Online Handwritten Signature Verification System using Time Sequence Algorithm

Abhilash Roy, Ashutosh Kumar, Komal Wankar, Sagar Yelne, Shreenarayan Sinha

*Students of Final Year, Department of Computer Technology, K.D.K. College of Engineering, Nagpur, India.*

**Abstract**

A new online handwritten signature verification algorithm is proposed. The proposed method divide the time functions into several segments which describing regional properties. And then a exact segment-to-segment mapping is found by a modified DTW method. Thus the proposed method utilized the dynamic features of signatures, which ensured the high security of identification systems. Furthermore, the proposed algorithm need not know any information about the characteristics of the forgeries, the decision boundary is constructed wholly according to the the obtained segment-to-segment mapping information in enrollment procedure. The proposed algorithm is tested on two separate signature verification tasks using two different signature databases, and the experimental results show affectivity of our algorithm. It also shows competitive performance of the proposed algorithm in comparison with other approaches. The fact that the signature is widely used as a means of personal verification emphasizes the need for an automatic verification system. Verification can be performed either Offline or Online based on the application. Online systems use dynamic information of a signature captured at the time the signature is made. Offline systems work on the scanned image of a signature. We have worked on the Online Verification of signatures using a set of segment-to-segment mapping features.

**1. Introduction**

Signature has been a distinguishing feature for person identification through ages. Signatures for long have been used for automatic clearing of cheques in the banking industry. Despite an increasing number of electronic alternatives to paper cheques, fraud perpetrated at financial institutions in the United States has become a national epidemic.

Since commercial banks pay little attention to verifying signatures on cheques mainly due to the number of cheques that are processed daily a system capable of screening casual forgeries will prove beneficial. Most forged cheques contain forgeries of this type. We in our project have tried developing a robust system that automatically authenticates documents based on the owner’s handwritten signature.

Approaches to signature verification fall into two categories according to the acquisition of the data: On-line and Off-line. On-line data records the motion of the stylus while the signature is produced, and includes location, and possibly velocity, acceleration and pen pressure, as functions of time. Online systems use this information captured during acquisition. These dynamic characteristics are specific to each individual and sufficiently stable as well as repetitive. Off-line data is a 2-D image of the signature.

Processing Off-line is complex due to the absence of stable dynamic characteristics. Difficulty also lies in the fact that it is hard to segment signature strokes due to highly stylish and unconventional writing styles. The non-repetitive nature of variation of the signatures, because of age, illness, geographic location and perhaps to some extent the emotional state of the person, accentuates the problem. All these coupled together cause large intra-personal variation. A robust system has to be designed which should not only be able to consider these factors but also detect various types of forgeries. The system should neither be too sensitive nor too coarse. It should have an acceptable trade-off between a low False Acceptance Rate (FAR) and a low False Rejection Rate (FRR).

**2. Literature Survey**

Currently a lot of different approaches have been proposed for online signature verification in the literatures. They can be broadly classified into two groups: approaches based on the parametric features and ones based on the functions . In the parametric approaches, only a set of global features derived from the complete signature are compared. Although it has lower computational complexity and the advantage of being very fast, the error rates are generally high. In the function-based approaches, a signature is represented as a signal function of time. And the time functions of different signatures are compared directly in accordance with correlation or elastic distance. This kind of approaches retain more information of the signing process than the global parametric approaches and acquire lower error rates. However, because different signatures have different signal duration and non-linear distortions, it is difficult to ensure the matching points between signatures is exact.

Xia, Boncelet, and Arce proposed a digital signature scheme based on the Discrete Wavelet Transform (DWT). The watermark, modeled as Gaussian noise, was added to the middle and high frequency bands of the image. The decoding process involved taking the DWT of a potentially marked image. Sections of the watermark were extracted and correlated with sections of the original watermark. If the cross-correlation was above a threshold, then the watermark was detected. Otherwise, the image was decomposed into finer and finer bands until the entire, extracted watermark was correlated with the entire, original watermark. This technique proved to be more robust than the DCT method when embedded zero-tree wavelet compression and halftoning were performed on the watermarked images.

