ISSN:0975-9646

Rapanjot Kaur et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (3) , 2014, 3648-3652

Review on: Enhanced Offline Signature Recognition Using Neural Network and SVM

Rapanjot Kaur[#], Gagangeet Singh Aujla[*]

[#]*Computer Science Department, Punjab Technical University*
Punjab,India

[*]*Assistant professor*
Chandigarh Engineering College,Landran(Punjab)

Abstract—**Biometrics, which refers to identifying an individual based on his or her physiological or behavioral characteristics, has the capability to reliably distinguish between an authorized person and an imposter. Signature verification systems can be categorized as offline (static) and online (dynamic). This thesis presents neural network and SVM with surf feature based recognition of offline signatures system that is trained with low-resolution scanned signature images. The signature of a person is an important biometric attribute of a human being which can be used to authenticate human identity. However human signatures can be handled as an image and recognized using computer vision and neural network and SVM with surf feature techniques. With modern computers, there is need to develop fast algorithms for signature recognition. There are various approaches to signature recognition with a lot of scope of research. In this thesis, off-line signature recognition & verification using neural network and SVM and surf feature is proposed, where the signature is captured and presented to the user in an image format [4, 5] . Signatures are verified based on parameters extracted from the signature using various image processing techniques. The Off-line Signature Recognition and Verification is implemented using Matlab. This work has been tested and found suitable for its purpose. For the implementation of this proposed work Matlab software is used.**

Keywords— **Signature verification, Indian script, Hindi signatures, Document security, Neural Network and SVM**

I. INTRODUCTION

In our society, traditional and accepted means for a person to identify and authenticate himself either to another human being or to a computer system is based on one or more of these three general principles:

1. What the person knows
2. What he possesses or
3. What he is

The written signature is regarded as the primary means of identifying the signer of a written document based on the implicit assumption that a person's normal signature changes slowly and is very difficult to erase, alter or forge without detection. The handwritten signature is one of the ways to authorize transactions and authenticate the human identity compared with other electronic identification methods such as fingerprints scanning and retinal vascular pattern screening. It is easier for people to migrate from using the popular pen-and-paper signature to one where the handwritten signature is captured and verified electronically. The signature of a person is an important biometric attribute of a human being and is used for authorization purpose. Various approaches are possible for signature recognition with a lot of scope of research. Here, we deal with an off-line signature recognition technique. Signatures are composed of special characters and flourishes 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. Signature recognition is the process of verifying the writer's identity by checking the signature against samples kept in the database. The result of this process is usually between 0 and 1 which represents a fit ratio (1 for match and 0 for mismatch). Signature recognition is used most often to describe the ability of a computer to translate human writing into text. This may take place in one of two ways either by scanning of written text (off-line method) or by writing directly on to a peripheral input device. The first of these recognition techniques, known as Optical Character Recognition (OCR) is the most successful in the main stream. Most scanning suites offer some form of OCR, allowing user to scan handwritten documents and have them translated into basic text documents. OCR is also used by some archivist as a method of converting massive quantities of handwritten historical documents into searchable, easily-accessible digital forms [15, 16].

II. OVERVIEW OF SIGNATURE RECOGNITION

A problem of personal verification and identification is an actively growing area of research. The methods are numerous and are based on different personal characteristics; voice, lip movement, hand geometry, face, odor, gait, iris, retina and fingerprint are the most commonly used authentication methods. All these psychological and behavioral characteristics are called biometrics [10]. The driving force of the progress in this field is above all, the growing role of the internet and electronic transfers in modern society. Therefore considerable number of applications is concentrated in the area of electronic commerce and electronic banking systems.

The biometrics have a significant advantage over traditional authentication techniques (namely passwords, PIN numbers, smart cards etc) due to the fact that biometric characteristics of the individual are not easily transferable are unique of every person and cannot be lost, stolen or broken. The choice of one of the biometric solutions depends on several factors which include:

1. User acceptance
2. Level of security required
3. Accuracy
4. Cost and implementation time[8,9]

The method of signature verification reviewed in this paper benefits the advantage of being highly accepted by potential customers. The use of the signature has a long history which goes back to the appearance of writing itself. Utilization of the signature as an authentication method has already become a tradition in the western civilization and is respected among the others. The signature is an accepted proof of identity of the person in a transaction taken on his or her behalf. Thus the users are more likely to approve this kind of computerized authentication method. Signature verification systems differ in both their feature selection and their decision methodologies. More than 40 different feature types have been used for signature verification. Features can be classified into two major types: local and global. Global features are features related to the signature as a whole, for instance the average signing speed, the signature bounding box and Fourier descriptors of the signatures trajectory. Local features correspond to a specific sample point along the trajectory of the signature. Signature recognition and verification involves two separate but strongly related tasks: one of them is identification of the signature owner, and the other is the decision about whether the signature is genuine or forged. Also, depending on the need, signature recognition and verification problem is put into two major classes: (i) On-line signature recognition and verification systems (SRVS) and (ii) Off-line SRVS. On-line SRVS requires some special peripheral units for measuring hand speed and pressure on the human hand when it creates the signature. On the other hand, almost all Off-line SRVS systems rely on image processing and feature extraction techniques.

