INTERNATIONAL JOURNAL OF COMPUTER ENGINEERING AND APPLICATIONS
VOLUME XVI, ISSUE VI, JUNE 22, WWW.IJCEA.COM, ISSN 2321-3469

SIGNATURE BASED AUTHENTIATION USING DECISION TREE AND SUPPORT VECTOR MACHINE

Yerininti Venkata Narayana[1], Chintakrindi Harika[2], Katra Keerthana[2], ArlaTirumala[2]

[1] *Asst.Professor, Information Technology Department,*

Vasireddy Venkatadri Institute of Technology, Guntur, Andhra Pradesh, India

[2] *B. Tech Students, Department of Information Technology, Vasireddy Venkatadri Institute of Technology, Guntur, Andhra Pradesh, India*

ABSTRACT:

Every person has his/her own unique signature that is used mainly for the purposes of personal identification and verification of important documents or legal transactions. There are two kinds of signature verification: static and dynamic. Static(off-line) verification is the process of verifying an electronic or document signature after it has been made, while dynamic(on-line) verification takes place as a person creates his/her signature on a digital tablet or a similar device. Offline signature verification is not efficient and slow for a large number of documents. To overcome the drawbacks of offline signature verification, we have seen a growth in online biometric personal verification such as fingerprints, eye scan etc. In this project we created MACHINE LEARNING models like Support Vector Machine and K-means using python for offline signature and after training and validating, the accuracy of testing

Keywords: Machine Learning, Signature verification, Support Vector Machine, K-means, Decision Tree

[1] INTRODUCTION

The most common task in the field of forensic document analysis [1–5] is that of authenticating signatures. The problem most frequently brought to a document examiner is the question relating to the authenticity of a signature: Does this questioned signature (Q) match the known, true signatures (K) of this subject. A forensic document examiner– also known as a questioned document (QD) examiner–uses years of training in examining signatures in making a decision in case work. The training of a document examiner involves years of learning from signatures that are both genuine and forged. In case-work, exemplars are usually only available for genuine signatures of a particular individual, from which the

characteristics of the genuine signature are learnt. Algorithms for visual signature verification are considered in this paper. The performance task of signature verification is one of determining whether a questioned signature is genuine or not. The image of a questioned signature is matched against multiple images of known signatures Visual signature verification is naturally formulated as a machine learning task.

We discuss system overview in **[Figure-1]**. A dynamic signature verification system gets its input from data acquisition device like a digital tablet or other, dynamic input device. The signature is then represented as time-varying signals. The verification system focuses on how the signature is being written rather than how the signature was written. This provide s a better means to grasp the individuality of the writer but fails to recognize the writing itself. The Signature verification task is very critical and often presents difficulties like high variability i.e. a person's signature may vary each time and may change completely with age, behavior and environment, similarities between signatures of different person and similarity in duplication or forgery of one's signature.

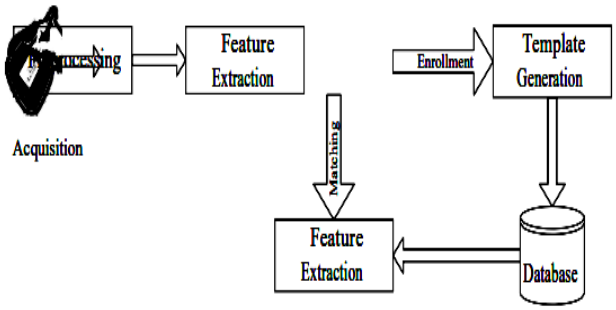

Figure:1 System Overview

Such hinders in authentication of handwritten signature can be tackled by two common ways: online and offline verification. Offline signature verification consist of use of static features of two dimensional image pixel data acquired from scanning signed documents. Whereas online signature verification consist of electronic signing system which results dynamic data features such as the speed, pressure, pen's position, azimuth/altitude angle etc. There have been numerous research and studies on different approaches to verification of handwritten signature, both online and offline.

