ONLINE SIGNATURE VERIFICATION FOR PERSONAL AUTHENTICATION BY USING NEURAL NETWORK & SVM CLASSIFIER

Prof. Miss. K. V. Gidde [1], Prof. Miss. M. J. Goski [2], Prof. Miss.A.S.Singh[3], Prof. Miss. M. Biswas [4]

Department of Electronics and Telecommunication Engineering
SVERI's COE Pandharpur, Solapur, Maharashtra, India

---***---

Abstract - The widely biometric used for certification is signature. There are numerous methods widely for the classification of signature as true or false .This paper aims at reviewing different approaches towards sign verification methods. Signature verification has very wide applications in fields of banking for processing of cheques, in monitory transactions etc. Verification, authencity and reliability of Signature is highly important in places such as boarding of aircraft, crossing international borders and performing economical transactions. A handwritten 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.

Key Words: **Histograms, Cartesian coordinate, Polar coordinates, Neural Network and SVM Classifier.**

1. INTRODUCTION

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. Signature Reliability, authenticity and authorizations are highly necessary for many common places such as aircraft boarding, crossing borders of international, entering in a secure physical location, and performing financial (economical) transactions. 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 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.

2. METHODOLOGY:

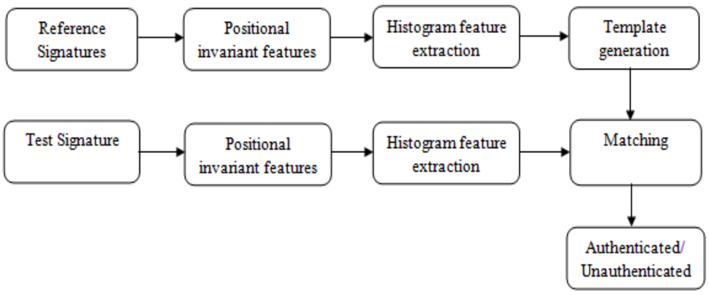

Reference Signatures
Positional invariant features
Histogram feature extraction
Template generation
Test Signature
Positional invariant features
Histogram feature extraction
Matching
Authenticated/ Unauthenticated

Figure 1:-Block Diagram

2.1 POSITIONAL INVARIANT ANALYSIS:

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

Let *X* = {*x*1, *x*2, ...,*xn*}, *Y* = {*y*1, *y*2, . . . , *yn*}, and *P* = {*p*1, *p*2, . . . , *pn*} be the *x* and *y* co-ordinates and pressure attribute, respectively, of a signature with length *n* sampled at times *T* = {*t*1, *t*2, . . . , *tn*}. For datasets used in this first experiment, all signatures were sampled at a constant rate. Hence the time information is implicit and is ignored. Note that if time intervals are not a constant, a normalization process using information from *T* can be applied to the sequences *X*, *Y*, and *P* prior to being processed by the system. To begin with, the vectors *X*1, *Y* 1, and *P*1 including their derivatives are computed as follows,

$$X^1 = \{x_i^1 | x_i^1 = x_{i+1} - x_i\},$$
$$Y^1 = \{u_i^1 | y_i^1 = y_{i+1} - y_i\},$$
$$P^1 = \{p_i\},$$

$$X^k = \{x_i^k | x_i^k = x_{i+1}^{k-1} - x_i^{k-1}\},$$
$$Y^k = \{y_i^k | y_i^k = y_{i+1}^{k-1} - y_i^{k-1}\},$$
$$P^k = \{p_i^k | p_i^k = p_{i+1}^{k-1} - p_i^{k-1}\},$$

Note that, by computing differences between each pair of successive points as above, the vectors *X*1 and *Y* 1 capture positional invariant features of the signature. And by repeating this process of taking differences *k* times yields the *kth* order derivative, *Xk* and *Y k* , of the original *X* and *Y* sequences respectively.

Then, a sequence of vectors

$$V = \{v_i^* | i = 1, 2, \ldots, n\}$$
$$v_i^k = \langle x_i^k, y_i^k, r_i^k, \theta_i^k, p_i^k \rangle$$

Where,

$$\theta_i^k = tan^{-1}\left(y_i^k / x_i^k\right), \ r_i^k = \sqrt{\left(x_i^k\right)^2 + \left(y_i^k\right)^2}$$

One dimensional histograms – these capture distributions of individual attributes. For example, the histogram _1 captures the angle distribution of an online signature which reflects the similarity between two signature shapes. Similarly, _2 captures the distribution of the angles of the first derivative since it provides information about how these vectors are aligned, an aspect that is completely ignored in the histogram _1. *R*1 captures the speed distribution of an online signature which is one of the distinctive features that is unique among users and especially useful in combating skilled forgeries.