A. Image Preprocessing and Features Extraction

We approach the problem in two steps. Initially, the scanned signature image is preprocessed to be suitable for extracting features. Then, the preprocessed image is used to extract relevant geometric parameters that can distinguish forged signatures from exact ones using the ANN approach.

Preprocessing:

The signature is first captured and transformed into a format that can be processed by a computer. Now it's ready for preprocessing. In preprocessing stage, the RGB image of the signature is converted into grayscale and then to binary image. The purpose of this phase is to make signatures ready for feature extraction. The preprocessing stage includes two steps: Colour inversion, Filtering and Binarization [1,3].

Colour Inversion:

The true colour image RGB is converted to the grayscale intensity image by eliminating the hue and saturation information while retaining the luminance. A grayscale image is a data matrix whose values represent intensities within some range where each element of the matrix corresponds to one image pixel.

Image Filtering and Binarization:

Any image when resample is filtered by a low pass FIR filter. This is done to avoid aliasing. This aliasing occurs because of sampling the data at a rate lower than twice the largest frequency component of the data. So a low pass filter will remove the image high frequency components. And for this purpose the filter used [13,14]. Now the grayscale image is segmented to

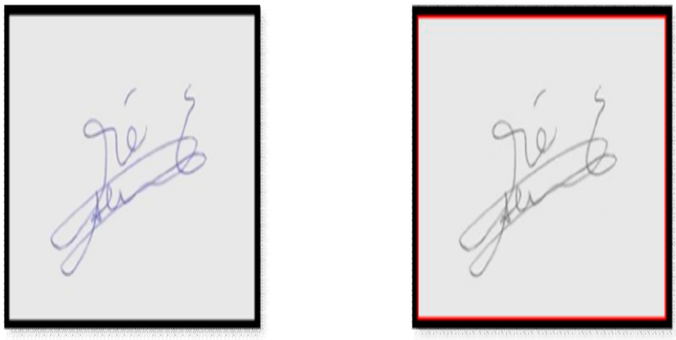

Figure.1. (a) A sample signature to be processed; (b) A Grayscale Intensity Image

get a binary image of objects. In a binary image, each pixel assumes one of only two discrete values: 1 or 0. A binary image is stored as a logical array.

Figure 2: Binary Image interpreting the bit value of 0 as black and 1 as white

Features Extraction is the key to develop an offline signature recognition system. We use a set of five global features that cannot be affected by the temporal shift.

B. Types of Signature Verification Based on the definitions of signature, it can lead to two different approaches of signature verification. Off-Line or Static Signature Verification Technique This approach is based on static characteristics of the signature which are invariant. In this sense signature verification, becomes a typical pattern recognition task knowing that variations in signature pattern are inevitable; the task of signature authentication can be narrowed to drawing the threshold of the range of genuine variation. In the offline signature verification techniques, images of the signatures written on a paper are obtained using a scanner or a camera.

On-line or Dynamic Signature Verification Technique

This is the second type of signature verification technique. This approach is based on dynamic characteristics of the process of signing. This verification uses signatures that are captured by pressure sensitive tablets that extract dynamic properties of a signature in addition to its shape. Dynamic features include the number of order of the strokes, the overall speed of the signature and the pen pressure at each point that make the signature more unique and more difficult to forge. Application areas of Online Signature Verification include protection of small personal devices (e.g. PDA, laptop), authorization of computer users for accessing sensitive data or programs and authentication of individuals for access to physical devices or buildings [17].

Nature of Human Signature

It is supposed that the features of the process of signing originate from the intrinsic properties of human neuromuscular system which produces the aforementioned rapid movements. Knowing that this system is constituted by a very large number of neurons and muscle, fibers is possible to declare based on the central limit theorem that a rapid and habitual movement velocity profile tends toward a delta-log normal equation. This statement explains stability of the characteristics of the signature. Thus, the signature can be treated as an output of a system obscured in a certain time interval necessary to make the signature.

