IOSR Journal of Electronics and Communication Engineering (IOSR-JECE)
e-ISSN: 2278-2834,p- ISSN: 2278-8735.Volume 12, Issue 3, Ver. I (May.-Jun. 2017), PP 23-25
www.iosrjournals.org

A Review Paper on Different Techniques of Feature Extraction methods of various online signature

Ms. Jyoti A.Kendule[1], Ms. Kalyani V.Gidde[2]
[1](*Electronics & Telecommunication, SVERI's College of Engineering, Pandharpur, India)*
[2](*Electronics & Telecommunication, SVERI's College of Engineering, Pandharpur, India)*

Abstract: *Signature is one of the most popular biometrics usedfor authentication. There are different techniques throughwhich one can classify the signature as true or forged .Thispaper reviews the different approaches towards sign verificationmethods. And this is what the reason that explains applicationsof signature verification in areas like mortgage, chequeprocessing, in financial transaction etc.Signature Reliability, authenticity and authorizations are highly necessary for many common places such as aircraftboarding, crossing borders of international, entering in a secure physical location, and performing financial (economical) transactions.Ahandwritten signature is a legally and socially accepted biometric trait for authenticating an individual. Typically, there are 2 types of handwritten signature verification systems: "off-line" and "online" systems. In off-line system, just an image of the user's signature is acquired without additional attributes, whereas, in online system, a sequence of x-y co-ordinates of the user's signature, along with associated attributes like time, pressure etc. are also acquired. So, an online verification system usually achieves more accuracy than off-line system.*

Keywords*: Histograms, Cartesian coordinate, Polar coordinates, Classifier.*

I. Introduction

The handwritten signature can be socially and legally accepted in the biometric trait. The signature is used for the person's identity verification. Everyone's signature is cannot be similar. If the people having same name but they have different signature. This uniqueness of the signature can be taken as advantage in the various fields to recognize the identity of the person. The applications of signature verification are needed in such way as banking, insurance healthcare, Document management, ID security, ecommerce. The signature verification systems can be classified into the two types i.e. the offline verification system and the on-line signature verification system. In the offline system just an image of the signature which is required for verification. It cannot be require any additional attributes of the signature for the verification of the signature. So the forger who gets the images of signature can misuse the signature. It has less security provided in off-line signature.

Signatures are most legal and common means for individual's identity recognition and verification since people are familiar with the use of signatures in their daily life. A signature is a unique identity of a person. Therefore we are in great need to develop a system which can recognize signatures. A signature verification system decides whether a given signature belongs to a claimed owner or not. A signature recognition system, on the other hand, has to decide a given signature belongs to which one of a certain number of writers. Signature recognition is split into two according to the available data in the input. Offline (static) signature recognition takes as input the image of a signature and is useful in automatic recognition of signatures found on bank checks and documents. Online (dynamic) signature recognition uses signatures that are captured by pressure sensitive tablets that extract dynamic properties of a signature in addition to its shape. Offline systems are of interest in scenarios where only hard copies of signatures are available where as in online systems most of the features are extracted at the time of signing. So the offline signature recognition is more challenging Therefore, in offline signature recognition methods, less information is available than online methods. Offline signature recognition primarily focus on the visual appearance of our signature for recognition purposes, Signature Recognition examines behavioral aspects that manifest themselves when we sign our name. Therefore it is essential to recognize the signatures with high accuracy.

II. Previous Work

Preeti S Pattankude, Tushar Bedke[1], International Journal of Advanced Research in Electrical,Electronics and Instrumentation Engineering.They conclude that a simple and effective online signature verification system that is suitable for user authentication on a mobile device. SVM classifier achieves better accuracy compared with Euclidian distance matching method.Vijila Rexline X, K. L. Neela[2] Journal of Network Communications and Emerging Technologies (JNCET).They conclude that the proposed scheme has the best performance and accuracy than the existing system. The main contribution of our method is to consider

