A Review of Online Signature Verification using Velocity Parameter

Rahul[1], K. S. S. K. Karthikeya[2]

[1,2]Student, Dept. of Electronics and Telecommunication, Thakur college of Engg. and Tech., Mumbai, India

***Abstract*: Signature verification has its importance in many fields today including, but not limited to, banking and customer services, Legal issues and complete and comprehensive biometric profile of a human being. There are two methods for signature verification i.e. the Online and the Offline signature verification. Offline method scans the signature and then proceeds to analyze it meaning it is static system. On the other hand, Online Signature Verification performs real time analysis while the user is signing using a signature pad. Online Signature verification has a much better forgery tolerance than offline method. Different methods have been used in the past to implement the system like Hidden Markov Model (HMM), Support Vector Machine (SVM), Dynamic Time Warping (DWT) and Neural Networks. Each of them has a distinct and unique advantage when used for the signature verification purpose. Dynamic Time Warping was one of the first methods used and is gaining traction again in recent times. HMM is a popular method because of its ability of providing a good recognition of spatio-temporal pattern such as signature. Neural Networks have also shown promise in recent times since they have good fault tolerance and can work with incomplete data.**

***Keywords*: HWT, HMM, SVM, neural networks.**

1. Introduction

For a long time, signature verification has been used for the authentication purposes in the Banking transactions, contract documents and other authenticate materials. The classification of biometrics can be done into two broad categories, Behavioral (signature verification, keystroke dynamics, handwriting, speech etc.) and Physiological (face, iris, fingerprint, retina etc.) [1], [2]. Signatures are composed of special characters and therefore most of the time they can be unreadable. Also, intrapersonal variations and interpersonal differences make it necessary to analyze them as complete images and not as letters and words put together [1]. As signature is the primary mechanism both for authentication and authorization in legal transactions, the need for research in efficient auto-mated solutions for signature recognition and verification has increased in recent years. Recognition is finding the identification of the signature owner whereas Verification is the decision about whether the signature is genuine or forged. There are two types of signature verification that are online and offline. In offline, users write their signature on paper, digitize through an optical scanner or a camera, and the biometric system recognizes the signature analyzing its shape, length, height etc. but in online signature verification it also measures pressure applied by users, Speed of writing, inclination of pen along with the signature image obtained in the offline signature.

We obtain the signature database using a Wacom Intuous Pro pressure pad and a digital pen, we also obtain dynamic information of the signature. This dynamic information generates online signature; each dynamic information is a function according to time of signing process. The signing process generates a set of the data function over time. Because dynamic information is more difficult to forge than the image of the signature, the online signature gives more authenticity to the system [3].

Fig. 1. Wacom Intuous Pro pressure pad and a digital pen

The classification of biometrics can be done into two broad categories, Behavioral (signature verification, keystroke dynamics, handwriting, speech etc.) and Physiological (face, iris, fingerprint, retina etc.). Human Signature is proven to be the most natural, widely accepted biometric attribute of a human being which can be used to authenticate human identity and is even less intrusive and has no negative or undesirable health connotations. Signatures are composed of special characters and therefore most of the time they can be unreadable. Also, intrapersonal variations and interpersonal differences make it necessary to analyze them as complete images and not as letters and words put together. As signature is the primary mechanism both for authentication and authorization in legal transactions, the need for research in efficient auto-mated solutions for signature recognition and verification has increased in recent years. Recognition is finding the identification of the signature owner whereas Verification is the decision about whether the signature is genuine or forged. There are two types of signature verification that are online and offline. In offline, users write their signature on paper, digitize through an optical scanner or a camera, and the biometric system recognizes the signature analyzing its shape, length, height etc. but in online signature verification it also measures pressure applied by users, Speed of writing, inclination of pen along with the signature image obtained in the offline signature [1], [2], [5].

A. HMM (Hidden Markov Model)

HMMs have been used in a multitude of application areas such as signal processing, speech recognition, pattern recognition and is successfully implemented in signature verification as well. HMM is an effective statistical modeling approach in which an observable sequence is generated by the underlying process. HMM, a generalization of Markov Model is a robust method for modeling the variability of distinct time random signals if the time information is accessible. Since, HMM can handle time duration signals variation, for instance, signatures speech etc., it is prominent for signature and speech recognition applications. In HMM, the division of signing process into multiple states is made that makes up a Markov chain [4], [5]. A sequence of probability distributions of the different features are taken that are implied in the verification task and matching is performed on it. Signature's likelihood is the measure used in these verification systems to determine the verification score which is then normalized to get a threshold value. It shows whether a given signature (test) is genuine or forged. The model using HMM in signature verification consist of States (genuine or forged) and Observations (x, y coordinates, pressure etc.). The drawback of applying HMM in signature verification is that it needs huge features to be set in huge number. Also, the amount of data in training the model is very large thus resulting in a very high time complexity. Adding additional parameters such as speed, acceleration, mass center, inertia axis, linear and circular segments length, curvature radii, etc. would result in a large EER improvement of the system, satisfying commercial requirements [4]-[6].

