International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Impact Factor (2012): 3.358

Survey of Various Techniques for Signature Recognition and Verification

Sharayu S. Sangekar[1], D. C. Dhanwani[2]

[1]Student, Computer Science & Engineering, P.R.Pote College / Sant. Gadge Baba Amravati University, India

[2]Assistant Professor, Computer Science & Engineering, P.R.Pote College / Sant. Gadge Baba Amravati University, India

Abstract: ***Signatures are widely accepted bio-metric for authentication and identification of a person because every person has a distinct signature with its specific behavioural feature; hence it is very much necessary to prove the authenticity of signature itself. A large increase in forgery cases relative to signatures induced a need of efficient "Signature Recognition System". These signature recognition systems can be online or offline based on the type of input taken by the system. Handwritten signature is used widely as biometric traits for authentication of person as well as document. After preprocessing the signature, various features are extracted.***

Keywords: Signature Recognition, Biometric, HMM, Support Vector machine (SVM), Neural Network.

1. Introduction

Signature recognition is a behavioural biometric. It may be operated in two alternative ways static and dynamic. Signature Recognition Systems needs to preprocess the data. It includes a number of operations to induce the results. The major steps are Data Acquisition, Signature Pre-processing, Feature Extraction, Enrollment& Training and Performance Evaluation[1].

The word biometrics comes from the Greek word bios (life) and metrikos (measure). In general, there are three levels of computer security schemes. The primary one depends on something a person can carry, such as an ID badge with a photograph or a computer card key. The second depends on something a person aware of, such as a password or a code number. The last one depends on something a part of a person's biological makeup or behaviour, such as fingerprint, facial image, or a signature. Biometric verification is defined as a method of uniquely identifying a person by analyzing one or more of his/her biological traits. Biometrics is basically of two categories, physical and behavioural [2].

Major analysis issue with these systems is change of state of biometric information over time as per the physical conditions or emotional situations of human beings. Signature is found to be the foremost authentic parameter within the field of authentication. Signature is that special pattern provided by human to authenticate himself/herself at secured and private zones. [3].

Signature is the most common authentic entity from the user aspect that has been used earlier in numerous confidential purposes. For improving security of authentication system, the signature should be enrolled and verified. The Proposed authentication system is the replacement for password based authentication[4].

Signatures acts as a strong authentication feature of the signer. But, the manual verification of signatures by humans is tedious job. Therefore, an automated Signature verification system is required which will improve the authentication process and hence provide some secure means for authorization of legal documents. The main objective of signature verification system is to discriminate between two classes i.e. original and forgery.[5]

Signature recognition involves identity verification by making comparison between test signatures and sample signatures in database. Signature recognition can be closely related to the interpretation of human handwriting to text by a machine. One of the most popular technique widely used for such an interpretation is an Optical Character Recognition (OCR).

2. Literature Survey

A lot of research has been done in off-line signature recognition and verification. Bakri & Nurhaniza stated that the design and development of an offline signature verification system that is mainly based on Hidden Markov Modelling (HMM) technique which is performed on a series of a localized direction features extracted from a scanned signature image[6].

Pradeep Kumar and Shekhar Singh elaborates, there is an effort to describe how a HMM are stochastic models and they have the ability to acquire pattern differences and the similarities. It describes the analysis of the testing results by varying the number of HMM states and their state transition topology. The testing reported in this paper has been carried out on signature samples of 100 users which contain both their genuine as well as their skilled and random forged signature samples counterparts[7].

Ashwini Pansare & Shalini Bhatia describes that the neural network is widely used approach because of their simplicity and power of usage. It involves, firstly extracting a feature set representing the signature and in second step involves finding out the relationship between signature and its class. Once this relationship has been determined, it gives results proposing test signature belongs to a particular signer[8].

H.S.Srihari & M.Beall attempts to study two specific approaches. The objective is to determine the class and to match the signature. The very First method is the Resilient Back propagation (RBP) neural network and second one is

Radial Basic Function (RBF). A database of around 2K signatures containing 40% genuine and 60% forgeries is used[9].

Ashwini Pansare & Shalini Bhatia also focuses on the Support Vector Machines (SVMs). These are machine learning algorithms. These algorithms uses a high dimensional feature space to derive unseen data by calculating differences between classes of given data. Several attributes of signature such as grid features and directional are used[8].