the geometric properties of signature in recognition problems, using the segmented dissimilarity scores for verification. Sonica Sharma, Swati Bhasin [3], © 2016 IJEDR. They conclude that this methodology of verification is mostpopular over ancient ways involving passwords and PIN numbers for its accuracy and case sensitiveness.Jadhav Hemant B. IJSTE[4] - International Journal of Science Technology & Engineering.They conclude thata simple and effective method for online signature verification system is suitable for the user authenticationson a mobile device.FaziaAther Mubeena, S. MahaboobBasha[5]- International Journal of Science Technology Research.TheyConclude that the performance of the proposed technique is comparable and often superior to state-ofthe-art algorithms despite its simplicity and efficiency.Napa Sae-Bae and Nasir Memon[6]- IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY. They conclude that a simple and effective online signature verification system that is suitable for user authentication on a mobile device. EmmanuelleMaioranaet al[7]- IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY. They conclude that the properties of UBMs to derive a biometric representation which can be used to perform authentication in a protected system based on the fuzzy commitment scheme.

III. Methods for Feature Extraction

1. DTW :(Dynamic Time Warping**)**

The distance between two signatures is computed by using Dynamic Time Warping(DTW)method.The references signatures are used to assign special parameters for each signer,which makes the system cover the intra signer variation.Several features are extracted. Systems with single and multi-features are tested.Curvature change and speed enhance success verification rate .The experiment have been carried out using the SUSIG online signature database.

This application utilizes segment difference values obtained by Dynamic Time Warping (DTW) as observation of HMM.It combines the advantages of segmentation DTW which measures the features in local and advantages of HMM which models the variability of observation sequences in global. Firstly,correspondences of the critical points in signatures are marked by segmentation DTW. Then, a variety of differences between corresponding segments are calculated by classical DTW.

2. HMM :(Hidden Markov Model**)**

A Hidden Markov Model is a Markov Chain with an associated output mechanism which takes either states or transitions between states to either symbols or distributions on symbols. We will refer to the Markov Chain as the *underlying Markov Chain* of the HMM. We will calculate exclusively with finite presentations — those in which the Markov Chain has finitely many states. However, we will, at times, consider infinite presentations. Hidden Markov Models appear in the literature in several forms, the most frequent being Functions of a Markov Chain[1] and State-output Hidden Markov Models[2]. These forms are equivalent in the sense that for any HMM in one of these forms, there is an HMM in each of the other forms which defines the same process. The HMMs in this work will be Edge-output Hidden Markov Models, the elements of which are the set of states, the set of symbols, a stationary distribution on those states, and, for each state, a joint distribution on symbols and next states.

A process in the HMM class can be described as a finite-state Markov Chain with a memoryless output process which produces symbols in a finite alphabet. This is the sense in which these processes have finitely many states. However, from the perspective of an observer who knows the parameters of some representation of the process and is able to observe the output symbols but not the internal states, things look different. For some processes there are infinitely many distinct states of such an observer's knowledge about the status of the process.

This knowledge is defined in terms of conditional distributions on future symbols. This is the sense in which there can be infinitely many states. These states are more relevant than the original finite set of states to the study of the process, since they allow for optimal prediction.

Functions of Markov Chains were the first descriptions of these processes to be studied, and they were initially studied as mathematical information sources [1]. There were a handful of papers such as published in the 1950s and early 1960s, which define HMMs and lay out these theoretical questions. What is the entropy rate for a function of a Markov Chain? Do these two functions of Markov Chains define the same process (the identifiability question)? What is the smallest function of a Markov Chain equivalent to the given one (the minimality question)? This work was done by researchers with mathematical backgrounds, studying HMMs from a perspective of probability and information theory. From the 1970s onward, HMMs have been used for modeling observed patterns, especially in speech recognition. There are a large number of papers, such as thatpresent HMMs as tools for use on these practical problems.