III. Neural Network

Neural network is set of interconnected neurons. It is used for universal approximation. Artificial neural networks are composed of interconnecting artificial neurons (programming constructs that mimic the properties of biological neurons). Artificial neural networks may either be used to gain an understanding of biological neural networks, or for solving artificial intelligence problems without necessarily creating a model of a real biological system. The real, biological nervous system is highly complex: artificial neural network algorithms attempt to abstract this complexity and focus on what may hypothetically matter most from an information processing point of view. Good performance (e.g. as measured by good predictive ability, low generalization error), or performance mimicking animal or human error patterns, can then be used as one source of evidence towards supporting the hypothesis that the abstraction really captured something important from the point of view of information processing in the brain. Another incentive for these abstractions is to reduce the amount of computation required to simulate artificial neural networks.

A. Architecture of artificial neural network

The basic architecture consists of three types of neuron layers: input, hidden, and output. In feed-forward networks, the signal flow is from input to output units, strictly in a feed-forward direction. The data processing can extend over multiple layers of units, but no feedback connections are present. Recurrent networks contain feedback connections. Contrary to feed-forward networks, the dynamical properties of the network are important. In some cases, the activation values of the units undergo a relaxation process such that the network will evolve to a stable state in which these activations do not change anymore[12].

B. Artificial Neural Networks

Artificial neural networks are composed of interconnecting artificial neurons (programming constructs that mimic the properties of biological neurons). Artificial neural networks may either be used to gain an understanding of biological neural networks, or for solving artificial intelligence problems without necessarily creating a model of a real biological system. The real, biological nervous system is highly complex: artificial neural network algorithms attempt to abstract this complexity and focus on what may hypothetically matter most from an information processing point of view. Good performance (e.g. as measured by good predictive ability, low generalization error), or performance mimicking animal or human error patterns, can then be used as one source of evidence towards supporting the hypothesis that the abstraction really captured something important from the point of view of information processing in the brain [20].

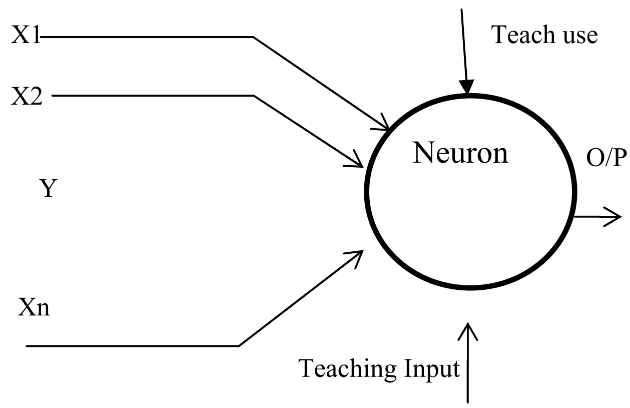

Figure 3: Neural Network

Another incentive for these abstractions is to reduce the amount of computation required to simulate artificial neural networks, so as to allow one to experiment with larger networks and train them on larger data sets.Application areas of ANNs include system identification and control (vehicle control, process control), game-playing and decision making (backgammon, chess, racing), pattern recognition (radar systems, face identification, object recognition), sequence recognition (gesture, speech, handwritten text recognition), medical diagnosis, financial applications, data mining (or knowledge discovery in databases, "KDD"), visualization and e-mail spam filtering.

C. Delta Rule

The delta rule is a gradient descent learning rule for updating the weights of the artificial neurons in a single-layer perceptron. It is a special case of the more general back propagation algorithm. For a neuron j with activation function g(x), the delta rule for j's, ith weight is given by

$$\Delta W_{ij} = (t_j - y_j)\, g'\,(h_j) x_i \qquad (1)$$

The delta rule is commonly stated in simplified form for a perceptron with a linear activation function as $\Delta W_{ij} = \alpha\,(t_j - y_j)\, x_i$, where α is known as the learning rate parameter.

IV SUPPORT VECTOR MACHINE

The Support Vector Machine (SVM) is a state-of-the-art classification method introduced in 1992 by Boser, Guyon, and Vapnik. The SVM classifier is widely used in bioinformatics (and other disciplines) due to its highly accurate, able to calculate and process the high-dimensional data such as gene expression and exibility in modeling diverse sources of data .SVMs belong to the general category of kernel methods. A kernel method is an algorithm that depends on the data only through dot-products. When this is the case, the dot product can be replaced by a kernel function which computes a dot product in some possibly high dimensional feature space. This has two advantages: First, the ability to generate non-linear decision boundaries using methods designed for linear classifiers. Second, the use of kernel functions allows the user to apply a classifier to data that have no obvious fixed-dimensional vector space representation. The prime example of such data in bioinformatics are sequence, either DNA or protein, and protein structure. Using SVMs effectively requires an understanding of how they work. When training an SVM the practitioner needs to make a number of decisions: how to preprocess the data, what kernel to use, and finally, setting the parameters of the SVM and the kernel [1]. Uninformed choices may result in severely reduced performance. We aim to provide the user with an intuitive understanding of these choices and provide general usage guidelines [7,13]. All the examples shown were generated using the PyML machine learning environment, which focuses on kernel methods and SVMs.