B. SVM (Support Vector Machine)

The Support vector machines (SVMs) is one of the learning models, it is used for classification and regression analysis.

In this learning model the data points are represented as points in space. It is represented in such a way that the points obtained from different categories are separated by a plane called hyperplane. New data is mapped into same space and their location which is like the plane, it is used to predict which categories each of the point belongs to, with the plane that are belonged to the decision boundary. In the case where the decision boundary needs to be non-linear i.e. where classes which cannot be separated through a straight line, SVM also could project the space by a function which is non-linear in nature, lifting the data to a space with a higher dimension where a linear decision boundary do work of separating classes [10].

An SVM classifies data through finding the best hyperplane that separates all data points of one class by those of the other class. The best hyperplane for an SVM is the one with the largest margin between the two classes. Margin is the maximal width of the slab parallel to the hyperplane that do not have any interior data points.

In the one-class SVM, the support vector model is to be trained on data that consist of only one class, which is the "normal" class. It inherits the properties of normal cases and from these properties we can predict which examples are unlike the normal examples [10].

That is in our case, we have only genuine signature and the model is trained depending on this training data. It will infer properties of genuine signature and while testing it will check whether the sample has the properties same as the genuine signature and depending on that then it will identify that whether the signature is genuine, or it is forged [10].

C. DTW (Dynamic Time Warping)

DTW is a very popular technique for implementing signature verification. This method determines the similarity between two time varying sequences. DTW can efficiently determine the most optimal distance between two sequences even if the accelerations of these time varying patterns are different. The most important feature of DTW is its ability to compute fast which makes it the most popular method in signature verification. It does not require huge data for training. It simply takes two sequences of time varying data or features and compares them and finds an optimal similarity between the two-sample set. DTW uses a dynamic programming strategy that can manage the variability on the signatures length. In this method two signature samples are taken as sequences where points are taken in different discrete times. S={s1,s2,…,sn}, T={t1,t2,…,tm} are two time varying sequences that represents the value of the features at 1st,2nd and nth time. S is the sample signature stored in the database and T is the test signature sample. The time complexity of DTW is O(n2) where n is the number of points in the sequence. Although DTW is a fast technique but if the points taken on the sequence is very large then the time taken to compute the results in DTW becomes very high and therefore a variation of DTW i.e. VQ-DTW is used. VQ stand for vector Quantization. In this method clustering of some points that are in the same region are clustered together thus reducing the time complexity of algorithm [9].

D. Neural networks

A neural network is an information processing system. It consists of massive simple processing units with a high degree of interconnection between each unit. The processing units work cooperatively with each other and achieve massive parallel distributed processing. The design and function of neural networks simulate some functionality of biological brains and neural systems. The advantages of neural networks are their adaptive-learning, self-organization and fault-tolerance capabilities. For these outstanding capabilities, neural networks are used for signature verification applications. Some of the best neural models are back-propagation, high-order nets, time-delay neural networks and recurrent nets [8], [11].

Normally, only feed-forward networks are used for signature verification. Feed-forward means that there is no feedback to the input. Like the way that human beings learn from mistakes, neural networks also could learn from their mistakes by giving feedback to the input patterns. This kind of feedback would be used to reconstruct the input patterns and make them free from error; thus, increasing the performance of the neural networks. Of course, it is very complex to construct such types of neural networks. These kinds of networks are called as auto associative neural networks. As the name implies, they use back-propagation algorithms. One of the main problems associated with back-propagation algorithms is local minima. In addition, neural networks have issues associated with learning speed, architecture selection, feature representation, modularity and scaling. But one of the advantage of Neural Network is its ability to generalize the new data and having a good fault tolerance [11].

2. Data acquisition and pre-processing

Data acquisition is required to acquire the signature of the user which can be based on a variety of input tools. Data acquisition process is a process where the real time inputs of signature from the digitizing tablet and the special pen are read into the CPU for processing and to store the signature in the database which called Signature database. The digitizing tablet is sending the real time inputs to the CPU for further processing and storage. Electronic pens are generally used for detecting position, velocity, acceleration, pressure, pen inclination, and writing forces. Some input devices use ink pen, which is exactly like using a conventional pen on standard paper positioned on the tablet. In this case, the pen produces conventional handwriting using ink, while producing an exact electronic replica of the actual handwriting [5], [7].