Improvements on the above schemes were possible by utilizing properties of the Human Visual System. Bartolini et al. first generated a watermarked image from DCT coefficients. Then spatial masking was performed on the new image to hide the watermark. Kundur and Hatzinakos embedded the watermark in the wavelet domain. The strength of the watermark was determined by the contrast sensitivity of the original image. Both techniques showed resistance to common signal processing operations. Delaigle et al. proposed a unique watermarking scheme based on the Human Visual System. Binary m-sequences were generated and then modulated on a random carrier. This image served as the watermark, and then it was masked based upon the contrast between the original signal and the modulated image. The masked watermark was added to the original image to form the watermarked image. Their technique was robust to additive noise, JPEG coding, and rescanning.

**3. Implementation**

**System Architecture:**



Segmentation is one of the most difficult problems and it is also so important that it should be considered separately. There are many techniques about segmentation reported in the literature. Immunity to intra-signer variations offers the greatest challenge to most techniques applied. In this project, a novel algorithm is proposed to yield consistent and reliable results for different signature instances of a signer. Signatures include many smooth curve elements other than line segments and sharp angle elements. Important information about individuals’ biometric features is included in signatures . They change from one to another instance, but the forged signatures deviate much bigger than the genuine. In order to analysis these smooth curve elements, segments signatures at relatively non-complex shape. In this paper, a novel algorithm is also proposed to analysis them. First, divide the input signature to several segments using HMM. Then, combine two conjoint segments together to form a long segment and get its spectral and tremor information using FFT. At last, accept it or reject it based on the distance between the spectral and its prototype. In addition, a novel initialization algorithm is used to avoid local optimal of the re-estimation algorithm and at meantime a novel algorithm is also proposed to retain the important information at the cusps. An on-line signature sample consists of a sequence of sample points that contains variety of features, e.g. pen position and pen-tip pressure, depending on the data acquisition device. Based on these features directly extracted from original sample, more complex features can be computed, e.g. pen velocity, acceleration, moving direction

, etc.

To represent an on-line signature S, which contains N sample points, with a graph, firstly, each sample point is seen as a node of a graph, i.e. S = {v1, v2, ..., vN}. Most of the on-line signature acquisition devices are able to directly extract features of x-position, y-position and pressure at sample points. We denote these features at vi as xi, yi and pi. Secondly, certain features are chosen to be the weight of nodes and edges. As discussed above, weight of nodes should be local features that describe properties of sample points, while weight of edges describes relationship between nodes.

Therefore, a signature can be represented by a N×N metric

**4. Algorithm of verification**

The algorithm of verification includes preprocessing, feature extraction, time Sequence match, similar degree calculating and verification.

4.**1. Preprocessing**.

Preprocessing is to delete virtual pen-up. The main reason of virtual pen-up is not keeping enough pressure of the pen all through the signing. When the pressure of the pen point is less than minimum pressure which the tablet can detect, it causes virtual pen-up. Generally, in the process of signing, the pressure of the signature segments is always large at two endpoints or turning point, at which speed of signing is slow. So virtual pen-up occurs in the middle of straight segments, which is called straight virtual pen-up. If virtual pen-up occurs at the turning point of the signature segments, it is called turning virtual pen-up.

**4.2. Feature extraction**.

With a fixed sample frequency, a signature can be de-scribed by a series of points *{X* (*t*) *, Y* (*t*) *}* where *X* (*t*) *,Y* (*t*) are x- and y coordinates in the signing.

*vx* =*X*(*t*)

*vy* =*Y*(*t*)

Where, *vx, vy* are the speed in x- and y- coordinates.

**4.3. Time sequence match**.

There are always some stops in the process of signing. Sample signature defines a time sequence, so does every test signature. How to match time sequence of test signature with that of sample signature quickly determines the efficiency of the algorithm.

With time sequence, sample signature *S* can be defined as S = S0, S1, …., *Si,…, SM*, where, *Si* is the ith stroke of sample signature and *M* is the total strokes of sample signature. Test signature *T* can be defined as *T* = *T*0*, T*1*,… ,Tj ,… , TN*,where, *Tj* is the jth stroke of test signature and *N* is the total strokes of test signature. Generally, *M 6*= *N*. Before comparing test signature with sample signature, we must find the stroke relations between test signature and sample signature. For the continuous strokes and virtual pen-up and some other disturbs, the stroke relations of test signature and sample signature is not always one to one, but many to one, one to many, and many to many. In order to find the optimum corresponding relations, this paper presents a time sequence match algorithm of the large stroke. It overcomes the influence of the standardization of the coordinate in other time sequence match algorithms [9]. The algorithm is effectual to be examined. The large stroke is relatively stable in the signature from the research. This algorithm is based on similar characters of pressure changes, especially the large stroke in time sequence match.

