ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 6, Special Issue 5, March 2017

National Conference on Advanced Computing, Communication and Electrical Systems - (NCACCES'17)

24th - 25th March 2017

Organized by

C. H. Mohammed Koya
KMEA Engineering College, Kerala- 683561, India

A Survey on Signature Verification

Fasna T A [1], Dr. Rekha Lakshmanan [2]

P.G. Student, Department of Computer Science and Engineering, KMEA Engineering College, Edathala, India[1]

HOD, Department of Computer Science and Engineering, KMEA Engineering College, Edathala, India[2]

ABSTRACT: The most widely accepted bio-metric for identification and authentication of a person are signatures. Signature verification is a technique used by banks, intelligence agencies and high-profile institutions to validate the identity of an individual. There are various techniques for signature verification, both online and offline. This paper aims at providing detailed overview on different signature verification techniques. Advantages and disadvantages of each method are studied.

KEYWORDS: Forgery, Global Features, Local Features, Preprocessing, Signature Verification.

I. INTRODUCTION

Biometrics is a technology used for analyzing and measuring a person's unique characteristics. Biometrics can be classified into two broad categories, behavioral (handgrip, keystroke dynamics, mouse dynamics etc.) and physiological (iris, hand geometry, fingerprint, ear, face etc.).

The most widely accepted behavioral biometrics for personal identification and verification are Handwritten Signatures. Even with the emerging new technologies, handwritten signature is still continuously used as a means of communication in day to day life as, in a formal agreements, financial systems, government use, marketing documents or paintings etc.

Signatures acts as a strong authentication feature of the signer. As the manual verification of signatures by humans is not easy, an automated Signature verification system is essential in improving the authentication process thereby providing some secure means for authorization of legal documents. The main objective of signature verification system is to discriminate between two classes of signatures-original and forgery. Signature recognition involves identity verification by comparing test signatures with sample signatures in database.

The main difficulty observed in a signature verification process is that individual's signature are not consistent, variation may appear due to signing position, pen width, weight, stress, mood, time etc. Depending on data acquisition method, signature verification can be classified into online and offline verification.

A. ON-LINE

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

B. OFF-LINE

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

II. BASIC CONCEPTS OF SIGNATURE VERIFICATION

The main phases of the signature verification are:
(a) Preprocessing
(b) Feature Extraction
(c) Data Training
(d) Signature verification

Preprocessing: Preprocessing is the sequence of operations applied for the improvement of signature image quality. This improvement in quality of image can increase the accuracy of further steps involved in processing without losing any relevant information. It improves the quality of elements of the digital images called pixels.

Feature Extraction: Feature means similar characteristics and Extraction refers to accurately retrieving those features. A proper feature extraction can increase the recognition ratio. This phase is based on following types of features: Local features, Global features and Transition feature.

Local features describe the properties of signature image in specific parts. They can be calculated by partitioning the signature image into different parts with the help of geometric canter or some other means. Global features describe the entire signature image using the features like width, height, aspect ratio etc. These features are used in combination with other features. They are less sensitive to noise. Transition features counts the transition in the signature image from black to white pixel or vice versa in binarised signature images. It is used in combination with the above features.

Data Training: In this stage, signatures are collected from different individuals for creating a signature database. This collection involves both original and forgery signatures. From these signatures, feature vectors are generated which can act as template for the verification stage.

Signature verification: It is the stage in which individuals are authenticated by comparing their signatures with the features stored in the database as templates.

III. SURVEY

FranckLeclerc and Rejean Plamondon [1] stated that the technique is used for static signature verification. Static signature verification is widely used in the real application, like the automated verification of cheque signatures and signatures on official documents. A signature verification system is designed in the following stages: acquisition, preprocessing, comparison and evaluation. Neural networks obtain results comparable to this approach. The main difficulty in this approach is the necessity of introducing forgers during the training phase. Solutions to this problem are to use networks designated for one class of signers, to use random forgeries or computer-generated forgeries. Another difficulty is the number of signatures needed for the enrolment process.

Donato Impedovo and Giuseppe Pirlo [2] presented the automatic signature verification, with special attention to the most recent advancements. Static systems use offline signature acquisition devices that perform data acquisition after the writing process has been completed. In this case, the signature is represented as a gray level image. Dynamic systems use online acquisition devices that generate electronic representation of data. Online acquisition devices are digitizing tablets. Signature segmentation is a complex task because different signatures produced by the same writer can differ from each other due to several factors like local stretching, compression, omission or additional parts .Two types of features can be used for signature verification: functions or parameters. The authenticity of the test signature is evaluated by matching its features against those stored in the knowledge base developed during the enrolment stage. Automatic signature verification can produce two types of errors: Type I errors concern the false rejections of genuine signatures [false rejection rate (FRR)] Type II errors concern the false acceptance of forged signatures [false acceptance rate (FAR)].

Mostafa I. Khalil, Mohamed Moustafa and Hazem M. Abbas [3] proposed an enhanced technique for on-line signature verification. The distance between two signatures is computed by dynamic time warping (DTW) method. The reference signatures assign special parameters for each signer. Several features are extracted from the signature. Systems with single and multi-features are tested. The experiments have been carried out using the SUSIG online signature database. Global features are average speed, the signature width and height, and total number of samples. Local features include pressure (force) exerted and curvature change between successive points on the signature trajectory. The proposed system is designed to receive five signatures for the reference set per signer. Feature vectors are calculated from each signature. The signature feature vectors are calculated in order to verify a signature with specific signer .These feature vectors are matched with all reference set of this signer.