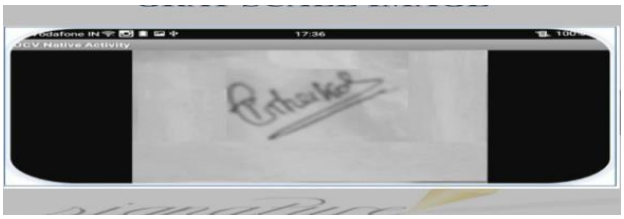

Figure:2.Gray Scale Image

In **[Figure-2]** we discuss how to convert binary/colour image to gray scale image**.** The handwritten signature of a person is commonly accepted as a means of verifying the legality of documents such as certificates, checks, drafts, letters, approvals, visa, passport etc. and is indispensable in countering the forgery and falsification of such documents in diverse financial, legal, bureaucratic, academic, and other commercial settings. Take for example, in any bank whenever cashier receives a cheque from client, such cheque is verified with

signature in it. The cashier compares that signature with stored record of genuine signatures before proceeding with any legal transaction. This convention of using signature as the route for confirming the authenticity of documents has been followed from medieval time to present and will continue in future. Such authentication with signature is at times very critical and crucial in legal scenario. For instance, a signature in any contracts has a vital role to indicate the identity of person of interest and also to provide evidence of intent and informed consent. Any falsification and fraudulent regarding such signature may result severe damages in persons lives and assets. In such cases, a systematic approach to verifying the signature is very necessary to prevent such forgery. class classification problem where the input consists of the difference between a pair of signatures.A signature is a person's name, or a mark, often stylized and handwritten that a person writes, indicating his/her identity and genuine intent. The handwritten signature of a person is commonly accepted as a means of verifying the legality of documents such as certificates, checks, drafts, letters, approvals, visa, passport etc.

[2] STATE OF THE ART

In human life security takes important role. Nowadays it's the basic fundamental of all systems developed. For this purpose, biometric authentication system got a lot of importance. Biometric authentication systems are secure, easy to use, easy to develop, uses basic techniques of signal processing and cheap to build. This improves the familiarity of biometric authentication system. Among these techniques signature verification is the most famous one because of cheap data acquisition devices. We can see the use of on-line signature verification in every kind of real time applications, such as credit card transactions, document flow applications, and identity authentication prior to access of sensitive resources. There have been several studies on on-line signature verification algorithms. Most commonly used on-line signature acquisition devices are pressure sensitive tablets, digitizer and webcam etc. Smart pens are also widely used in signature verification systems, which are capable of measuring forces at the pen1tip, exerted in three directions.

Special hand gloves with sensors for finding finger bend and hand position and orientation, and a CCD camera based approaches were also in signature acquisition; however, due to their high cost and impracticality, such devices couldn't find use in real systems. Depending on the device used, fair amount of preprocessing may be required to a signature data before the feature extraction phase. This portion of thesis is to describe about the previous work in the field of signature verification. The on-line signature verification techniques can be classified into two broad areas. 1. Using features extracted from the visible parts of the signature. 2. Using features extracted from virtual strokes or invisible parts of the signature (the parts that are not created but are imagined to be created). The area of Handwritten Signature Verification has been broadly researched in the last decades and still remains as an open research problem. This project focuses on offline signature verification, characterized by the usage of static (scanned) images of signatures, where the objective is to discriminate if a given signature is genuine (produced by the claimed individual), or a forgery (produced by an impostor). We present an overview of how the problem has been handled by several researchers in the past few decades and the recent advancements in the field. Article published in International Journal of Scientific & Engineering examined signature verification using neural network approach and analyzed its strengths and weakness [6]. Paper presented method which uses geometric features extracted from preprocessed signature images, which

trained neural network using error back propagation training algorithm for verification of signature.

[3] PROBLEM PP

Whenever any documents is verified on the basis of signature in it, person verifying it is taking a great risk and he/she should be absolutely certain of his/her decision. The validation of signature in many of the cases are highly critical and any inaccuracy in the authentication may result serious consequences and damages. With the advancement in technology, new and complex forgery and fraud techniques are emerging. In order to avoid such scenario and prevent potential damage, modern robust approach must be adopted in verifying the genuineness of signature. Adopting such approach will assists person in making decision over authenticity of signature and prevents mistakes.

The biometric signature authentication system using decision tree is existing system. This algorithm belongs to family of supervised learning. It is used for training the data. The goal of decision tree is to create a training model that can use to predict the class or value of the target variable by learning simple decision rules conclude from training data.