Hemant Saikiaand and Kanak Chandra Sarma proposes that one of the simpler approach is the template matching approach. It is not only a very primitive approach but also simple and robust for pattern recognition. Although not all is correct, its robustness provides a numerous drawbacks. In case ,the patterns are distorted then it fails in signature recognition. In signatures patterns there are often large intra class variations. Nevertheless detection of light distortion will be successful. But for the adept ones it is not advisable[10]. The template matching method can be divided into several forms such as graphics matching, stroke analysis and geometric feature extraction, depending on different features.

Hemant Saikiaand and Kanak Chandra Sarma elaborate another approach named as the statistical approach; this approach considers each pattern as d features and treats it as a point in a d-dimensional space. In this approach pattern vectors categorized separately when shown in a d-dimensional feature space must be employed in close and disjoint regions.

A feature set is considered as useful if patterns from the different classes are well detached. Some of the popular example for the statistical approach is Hidden Markov Model (HMM) and Bayesian which are used for pattern recognition. The difference between statistical approach and the template matching approach is not only the lightly faked signatures but even the adept forgeries do not pass and are caught. Analysis has been drawn from the comparative study of each of the above given an approach which is shown in table:

Approaches	*Advantages*	*Disadvantages*
Hidden Markov Model	It is easy to implement which results in quick verification operation	It is expensive approach
Neural Network Approach	It is widely used approach mainly because of its simplicity and power of usage	Neural Network cannot be retained ,if you add data later.
Support Vector Machine Approach	This approach use high dimensional feature space to drive unseen data.	Lack of transparency of result.
Template Matching Approach	It is simple and robust	It can detect only unskilled forgery but fails just in case of skilled forgery.
Statistical Approach	It is widely used and can detect skilled forgery as well.	It is also expensive

3. Overview of Proposed Methodology

The overall design of signature recognition system is as follows:

- Signature acquisition,
- Preprocessing,
- Feature extraction, and
- Classification.

A signature verification system is employed to authenticate the identity of any person, based on an analysis of his/her signature by using a set of different processing steps.

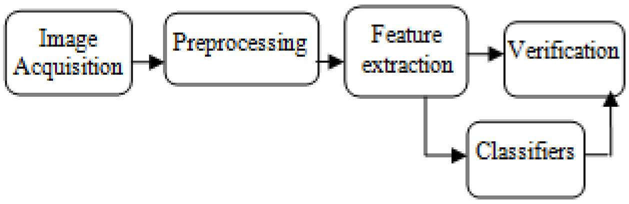

Figure 1: Basic Stages in Signature Verification

In the pre-processing stage, RGB image of the signature is converted into gray scale and then to the binary image. Thinning is then applied to make the signature lines as single thickness lines and any noise present in scanned images are removed thus creating the signature image ready for extracting features. Features available to extract in offline signatures can be either global features or it can be texture feature i.e. the features extracted from whole images.

In this system, the features extracted are mainly Aspect ratio, Signature Area, Maximum horizontal and maximum vertical histogram, End point number of the signature, Texture contrast, Entropy. These features which are extracted form the basis to make comparison and there by classify Signatures as either genuine or forge. The features extracted from the database are then compared with the features extracted from the test signatures and based on the classification criteria the signatures are classified either genuine or forged.

4. Conclusion

There are various approaches for offline signature verification, each technique has its own advantages and disadvantages, depending on the feature set selected for various techniques can be used to obtain better results.

References

[1] V.A.Bharadi,"Off-line Signaature Recognition Systems",International Journal of computer applications ,Volume1-No.27,2010.

[2] Syed Faraz Ali Zaidi,"Biometric Handwritten Signature Recognition",InformationSecuriy Course.

[3] PiotrPorwik,"Some Handwritten Signature parameters in Biometric Recognition Process"Institute of Informatics,Poland.

[4] Anil.k.Jain,"Online Signature Verification ", Pattern recognition 35(2002)2963-2972.

[5] 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.

[6] Bakri, Nurhaniza B. T.; Syed Ahmsinatured, Sharifah Mumtaza h; Shak "Offline digital signature verification using hidden markov mode"l feb-march 2010.

[7] Pradeep Kumar,Shekhar Singh "Hand Written Signature Recognition &Verification using Neural Network" march 2013.

[8] Ashwini Pansare, Shalini Bhatia "Handwritten Signature Verification using Neural Network" January 2012.

[9] H. S. Srihari and M. Beall, "Signature Verification Using Kolmogrov Smirnov Statistic" Proceedings of International Graphonomics Society, Salemo Italy, pp. 152–156, june, 2005.

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