We choose the largest strokes from sample and test signature, where, *n* (*· min* (*M,N*) *-* 1). Set *n* = 2. If they are similar in pressure, they are considered as the broken points. The flow of the algorithm is shown as follows:

**Algorithm :**

Time Sequence Match Algorithm:

Step 0: *n* = 2.

Step 1: If *n > min* (*M;N*) *¡* 1, time sequence match fails.

Step 2: Compute the serial number similarity degree of the corresponding largest strokes. If the similarity degree is less than the threshold, go to step 6, else go to next step.

Step 3: Compute the pressure similarity degree of the corresponding largest strokes. If the similarity degree is less than the threshold, go to step 6, else go to next step.

Step 4: The largest strokes are considered as the broken points. If the stroke number is the same in every pile, time sequence match succeed, otherwise go to next step.

Step 5: If there are some strokes that can be combined, combine them and go to step 4, else go to step 6.

Step 6: *n* = *n* + 1. Go to step 1.

**4.4. Similarity degree calculating**.

After time sequence match, a function on the strokes between test signature and sample signature can be found: *f* : *T ! S*. *f* meets the following condition: any stroke*Tj* in the test signature *T* corresponds to only one stroke *Rj* = *f*(*Tj*)in the sample signature *S*with the function *f; Rj* is the corresponding stroke of *Tj* . Similarity degree calculating can't be separated as stroke combination, time transform, and distance calculation.

**4.5. Stroke combination**.

There are many kinds of stroke relations between test signature and sample signature, such as many to one, one to many, and many to many. It is necessary to design an algorithm for the stroke combinations. Linear inserting value method using time as the independent variable can be used to join the character data of a stroke end point with the next stroke starting point. Because the captured interval time is fixed on the tablet, character data can be added to the point where there are no sample points.

**4.6. Verification**.

So we can define the inequality as following:

*di f* (*F,G*) *< £*0

where *£*0 is the threshold.

If *di f* (*F, G*) is less than the threshold, we reject it as a forger, otherwise, accept it as a genuine signature.

**5. Conclusion**

In this project, a new segment-to-segment method based a modified DTW technique is proposed for signature verification. The main contribution of our method is to consider the geometric properties of a signature in recognition problem, using the segmental dissimilarity scores for verification. Thus the proposed method utilized the dynamic features of signatures, which ensured the high security of identification systems. Furthermore, the proposed algorithm need not know any information about the characteristics of the forgeries, the decision boundary is constructed wholly from the signatures in enrollment procedure. Also, experimental results demonstrated good performance of the proposed algorithm.

**6. References**

[1] J. Yi, C. Lee and J. Kim, ”Online signature verification usingtemporal shift estimated by the phase of gabor filter”, IEEE Transactions on Signal Processing, 2005, pp 776-783.

[2] R. Plamondon, S.N. Srihari, ”On-line and off-line handwriting recognition: A comprehensive survey”, IEEE Trans. Pattern Anal. Machine Intell., 2000, pp 63-84.

[3] J. Fierrez, J.O. Garcia, D. Ramos, J.G. Rodriguez, ”HMMbased on-line signature verification: Feature extraction and signature

[4] D. Impedovo and G. Pirlo, “Automatic signature verification: the state of the art,” IEEE Trainsactions on System, Man and Cybernetics - Part C: Applications and Reviews, vol. 38, no. 5, pp. 609–635, 2008.

[5] A. Kholmatov and B. Yanikoglu “Identity authentication using improved online signature verification method,” Pattern Recognition Letters, vol. 26, pp. 2400–2408, 2005.

[6] M.Wirotius, J.-Y. Ramel, and N.Vincent, “election of points for on-line signature comparison,” in The 9th International Workshop on Frontiers in Handwriting Recognition, 2004, pp. 503–508.

[7] H. Lei, V. S. Palla, and G. ER, “An intuitive similarity measure for on-line signature verification,” in The 9th International Workshop on Frontiers in and writing Recognition, 2004, pp. 191–195.

[8] R. Kashi, J. Hu, and W. Nelson, “A hidden markov model approach to online handwritten signature verification,” in International Journal on Document Analysis and Recognition, 1998, pp. 102–109.

[9] C. T.Wessels, “A hybrid system for signature verification,” in International Joint Conference on Neural Networks, 2000, pp. 509–514.