The histograms above are computed by splitting the range of attribute values, into a number of equal width bin intervals, and counting the number of elements that fall into each particular bin. For an angle attribute and its derivative, the range of its histogram is defined as [−*π*, *π*]. For an attribute that has no explicit boundary, an outlier process with cutoff at three standard deviations from its mean is applied prior to computing the mean and standard deviation of the attribute in order to derive its implicit range described For example, the histogram _1 is derived from a sequence {*θi*1 ; *i* = 1, . . . , *n*} by forming a 24 bin histogram with equal width bin intervals beginning from −*π* to *π* and counting the number of elements, {*θ*1 *I* }, that fall into each of the 24 bins. It then results in a vector of 24 bin frequencies. histograms comprise of two types of frequencies: 1) absolute frequency, an actual count of elements that fall into a particular bin, and 2) relative frequency, the absolute frequency normalized by the total number of elements in the histogram, or in other words the length *n* of a signature. Using the absolute frequency results in more implicit importance given to the length of the signature whereas using the relative frequency ignores the length. Out of the 21 histograms listed, only 5 are described by absolute frequency.

These five histograms were empirically chosen as they derive from the lowest order derivative of online signature attributes as well as they provide higher recognition rate when describe with absolute frequency.

2.2 NEURAL NETWORK CLASSIFIER

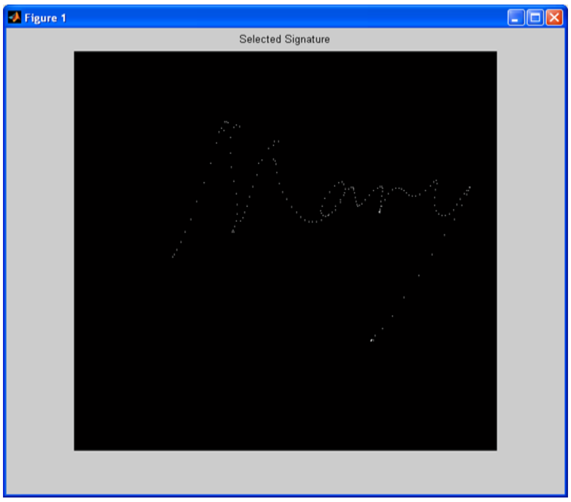
Neural networks are predictive models loosely based on the action of biological neurons. The selection of the name "neural network" was one of the great PR successes of the Twentieth Century. It certainly sounds more exciting than a technical description such as "A network of weighted, additive values with nonlinear transfer functions". However, despite the name, neural networks are far from "thinking machines" or "artificial Lungs". A typical artificial neural network might have a hundred neurons. In comparison, the human nervous system is believed to have about 3x10^{10} neurons. We are still light years from "Data".

2.3 SVM CLASSIFIER

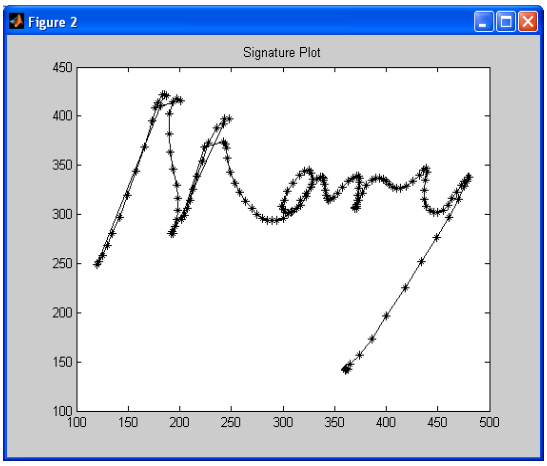
The goal of the SVM is to train a model that assigns new unseen objects into a particular category. It achieves this by creating a linear partition of the feature space into two categories. Based on the features in the new unseen objects (e.g. documents/emails), it places an object "above" or "below" the separation plane, leading to a categorization (e.g. spam or non-spam). This makes it an example of a non-probabilistic linear classifier. It is non-probabilistic, because the features in the new objects fully determine its location in feature space and there is no stochastic element involved.