3. Fourier Descriptor:

The advantage of using the Fourier domain is the ability to compactly represent on online signature using a fixed number of coefficients. The fixed length representation leads to fast matching algorithm and is essential in certain to find the right preprocessing steps and matching algorithm for this representation .We report on the effectiveness of the proposed method along with the effects of individual preprocessing and normalization steps,based on comprehensive tests over two public signature databases. We also propose to use the pen-up duration information in identifying forgeries. The FFT system shows promise both as a stand-alone system and especially in combination with approaches that are based on local features.

4. Positional Invariant Analysis:

An online signature is represented by a set of histograms. These histogram features are designed to capture necessary attributes of the signature as well as relationships between these attributes of the signature. It should be noted that histograms are extensively used as a feature set to capture attribute statistics in many recognition tasks. For example, in an object recognition and off-line signature verification process. Using histograms for online signature verification was first suggested by Nelson et al . They have also used as part of the feature set and the use of histograms arerestricted only to angles derived from vectors connecting two successive points in an online signature. In statistic, as is shown below, more information can be used to derive histograms beneficial in online signature verification. These include speed, x-y trajectories, pressure, angles, and their derivatives. The feature extraction process of the proposed method begins with converting time-series data of a signature in to a sequence of Cartesian vectors and attributes, as well as their derivatives. Then, every Cartesian vector is converted to a vector in the polar coordinate system. Lastly, histograms from these vector sequences are derived. Detailed process of feature extraction is as follows.

Let $X = \{x1, x2, \ldots, xn\}$,
$Y = \{y1, y2, \ldots, yn\}$, and
$P = \{p1, p2, \ldots, pn\}$

be the *x co-ordinate* and *y* co-ordinates and pressure attribute, respectively, of a signature with length *n* sampled at times $T = \{t1, t2, \ldots, tn\}$. For datasets used in this experiment, all signatures were sampled at a constant rate. Hence the time information is understood and is overlooked. One important observation is that if time intervals are not constant, a normalization process using information from *T* can be applied to the sequences X, *Y*, and *P* former to being processed by the system.

IV. Conclusion

The signature is one of the unique identities but still signature of the same person may vary with time, age,emotional state of a person. Signatures are a subconscious expression. Both the signer and the authorizer are impacted by mood environment, writing instrument, writing Surface, fatigue. Due to this signatures are highly vulnerable. So it becomes necessary to be secured from attacks like forgeries or frauds. So the main approach of this paper is to review the different methods to avoid and control the forgeries which can be either random forgery, unskilled forgery or skilled forgery where we can say that skilled forgery is somehow difficult to detect among other type of forgeries.

References

[1]. Preeti S Pattankude, Tushar Bedke," Positional Invariant Features Based Online Signature Verification for Personal Authentication", International Journal of Advanced Research in Electrical,Electronics and Instrumentation Engineering, Vol. 5, Issue 5, May 2016.

[2]. Vijila Rexline X, K. L. Neela,"Enhanced Digital Human Signature Verification over Web and Mobile Interfaces", Journal of Network Communications and Emerging Technologies (JNCET) www.jncet.org Vol 6, Issue 5, May (2016).

[3]. Sonika Sharma, Swati Bhasin,"System and Methods for Online Signature Verification on Mobile devices", © 2016 IJEDR | Volume 4, Issue 2 | ISSN: 2321-9939.

[4]. Jadhav Hemant B. IJSTE," Online Signature Verification on Mobile Devices", IJSTE - International Journal of Science Technology & Engineering | Volume 2 | Issue 10 | April 2016

[5]. Fazia Ather Mubeena, S.Mahaboob Basha,"Online Signature Verification on Mobile Devices", International Journal of Science Technology Research, Vol.04, Issue.35, August-2015.

[6]. Napa Sae-Bae and Nassir Memon,"Online Signature Verification on Mobile Devices", IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 9, NO. 6, JUNE 2014.

[7]. Emanuele Maioranaet al," Biometric Template Protection Using Universal Background Models: An Application to Online Signature", IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 7, NO. 1, FEBRUARY 2012.

[8]. M. Faundez-Zanuy, ―On-line signature recognition based on VQ-DTW, ‖ Pattern Recognit., vol. 40, no. 3, pp. 981-992, 2007.