A. PRELIMINARIES: LINEAR CLASSIFIERS

Support vector machines are an example of a linear two-class classifier. This section explains what that means. The data for a two class learning problem consists of objects labeled with one of two labels corresponding to the two classes; for convenience we assume the labels are +1 or -1. In what follows boldface x denotes a vector with components xi. The notation xi will denote the ith vector in a dataset, f(xi; yi)gni =1, where yi is the label associated with xi. The boundary between regions classified as positive and negative is called the decision boundary of the classifier. The decision boundary defined by a hyper plane is said to be linear because it is linear in the input examples. A classifier with a linear decision boundary is called a linear classifier. Conversely, when the decision boundary of a classifier depends on the data in a non-linear the classifier is said to be non-linear.

B. *KERNELS: FROM LINEAR TO NON-LINEAR CLASSIFIERS*

In many applications a non-linear classifier provides better accuracy. And yet, linear classifiers have advantages, one of them being that they often have simple training algorithms that scale well with the number of examples [9, 10]. This begs the question: Can the machinery of linear classifiers be extended to generate non-linear decision boundaries? Furthermore, can we handle domains such as protein sequences or structures where a representation in a fixed dimensional vector space is not available? The naive way of making a non-linear classifier out of a linear classifier is to map our data from the input space X to a feature space F using a non-linear function.

The approach of explicitly computing non-linear features does not scale well with the number of input features: when applying the mapping from the above example the dimensionality of the feature space F is quadratic in the dimensionality of the original space. This result in a quadratic increase in memory usage for storing the features and a quadratic increase in the time required to compute the discriminant function of the classifier. This quadratic complexity is feasible for low dimensional data; but when handling gene expression data that can have thousands of dimensions, quadratic complexity in the number of dimensions is not acceptable. Kernel methods solve this issue by avoiding the step of explicitly mapping the data to a high dimensional feature-space.

Gaussian kernel is defined by:

$$K(\mathbf{x_i}, \mathbf{x_j}) = \exp(-\frac{\left\|\mathbf{x_i} - \mathbf{x_j}\right\|^2}{2\sigma^2}) \qquad (2)$$

Where k > 0 is a parameter that control the width of Gaussian. It plays a similar role as the degree of the polynomial kernel in controlling the exibility of the resulting classifier. We saw that a linear decision boundary can be kernelized i.e. its dependence on the data is only through dot products. In order for this to be useful, the training algorithms need to be kernelizable as well [6]. It turns out that a large number of machine learning algorithms can be expressed using kernels | including ridge regression, the perceptron algorithm, and SVMs [16].

C. SVMS FOR UNBALANCED DATA

Many datasets encountered in bioinformatics and other areas of application are unbalanced, i.e. one class contains a lot more examples than the other. Unbalanced datasets can present a challenge when training a classifier and SVMs are no exception see [13] for a general overview of the issue. A good strategy for producing a high-accuracy classifier on imbalanced data is to classify any example as belonging to the majority class; this is called the majority-class classifier. While highly accurate under the standard measure of accuracy such a classifier is not very useful [12]. When presented with an unbalanced dataset that is not linearly separable, an SVM that follows the formulation will often produce a classifier that behaves similarly to the majority-class classifier. The crux of the problem is that the standard notion of accuracy (the success rate, or fraction of correctly classified examples) is not a good way to measure the success of a classifier applied balanced data, as is evident by the fact that the majority-class classifier performs well under it. The problem with the success rate is that it assigns equal importance to errors made on examples belonging the majority class and errors made on examples belonging to the minority class. To correct for the imbalance in the data we need to assign different costs for misclassification to each class.

VI. CONCLUSION

A problem of personal verification and identification is an actively growing area of research. The methods are numerous and are based on different personal characteristics; voice, lip movement, hand geometry, face, odor, gait, iris, retina and fingerprint are the most commonly used authentication methods. Therefore considerable number of applications is concentrated in the area of electronic commerce and electronic banking systems. Many signature verification techniques have been proposed earlier but they were not secure enough and can be temporarily tampered with so the task was not fulfilled. Signature Verification using Neural Network alone could not provide better results. We use Signature Verification Technique using neural network and svm with surf feature. The results of matching are improved as we use neural network and svm with surf feature technique for matching. Better improved quality of signature and matching results are obtained.

