirendra Mishra, Ms. Shilpa Buddhadev, "SIGNATURE VERIFICATION", International Journal on Computer Science and Engineering (IJCSE) june 2013.
4. Saba Mushtaq, A.H.Mir, "Signature Verification: A Study" 4th International Conference on Computer and Communication Technology (ICCCT)2013.
5. Arya M S and Inamdar V S. (2010),"A Preliminary Study on Various Off-line Hand Written Signature Verification Approaches", 2010 International Journal of Computer Applications. Volume 1, No. 9 (pp 0975 – 8887).
6. Jain A K, Duin R P W, and Mao J. 2000, "Statistical Pattern Recognition: A Review. IEEE Transactions on Pattern Analysis and Machine Intelligence", (pp 4 – 37) Vol. 22, No. 1, JANUARY 2000.
7. R. Abbas and V. Ciesielski, "A Prototype System for Off-line Signature Verification Using Multilayered Feed forward Neural Networks", February 1995.
8. 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.
9. Surabhi Garhawal, Neeraj Shukla, "A Study on Handwritten Signature Verification Approaches", International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 2, Issue 8, August 2013.
10. Nguyen V, Blumenstein M and Leedham G. Global Features for the Off-Line Signature Verification Problem. 2009 10th International Conference on Document Analysis and Recognition (IEEE) 2009.