Pre-processing techniques used with online signature's features vary a great deal and may involve noise reduction, normalization, alignment, segmentation, translation, rotation and scaling invariant transformations. In, Gaussian filtering is used for noise reduction, while in, signature normalization is realized by employing Fourier Transform. Alignment based on the mass centre and the principal axis of inertia is applied in. Length-, time-based or pen up are some of the examined options for signature segmentation. More advanced techniques, such as those based on signatures geometric characteristics, mainly use geometric extreme points [5].

In the preprocessing phase, generally the input data is based on techniques originating from standard signal processing algorithms. Typical preprocessing algorithms involves filtering, noise reduction, and smoothing. Fourier transform, mathematical morphology, and Gaussian functions are generally used for the preprocessing phase.

An important preprocessing step, of signature verification, is segmentation. It is a complex task since different signatures produced by the same writer can differ from each other due to local stretching, compression, omission or additional parts. Due of this, specific attention has been devoted to signature segmentation, and several techniques have been proposed. In general, some segmentation techniques derive from specific characteristics of handwritten signatures and reflect specific handwriting models. Some segmentation techniques are pen-up/pen-down, angular and curvilinear velocity [5], [8].

3. Feature extraction

One of the most important processes in signature verification is feature extraction. Since, the data in online signature verification is represented as a series of points, features are extracted from a sequence of points. After pre-processing, features such as x & y coordinates, pen status, pressure etc. are extracted from the input signatures for each segment. New features such as velocity of x (vx) and velocity of y (vy) etc. can be derived from these signatures. The features that are not reverse engineered by any imposter, & maximize the interpersonal variability and minimize the intrapersonal variability, need to be selected and saved in the database as reference signature along with the calculated threshold value [10].

Normally Parameters are classified into two main categories: global parameters and local parameters. Global parameters concern the whole signature. The typical global parameters are total time duration of a signature, number of components, global orientation of the signature, coefficients obtained by mathematical transforms, number of pen lifts, etc. Local parameters concern features extracted from specific parts of the signature. It depends on the level of detail considered, local parameters can be divided into component-oriented parameters, which are extracted at the level of each component (i.e., height to width ratio of the stroke, relative positions of the strokes, stroke orientation, etc.), and pixel-oriented parameters, which are extracted at pixel level (i.e., grid-based information, pixel density, grey-level intensity, texture, etc.).

Generally Position, velocity, and acceleration functions are used for online signature verification. Position, velocity, and pen inclination functions are consistent features in online signature verification, when a distance-based consistency model is applied. This model starts from the consideration that the characteristics of a feature must also be estimated by using the distance measure associated to the feature itself [8].

But recently pressure and force functions are widely becoming popular and specific devices have been developed to capture these functions directly during the signing process. Pressure information can be registered with respect to various velocity bands. It has been exploited for signature verification in order to take advantage of inter feature dependencies.

A. Database

There are multiple database available for signature verification, one such database is.

SUSIG: It is a new online signature database which is available for use in developing or testing signature verification systems. The SUSIG database consists of two parts, collected

Table 1
Comparison of the techniques

Techniques	Attributes		
	Advantages	Disadvantages	Appropriateness in signature Verification
Hidden Markov Model (HMM)	HMM can manage signals of different time durations.	If samples are less in number, it does not perform well	Because HMM is computationally less complex, it is very popular and gives quite accurate results.
	Can be trained automatically		
	It is computationally less complex		
Support Vector Machine (SVM)	It has Good Generalization Properties	Direct decision problem cannot be extended to multi class problem	Since it is a direct decision problem and signature verification is also a direct decision problem that either the signature belongs to genuine class or forgery class therefore it is appropriate for signature verification problem.
	Convex objective function with efficient training algorithm	In SVM training time is quite long	
	SVM is good for smaller number of training samples	Parameter selection is also quite difficult	
Neural Networks	It has the ability to work with incomplete knowledge and has a good fault tolerance.	Complexities increase with increase in neurons. Also, it is computationally expensive.	A neural network can create its own interpretation of the input data thus making it useful for signatures which have interclass variations
Dynamic Time Warping	Robust distance measurements are for accurate pattern classification	Memory space problem	This method can be effectively applicable to this problem since this would not require too many samples of input signatures to be stored and nonlinear time variations that persists even for genuine signatures can be reduced.
	Non-linear time variations of time series are reduced	If training data is too large, performance of DTW degrades	
	DTW is Fast	Each sample must have its own reference template	

using different pressure sensitive tablets.