Michael Brockly, Richard Guest and Stephen Elliott [4] focused on the development of the human biometric sensor interaction model for dynamic signature verification. It is an application of the HBSI model. Behavioral biometrics is more complicated to analyze as they may contain a temporal modification as part of a valid capture interaction. Based on two different signature digitizers, a framework for the development of an HBSI model is outlined . Both devices

enabled the capture of both temporal data as well as an image of the completed signature. Using this data, a signature modality revision to the HBSI model was proposed. The findings in this paper are based strictly on the actions of genuine signers.

Ruben Tolosana, Ruben Vera-Rodriguez [5] described the need for using authentication based on biometric approaches. There are different input devices acting in a device interoperability manner. Focus was on interoperability device compensation for online signature verification. This biometric trait is used in the fields of banking and commercial sector. This approach is based on two main stages. Preprocessing stage is the first stage where data acquired from different devices are processed in order to normalize the signals in similar ranges. The second one is based on feature selection which takes into account the device interoperability case, for selecting robust features. This approach was successfully applied to two common system approaches in online signature verification, i.e., a global features-based system and a time functions-based system. The performance of the proposed global features-based and time functions-based systems applying the two main stages provided an average relative improvement of performance. Finally, a fusion of the proposed systems has achieved a further significant improvement for the device interoperability problem, mainly for skilled forgeries.

S pal,A Alaei,U pal and M Blumenstein [6] worked on the Offline Verification of Banga (Bengali)signatures with the help of a threshold based scheme. Most of the characters of banga signatures are touching, less blocky and presents a more sinuous shape. Signatures were collected from different parts of West Bengal. A Bangla signature database that consists of 2400 genuine signatures and 3000 forgeries were studied. The main techniques used for feature extraction are under-sampled bitmap, intersection/endpoint and directional chain code. The method employed for classification is the Nearest Neighbour method.An average error rate of 15.57% were obtained as the verification result.

Surabhi Garhawal and Neeraj Shukla [7] focused on different Handwritten Signature Verification approaches. Template Matching uses two methods for the detection of skilled forgeries. One method is related to the optimizing matching and the other is based on the elastic matching. For classification two approaches compared are the Resilient Back propagation (RBP) neural network and Radial Basic Function (RBF) Hidden Markov Model. Another method discussed is Fuzzy Logic Based Approaches that has global features of the signature. Statistical approach uses statistical information, the relation, variation, etc between two or more data items. Support Vector Machines (SVMs) are machine learning algorithms that uses a feature space for learning and generalize unseen data. The Idea of structural and syntactic pattern recognition is to provide the patterns by means of symbolic data structures such as strings, trees, and graphs.

Aitor Mendaza-Ormaza, Oscar Miguel-Hurtado, Ramon Blanco-Gonzalo and Francisco-Jose Diez-Jimeno [8] focused on on-line signature verification on portable devices. The database contains data for 25 users, with 28 genuine and 25 skilled forged signatures per user, from 5 different devices. 4 portable devices of different sizes and screen technologies have been used. The 5th device is a traditional digital pen tablet, used as a baseline for results comparison. DTW and SVM, have been used to assess the performance of the signals captured on portable devices. Two experiments using both the algorithms and 5 sub-databases have been done. Results of the first experiment achieve good error rates for random forgeries. Comparing results between algorithms, for the same experiment and database, the DTW algorithm yields better results than the SVM-based algorithm. This was expected, as the DTW performs better than the SVM-based algorithms in traditional on-line biometric verification systems. For the device with bigger screen, higher error rates are due to the discomfort felt by the users. Devices having resistive screens have better error rates than those with capacitive screens. Finding a suitable pen is important for capacitive touch screens. A pen with a rigid thin tip will be desirable for improve the user experience and comfort while signing on portable devices.

IV. CONCLUSION

This paper presents a brief survey of the recent works done on different signature verification techniques. Different existing methods and approaches are discussed. Each method has its own advantages and disadvantages. Lots of work has been already done, still there are many challenges in this research field. So, Future work should be extended by fusion of different classifier for better verification results.

REFERENCES

[1] R. Plamondon and G. Lorette, "Automatic signature verification and writer identification-The state of the art," Pattern Recognit.,vol. 22, no. 2,pp. 107-131, 1989.
[2] D. Impedovo and G. Pirlo, "Automatic signature verification: The state of the art," IEEE Trans. Syst., Man, Cybern. C, Appl. Rev.,vol. 38, no. 5,pp. 609-635, Sep. 2008.
[3] Mostafa I. Khalil, Mohamed Moustafa And Hazem M. Abbas ,“Enhanced DTW Based On-Line Signature Verification”, in 16th IEEE International Conference on Image Processing, pp.2713-2716, Nov 2009.
[4] Michael Brockly, Richard Guest And Stephen Elliott,“Dynamic Signature Verification And The Human Biometric Sensor Interaction Model”, in Security Technology (ICCST) IEEE International Carnahan Conference, pp.1-6,Oct 2011.
[5] R.Tolosana, R.Vera-Rodriguez, J. Ortega-Garcia, and J. Fierrez,"Optimal feature selection and inter-operability compensation for on-line biometric signature authentication," in Proc. IEEE/IAPR Int. Conf. Biometrics (ICB),May 2015.
[6] S.Pal, A.Alaei, U.pal and M.Blumenstein,”Offline Bangla signature verification: An empirical study”, in IEEE/International Joint Conference on Neural Networks(IJCNN), Aug 2013.

[7] Surabhi Garhawal And Neeraj Shukla,"A Study On Handwritten Signature Verification Approaches" in International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 2, Issue 8, August 2013
[8] Aitor Mendaza-Ormaza, Oscar Miguel-Hurtado, Ramon Blanco-Gonzalo And Francisco-Jose Diez-Jimeno, "Analysis Of Handwritten Signature Performances Using Mobile Devices" in Security Technology (ICCST) IEEE International Carnahan Conference, pp.1-6,Oct 2011.