Disadvantages:

1. Small change in the training data tends to cause a big difference in the data, which causes instability
2. Calculations involved can also become complex compared to other algorithms
3. It takes longer time to train the data
4. It is also relatively expensive as the amount of time taken and the complexity levels are higher

[4] THE UUU

A SVM works on a dataset which has been partitioned into training and testing dataset. Training dataset contains known genuine and forged PNG signature images and testing dataset contains unknown signature images.

The steps for proposed algorithm using SVM are as follows:

Repeat the steps A1 to A3 for all images in training dataset to prepare reference feature vector.

1. Select a PNG image from training dataset.
2. Pre-process the selected image using following steps:
   a. Convert the image to grayscale image.
   b. Resize the image to [200,200] size.
   c. Convert the image to binary form.
3. Perform feature extraction of pre-processed image using following steps
   a. Compute shape, histogram of gradient, aspect ratio, bounding area, contour area, convex hull area
4. Now pass the image to the SVM Classifier

Proposed Solution Biometric signature authentication in proposed system we use SVM algorithm to implement the project. SVM algorithm belongs to family of supervised learning. The goal of SVM is to identify an optimal separating hyper plane which maximizes the

margin between different classes of the training data. Using SVM algorithm we can show the exactness for signatures.

A signature can be authenticated using either static (off-line) or dynamic (on-line) verification.

- **Static (off-line):** The signature is written either on a piece of paper and then scanned or directly on the computer using devices such as the digital pad. The shape of the signature is then compared with the enrolled (reference) signature. The difficulty with this technique is that a good forger will be able to copy the shape of the signature.
- **Dynamic (on-line):** The user's signature is acquired in real-time. By using this dynamic data, further feature such as acceleration, velocity, and instantaneous trajectory angles and displacements can be extracted.
- **Dynamic Feature Set:** The dynamic feature set describes how the signature is being signed rather than how it seems. Dynamics of the signature are very difficult to forge because these not only have the information of the overall shape of the signature, but also dynamic information of signature. When the user sign on a data acquisition module, it needs to be scanned at a rate high enough to capture this information, and from this dynamic data, relevant features are extracted. The dynamic feature set extracted consists of global parameter based features which allows us for easy and quick computing. This feature set requires less computational power and is of more cost efficient although it might not perform as well with compare to function based feature sets.

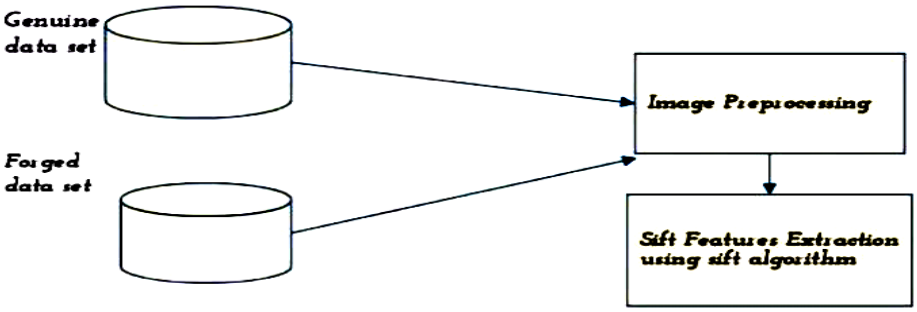

Figure:3. System Architecture

We discuss about system architecture in **[Figure-3]**. Biometric signature authentication in proposed system we use SVM algorithm to implement the project. SVM algorithm belongs to family of supervised learning. The goal of SVM is to identify an optimal separating hyper plane which maximizes the margin between different classes of the training data. Using SVM algorithm we can show the exactness for signatures. In the proposed solution we are having 2 steps:

1. Image preprocessing
2. Feature Extraction

1. Image preprocessing:

There are some common preprocessing steps, aimed to improve the performance of a verification system. These include size normalization, smoothing of the trajectory and re-sampling of the signature data. Low resolution tablet or low sampling rates tablets may give signatures that have jaggedness which is commonly removed using smoothing techniques. In

the systems where tablets of different active areas are used, signature size normalization is a frequently used as preprocessing technique. Comparing of two signatures having the same shape but of different sizes would result in low similarity scores. Size normalization is applied to remove that affect. Modern digital tablets have a sampling rate of more than 100 trajectory points per second. In some of the previous methods, re-sampling, as a preprocessing step, was used to remove possibly redundant data. After successful re-sampling, shape related features were reliably extracted.