The SUSIG database consists of two parts: Visual and Blind subcorpora. Signatures in the Visual subcorpus were collected using a pressure sensitive tablet with built in LCD display such that people could see their signatures while signing. On the other hand, no visual feedback was available for the Blind subcorpus.

The Blind subcorpus was collected approximately 4 years before the Visual subcorpus; as a result, the people who donated to the two subcorpora are largely different. However, the people who donated signatures are from the same demographics, resulting in similar signature complexity.

The Visual subcorpus, which is collected with a tablet with built-in LCD display, consists of signatures donated by 100 unique signers (29 women & 71 men). Most of the signers were students & faculty members of Sabanci University with ages varying between 21 and 52 years old. Each subject was briefly informed of the purpose of the data collection without further information about the working principles of an online signature verification system. A total of 10 skilled forgeries (5 skilled and 5 highly skilled) were collected for each person in the Visual subcorpusa total of 10 skilled forgeries (5 skilled and 5 highly skilled) were collected for each person in the Visual subcorpus.

The Blind subcorpus was collected prior to the Visual subcorpus and is named after the fact that the collection was done on a tablet without LCD display. The subcorpus consists of signatures donated by 100 individuals (25 women & 65 men), most of whom were students & faculty members of Sabanci University, with ages varying between 20 and 50 years old.

4. Conclusion

This paper provides an overview of some popular methods used in signature verification like HMM, SVM and Neural Networks. The advantages and disadvantages of these methods are given, it gives an estimate of which method should be used in which case. HMM performs stochastic matching of a model and a signature using a sequence of probability distributions of the features along the signature. After going through literature and research papers, we have concluded that a Hidden Markov Model operates at the best efficiency for signature verification at 6 States and 32 Symbols. It is evident from different papers that hidden markov model method is worthy of further research in order to obtain better performance.

References

[1] Akondi Vyasa Bharadwaja, “The Analysis of Online and Offline Signature Verification Techniques to Counter Forgery,” in Indian Journal of Science and Technology, vol. 8, no. 20, pp. 1-7, August 2015.

[2] Franck Leclerc and Rejean Plamondon, “Automatic Signature Verification: The State of the Art-1989-1993, Canada.

[3] Bryan Found Netherlands Forensic Institute, The Hague, The Netherlands and Forensic Science Institute, Ministry of Justice, Shanghai, China presented Signature Verification Competition for Online and Offline Skilled Forgeries.

[4] Igarza J.J., Goirizelaia I., Espinosa K., Hernáez I., Méndez R., Sánchez J. (2003) Online Handwritten Signature Verification Using Hidden Markov Models. In: Sanfeliu A., Ruiz-Shulcloper J. (eds) Progress in Pattern Recognition, Speech and Image Analysis. CIARP 2003. Lecture Notes in Computer Science, vol. 2905. Springer, Berlin, Heidelberg.

[5] K. Barkoula, G. Economou and S. Fotopoulos, “Online signature verification based on signatures turning angle representation using longest common subsequence matching,” International Journal on Document Analysis and Recognition, vol. 16, no. 3, pp. 261-272, September 2013.

[6] L. Yang, B.K. Widjaja, R. Prasad, Application of hidden Markov models for signature verification, Pattern Recognition, Volume 28, Issue 2, 1995, Pages 161-170.

[7] D. Impedovo and G. Pirlo, "Automatic Signature Verification: The State of the Art," in *IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews)*, vol. 38, no. 5, pp. 609-635, Sept. 2008.

[8] Igarza, Juan Goirizelaia, Iñaki Espinosa, Koldo Hernáez, Inmaculada Méndez, Raúl and Sanchez, Jon. (2003). Online Handwritten Signature Verification Using Hidden Markov Models, pp. 391-399.

[9] M. Bashir and J. Kempf, "Area bound dynamic time warping based fast and accurate person authentication using a biometric pen," Digital Signal Processing, 2012.

[10] E. Frias-Martinez, A. Sanchez and J. Velez, "Support vector machines versus multi-layer perceptrons for efficient off-line signature recognition," Engineering Applications of Artificial Intelligence vol. 19 pp. 693–704, March 2006.

[11] D. Bhattacharyya and T. H. Kim, "Design of Artificial Neural Network for Handwritten Signature Recognition," International Journal of Computers and Communications, Vol. 4, no. 3, pp. 59-66, 2010.