Volume 2, Issue 7, July 2017 ISSN (online): 2456-0006

International Journal of Science Technology Management and Research

Available online at: www.ijstmr.com

Online Signature Verification using DTW Algorithm: A Review

Vinod Rajendra Patil[1]
B.E., Dept. of Information Technology
R. C. Patel Institute of Technology
Shirpur, India

Yogini Ishwar Borse[2]
B.E., Dept. of Information Technology
R. C. Patel Institute of Technology
Shirpur, India

Roshani Rajendra Patil[3]
B.E., Dept. of Information Technology
R. C. Patel Institute of Technology
Shirpur, India

Ms. Punam Patil[4]
Assistant Professor, Dept. of Information Technology
R. C. Patel Institute of Technology
Shirpur, India

Abstract: ***Handwritten signatures are thought as unremarkably accepted biometric for authentication and identification of an individual since every one includes a distinctive signature with its specific behavioural property, thus it's important to prove the genuineness of signature itself. The target of research is to present online handwritten signature verification system based on Dynamic Time Wrapping (DTW) features extraction. This paper presents a simple and efficient method for Online Signature Verification using Dynamic Time Wrapping (DTW) algorithm. The steps for verifying on-line handwritten signature in this system start with extracting pen position data from input signature. Then data is pre-processed and normalized. To enhance the difference between a genuine signature and its forgery wrapping distance is calculated by applying DTW algorithm. Finally output of DTW algorithm is used for obtaining decision about verification result.***

Keywords: Signatures, Biometrics, Online Signature Verification, Dynamic Time Wrapping.

I. INTRODUCTION

Signature recognition is considered as an art: Whereas we may bring objective measures to bear on the problem, in the final analysis, the problem remains subjective. This art is both well studied and well documented as it applies to the verification by humans of signatures whose only records are visual – that is, as it is applied to signatures during whose creation no measurement is made of the pen trajectory or dynamics. We call such signatures, for which we have only a static visual record, off-line, and let us call signatures during whose production the pen trajectory or dynamics or pen-ups is captured, on-line. The attempts to automate the verification of offline signatures have fallen well short in need of human performance to the current purpose, we must prove that automatic on-line signature verification is feasible than offline signature verification [2].

In a break with the tradition, we challenge the notion that the success of online signature verification hinges on the capture of speed or shape of signature during signature production. Whereas speed and shape can help us in on-line signature verification, user should not depend on them completely, or even primarily. If we were indeed unavoidably consistent over the dimensions of time and force when we signed, the use of pen dynamics during signature production over and above that of signature shape would be very useful in detecting forgeries, as dynamic information pertinent to a signature is not as readily available to a potential forger as is the shape of the signature, given just the signatures off-line specimens. However, we have not seen any subjective evidence to the effect that our pen dynamics is as consistent as, or more consistent than the shape of final signature when user signs. Our own test experiments show that we typically exhibit similar temporal variations over the production of similar handwritten curves [5].

Signature recognition is called as behavioural biometric. It can be operated in two different ways[1]:

Static: In this type, the user have to write his signature on the piece of paper, then digitize it through an scanner or a camera, and the recognition system recognizes the shape of signature by analyzing it. This group is often referred as Off-line.

Dynamic: In this type, the user needs to write his signature on pen digitizing tablet, which acquires the signature in real time. Another way is the acquisition by using stylus operated PDAs. Some systems also use smart phones or tablets with a capacitive touch screen, where user have to sign using a finger or an appropriate pen. Dynamic recognition is often referred as On-line.

Usually the dynamic information contains following features in the signature:

- Spatial coordinate x(t),

- Spatial coordinate x(t),
- Pressure p(t),
- Speed s(t),
- Inclination in(t),
- Pen up/ down.

II. LITERATURE SURVEY

There have been two approaches proposed in the literature for signature verification, namely, function-based and feature-based approaches. The former refers to a system where the matching process is done using, directly or indirectly, the original time sequence of the signature. The latter refers to a system where the matching process is done using descriptive features of the signature.