ACKNOWLEDGMENT

Thanks to my Guide and family member who always support, help and guide me during my dissertation. Special thanks to my father who always support my innovative ideas.

REFERENCES

[1] Anil K Jain, Arun Ross and Salil Prabhakar, “An Introduction to Biometric Recognition,”*IEEE Transactions on Circuits and Systems for Video Technology*, vol. 14, no.1, pp. 1-29, 2004.

[2] K.R. Radhika, M.K. Venkatesha and G.N. Sekhar, “Off-Line Signature Authentication Based on Moment Invariants Using Support Vector Machine”, Journal of Computer Science 6 (3): 305-311, 2010.

[3] Reza Ebrahimpour, Ali Amiri, Masoom Nazari and Alireza Hajiany, “Robust Model for Signature Recognition Based on Biological Inspired Features”, International Journal of Computer and Electrical Engineering, Vol. 2, No. 4, August, 2010.

[4] . A. Piyush Shanker, A.N. Rajagopalan, “Off-line signature verification using DTW”, Pattern Recognition Letters 28 (2007) 1407–1414.

[5] Alessandro Zimmer and Lee Luan Ling, “Offline Signature Verification SystemBased on the Online Data”, EURASIP Journal on Advances in Signal Processing Volume 2008, Article ID 492910, 16 pages.

[6] Banshidhar Majhi, Y Santhosh Reddy, D Prasanna Babu, “Novel Features for Off-line SignatureVerification” International Journal of Computers, Communications & Control, Vol. I, No. 1, pp. 17-24, 2006.

[7] Migual A. Ferrer, Jesus B. Alonso and Carlos M. Travieso, "Off-line Geometric Parameters for Automatic SignatureVerification Using Fixed-Point Arithmetic", *IEEE Tran. on Pattern Analysis and Machine Intelligence*, vol.27, no.6, June 2005.

[8] Debasish Jena, Banshidhar Majhi, Saroj Kumar Panigrahy, Sanjay Kumar Jena “Improved Offline Signature Verification Scheme Using Feature Point Extraction Method”.

[9] B. Fang, C.H. Leung, Y.Y. Tan and Y.K. Wong, "Off-line signatures tracking of feature and stroke Recognition, pp. 91-101, 2003.

[10] G.A. Khuwaja. An adaptive combined classifier system for invariant face recognition. Digital Signal Processing 12, 21–46, DOI:10.1006/dspr.2001.0413, 2002.

[11] D. Zhang, J. Campbell, D. Maltoni, and R. Bolle. Special issue on biometric systems. IEEE Trans. Systems, Man and Cybernetics - C, 35(3):273–275, 2005.

[12] K. Bowyer, V. Govindaraju, and N. Ratha. Introduction to the special issue on recent advances in biometric systems. IEEE Trans. Systems, Man and Cybernetics - B, 37(5): 1091–1095, 2007.

[13] G. A. Khuwaja. Fingerprint identification with LVQ. Proc of the 9th IEEE Int Conf on Neural Information Processing (ICONIP'OZ), Vol. 2, Singapore, Nov. 2002.

[14] J.F. Vargas, M.A. Ferrer, C.M. Travieso, and J. B. Alonso. Offline signature verification based on pseudo-cepstral coefficients. 10th IEEE Int Conf on Document Anal. & Recognition, 2009.

[15] A.I. Al-Shoshan. Handwritten signature verification using image invariants and dynamic features. Proc of the IEEE Int Conf on Computer Graphics, Imaging and Visualization (CGIV'06), 2006.

[16] M. Piekarczyk. Hierarchical random graph model for off-line handwritten signatures recognition. IEEE Int Conf on Complex, Intelligent, Software Intensive Systems, 2010.

[17] S.M.S. Ahmad, A. Shakil, M.A. Faudzi, R.M. Anwar. Analysis of 'goat' within user population of an offline signature biometrics. 10th IEEE Int Conf on Information Science, Signal Processing and their Applications (ISSPA 2010).

[18] J.P. Drouhard, R. Sabourin, and M. Godbout. A neural network approach to off-line signature verification using directional PDF. Pattern Recognition, 29(3), (1996), 415--424.

[19] E.J.R. Justino, F. Bertolozzi, and R. Sabourin. A comparison of SVM and HMM classifiers in the offline signature verification. Pattern Recognition Letters, vol. 26, 1377-1385, 2005.

[20] K. Delac and M. Grgic. A survey of biometric recognition methods. Proc of 46th IEEE Int Symposium Electronics, Croatia, 184-193, June 2004.