3. RESULTS AND CONCLUSION

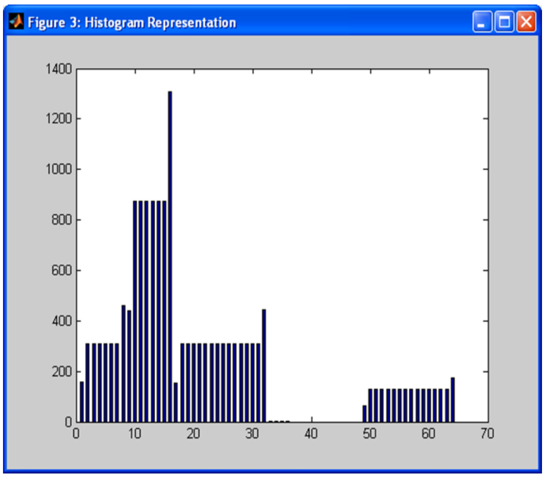
1) Sample Signature:



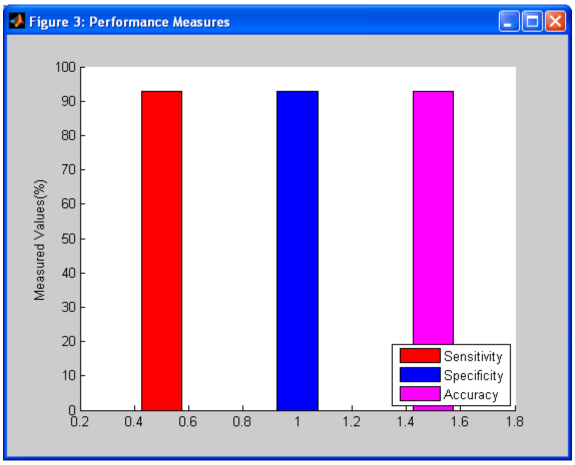
2) Signature Plot:



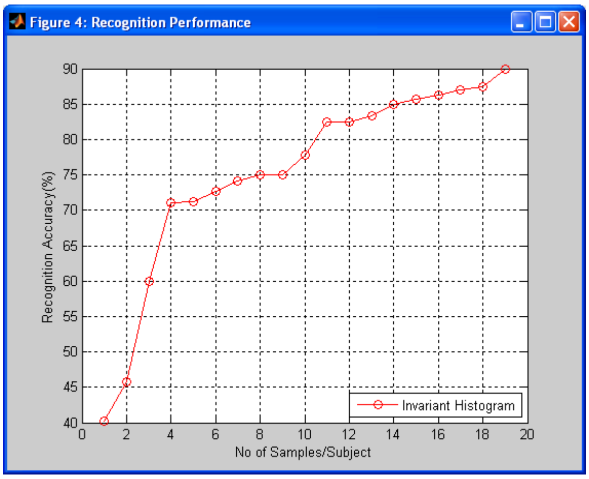
3) Histogram Representation:



4) Performance Measure



5) Recognition Accuracy:



4. CONCLUSIONS

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. By applying histogram feature extraction along with PNN classifier method we can achieve better performance parameter like accuracy of 92.59%, sensitivity92.85%, and Specificity 92.3077%.

REFERENCES

[1] L. G. Plamondon and R. Plamondon, “Automatic signature verification and writer identification—the state of the art,” *Pattern Recognit.*, vol. 22, no. 2, pp. 107–131, 1989

[2] H. Feng and C. C. Wah, “Online signature verification using a new extreme points warping technique,” *Pattern Recognit. Lett.*, vol. 24, no. 16, pp. 2943–2951, 2003

[3] A. Kholmatov and B. Yanikoglu, “SUSIG: An on-line signature database, associated protocols and benchmark results,” *Pattern Anal. Appl.*, vol. 12, no. 3, pp. 227–236, 2008.

[4] L. Nanni, “An advanced multi-matcher method for on-line signature verification featuring global features and tokenised random numbers,” *Neuro computing*, vol. 69, nos. 16–18, pp. 2402–2406, 2006.

[5] D. Guru and H. Prakash, “Online signature verification and recognition: An approach based on symbolic representation,” *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 31, no. 6, pp. 1059–1073, Jun. 2009.

[6] L. Nanni, E. Maiorana, A. Lumini, and P. Campisi, “Combining local, regional and global matchers for a template protected on-line signature verification system,” *Expert Syst. Appl.*, vol. 37, pp. 3676–3684, May 2010.

[7] N. Sae-Bae and N. Memon, “A simple and effective method for online signature verification,” in *Proc. Int. Conf. BIOSIG*, 2013, pp. 1–12