Ralph Niels described a complete biometric algorithm for signature verification based on three stages. Signature is normalized by means of a preprocessing that removes irrelevant information. From this aligned signature the most salient features are extracted and used as input to a GMM model, whose output is used to confirm or deny the users identity [8].

Xiaoyu Song et al. proposed a method of online signature verification based on stable features extracted dynamically. Some useful and effective information of signature features were extracted dynamically depending on individual and studied the result for the some iterations [3].

Mariano Lpez-Garca, et al. described the execution on Field Programmable Gate Arrays (FPGAs) of an embedded system for online signature verification. The recognition algorithm mainly consists of three stages. First, an initial preprocessing is applied on the captured signature, removing noise and normalizing information related to horizontal and vertical positions Afterwards, a dynamic time wrapping algorithm is used to align this processed signature with its template which is previously stored in a database. Finally, a set of features are extracted and passed through a Gaussian Mixture Model, which reveals the degree of similarity between both signatures. The algorithm was tested using a public database of 100 users, obtaining high recognition rates for both genuine and forgery signatures [4].

III. ONLINE SIGNATURE VERIFICATION

The figure below shows the architecture of the online signature verification system.

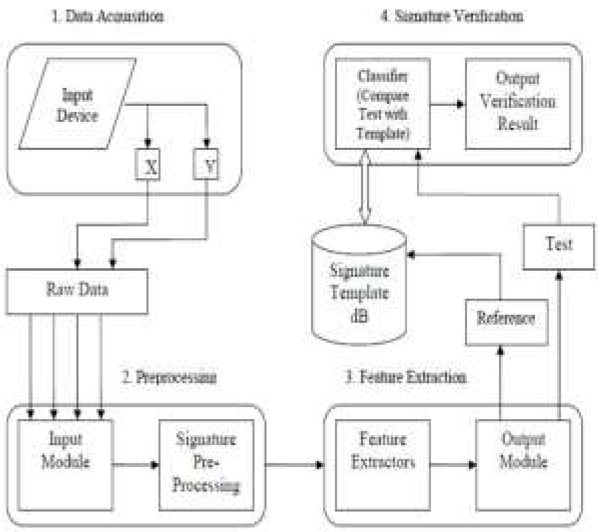

Fig. 1 A general Architecture of Online Signature Verification System

The steps for verifying on-line handwritten signature in this system start with extracting pen position data of points that forming the signature, Pen movement angles are then derived from pen position data. To reduce the variation in pen position and pen movement angles dimensionality, data is preprocessed and normalized. To enhance the difference between a genuine signature and its forgery wrapping distance is calculated by applying DTW algorithm. Finally output of DTW algorithm is used for obtaining decision about verification result.

A. Acquisition

The acquisition of a signature is performed by a specialized input device. In our experiments a commercial pen tablet (i.e. iBall Pen Digitizer) was used to obtain signature images for testing purposes. In this phase we extract pen position data (x, y coordinates) of points that forming the signature, Pen movement angles are then derived from pen position data.

B. Preprocessing

To reduce the variation in pen position and pen movement angles dimensionality, data is preprocessed and normalized. Prior to online signature verification, the user should be familiar with the signature acquisition device and be required to input signature skillfully. Online signature is captured in real-time through acquisition devices with a fixed sampled interval, thus online signatures are represented as time series. There might be noises, distortion and variation during signature acquisition, signatures should be preprocessed before verification. The signature dataset must take some preprocessing since there is no guarantee that different signatures of one user will always be the same. Many methods have been proposed for this phase, which generally consist of smoothing, rotation and normalization of the signature.

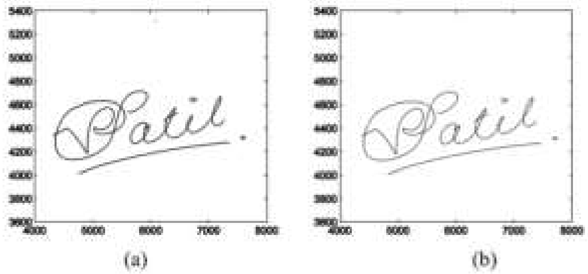

Fig. 2 A Signature Smoothing: (a) Original signature. (b) Signature after smoothing

C. DTW Comparison

Algorithm:

```
int DTWPath(s: array [1...n], t: array [1...m])
{
    DTW = array [0..n, 0..m]
    for i = 1 to n
        DTW[i, 0] = ∞
            for i = 1 to m
             DTW[0, i] = ∞
             DTW[0, 0] = 0
             for i = 1 to n
                 for j = 1 to m
                     cost := d(s[i], t[j])
                     DTW[i, j] = cost + min(DTW[i-1, j ],
                     DTW[i , j-1],
                     DTW[i-1, j-1])
    return DTW[n, m]
}
```

For Dynamic Time Warping to effectively compare two signature curves, they need to be represented as discrete and online. A curve is represented by unique ID, whose first character is the label, and is followed by a number specifying the number of points in given curve. Then the points (each consisting of an X and Y coordinate) are listed, in the order they were produced and the first listed point is also the starting point of the curve. A matching path technique basically follows the next steps to calculate the distance between two curves hence a matching path needs to be created.

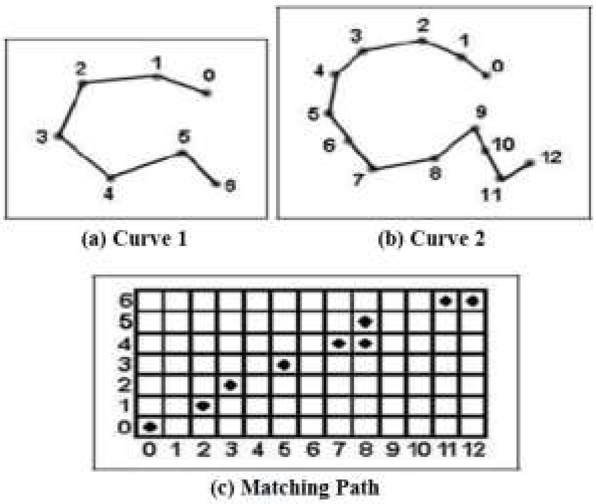

Fig. 3 Constructing Wrapping Path

A matching path is a list of combinations of the points of the first curve and the points of the second curve. The technique used for the creation of this list is what distinguishes different matching-path using methods, of which DTW is one. A detailed description of the creation of the matching path by the DTW-algorithm as mentioned above. For each of the combinations of points i, j in the matching path, the distance D(i,j) between them is calculated. Various methods for calculating the distance between two points exist. The distances calculated in the previous step are summed and this total distance is normalized by divided it by the number of combinations in the matching path. The resulting value is the distance between the curves [7].

IV. VERIFICATION

To verify a test signature T, the similarity measures of T with each of training signatures in database belonging to the ith person is calculated and the mean value of these similarities are considered as the similarity of Y with the template signatures. We call it S_i. To accept or reject test signature Y which is claimed to be belonged to the ith person, if the condition of $S_i > T_i$ is satisfied, then the input signature will be verified, otherwise, it will be rejected[8].

Fig. 4 Result of Verification as Genuine Signature

V. EXPERIMENTAL ANALYSIS

Experiments are carried out on the database of 10 users each of which include 10 genuine and 10 forged signatures. It was found that given a number of signatures, the system is able to detect fake signatures with an average accuracy of 90.4%.

TABLE I
Testing Result

No of Users	**Signature Type**	**Genuine**	**Verification Rate (%)**
1	Genuine	Yes	89
2	Genuine	Yes	94
3	Genuine	Yes	91
4	Genuine	Yes	83
5	Genuine	Yes	92
6	Genuine	Yes	96
7	Genuine	Yes	88
8	Genuine	Yes	94
9	Genuine	Yes	87
10	Genuine	Yes	90
		Average	**90.4**

Table 1 calculates the average accuracy of the system when tested against signatures of various users and the situations when the signature is verified and not verified.

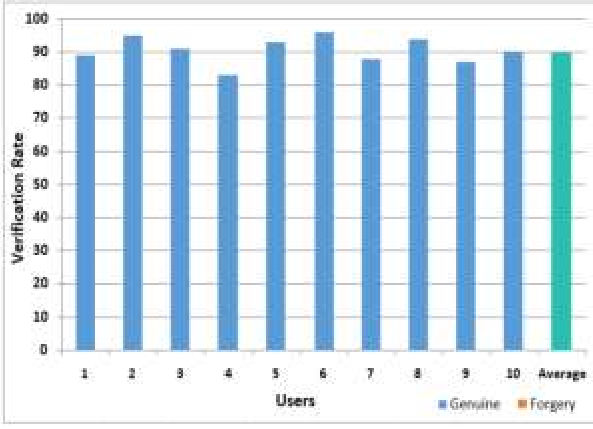

Fig. 4 Graph of Testing Analysis

CONCLUSION

In this paper we proposed a simple and effective Online Signature Verification system. It shows that Online Signature Verification system using DTW algorithm is an efficient approach for signature verification. Practice demonstrates that the Pen-Tablet system can also draw the sophisticated signatures as pen does and also gives the accurate result. Future prospect of the project includes improving the accuracy of the system by updating reference set of signatures over the specific time of period. However Signature verification System alone is not enough to provide strongest authentication mechanism. We can couple it with another biometric authentication technique to provide strongest mean of authentication.

REFERENCE

1. G. Rigoll, A. Kosmala, "A Systematic Comparison Between On-Line and OffLine Methods for Signature Verification with Hidden Markov Models", Gerhard Mercator-University Duisburg, Germany, 2013.
2. Kanawade M. V., Katariya S. S. "Review of Offline Signature Verification and Recognition" International Journal of Emerging Technology and Advanced Engineering, Volume 3, Issue 7, July 2013.
3. Xiaoyu Song, Xinghua Xia, and Fangjun Luan, "Online Signature Verification Based on Stable Features Extracted Dynamically", IEEE Transactions on Systems, Man and Cybernetics Systems, 2168-2216, April 2016.
4. Mariano Lpez-Garca, Rafael Ramos-Lara, Oscar Miguel- Hurtado, and Enrique Cant Navarro, "Embedded System for Biometric Online Signature Verification", IEEE Transactions on Industrial Informatics, VOL. 10, NO. 1, Feb 2014.
5. https://en.wikipedia.org/wiki/Signature_recognition.
6. https://en.wikipedia.org/wiki/Dynamic_time_warping.
7. Al-Naymat G., Chawla, "Toward Accurate Dynamic Time Warping in Linear Time and Space", International Journal of Advanced Research in Computer Engineering Technology (IJARCET), 2012.
8. Ralph Niels, "Dynamic Time Wrapping: An intuitive way of handwriting recognition", Department of Artificial Intelligence / Cognitive Science, Nijmegen, the Netherlands, 2004.
9. Stan Salvador Philip Chan, "Fast DTW: Toward Accurate Dynamic Time Warping in Linear Time and Space", KDD Workshop on Mining Temporal and Sequential Data, pp. 70-80, 2004.
10. Toai Q.Ton, Tung Thanh Pham, "Online Signature Verification Using Dynamic Time Wrapping and Extended Regression", International Journal of Advanced Research in Computer Engineering Technology (IJARCET) Volume 4, Issue 5, May 2015 Tavel, P. 2007 Modeling and Simulation Design. AK Peters Ltd.
11. Vishvjit S Nalwa, "Automatic On-Line Signature Verification", Bell Laboratories, Holmdel, NJ. Proceedings of IEEE, 85(2), pp. 213-239, 1997.

.