2. Feature Extraction:

Feature extraction stage is one of the crucial stages of an on-line signature verification system. Features cans be classified as global or local, where global features represents signature's properties as a whole and local ones correspond to properties specific to a sampling point. The global features examples are signature bounding box, trajectory length or average signing speed, and distance or curvature change between consecutive points on the signature trajectory are local features.

[5] CONCLUSION

We analyzed online signature verification by tracking the pen tip. The system does not need any special hardware like tablet, unlike fingerprint verification or iris scanning systems. It requires only low cost webcams. We evaluated the best placement for webcams. It was confirmed that the webcam should be placed to the side of the hand for best results. The data base used for the verification was not large. Thus, this technique should be verified with large data base. It is observed that several cases where the system lost its track of the pen tip when the user wrote with an extremely fast stroke and the images of the pen tip were blurred at that time. This problem can be solved by an approach that finds blurred images by using sequential marginal likelihood with sequential Monte Carlo marginalization, and re-estimates the pen tip positions. To avoid forgery of signature in any of the public, private or other sectors, signature is recognized as genuine or forged based on two different approaches. An approach to identify the genuineness of signature using Support Vector Machine and Decision Tree is discussed here. Performance comparison of both the approaches is discussed. Our next objective is to improve accuracy by adding more features

REFERENCES

[1] Kondo, M. Sasaki, S. Tachibana, and T. Matsumoto. "A markov chain monte carlo algorithm for bayesian dynamic signature verification". IEEE Transactions On Information Forensics and Security, 1(1):22–34, March,2006.

[2] K. Yasuda, D. Muramatsu, and T. Matsumoto, "Visual-based online signature verification by pen tip tracking", Proc. CIMCA 2008, 2008, pp. 175–180.

[3] Satoshi Shirato, D. Muramatsu, and T. Matsumoto, "camera-based online signature verification: Effects of camera positions." World Automation congress2010 TSI press.

[4] D. Muramatsu, K. Yasuda, S. Shirato, and T. Matsumoto. "Visual-based online signature verification using features extracted from video", Journal of Network and Computer Applications Volume 33, Issue 3, May 2010, Pages 333-341.

[5] R. Plamondon and G. Lorette. Automatic signature verification and writer identification - the state of the art. Pattern Recognition, 22(2):107–131, 1989.

[6] M. E. Munich and P. Perona. "Visual identification by signature tracking." IEEE Trans. Pattern Analysis and MachineIntelligence, 25(2):200–217, February 2003.

[7] F.A.Afsar, M. Arif and U. Farrukh, "Wavelet Transform Based Global Features for Online Signature Recognition", Proceeding of IEEE International Multi-topic Conference INMIC, pp. 1-6 Dec. 2005.

[8] Mohammad M. Shafiei, Hamid R. Rabiee, "A New On-Line Signature Verification Algorithm Using Variable Length Segmentation and Hidden Markov Models," Seventh International Conference on Document Analysis and Recognition vol. 1, pp. 443, 2003.

[9] R. S. Kashi , J. Hu & W. L. Nelson, "On-line Handwritten Signature Verification using Hidden Markov Model Features", Fourth International Conference Document Analysis and Recognition (ICDAR'97), pp. 253 – 257, 1997.

[10] Charles E. Pippin, "Dynamic Signature Verification using Local and Global Features", Georgia Institute of Technology, July 2004.

[11] Hao Feng and Chan Choong Wah, "Online Signature Verification Using New 49 Extreme Points Warping Technique", Pattern Recognition Letters, vol. 24, pp. 2943- 2951, Dec. 2003.

[12] F.A. Afsar, M. Arif and U. Farrukh, "Wavelet Transform Based Global Features for Online Signature Recognition", Proceeding of IEEE International Multi-topic Conference INMIC, pp. 1-6 Dec. 2005.

[13] Liang Wan, Bin Wan, Zhou-Chen Lin "On-Line Signature Verification with Two- Stage Statistical Models", Eighth International Conference on Document Analysis and Recognition 282 – 286, 2005.

[14] Alisher Kholmatov, "Biometric Authentication Using Online Signatures", MS Thesis, Sabanci University, June 2002

Author[s] brief Introduction

1. Yerininti Venkata Narayana, M.Tech(CSE) - having teaching experience of 7+ years – Working as an Assistant Professor in the Department of Information Technology, Vasireddy Venkatadri Institute of Technology, Nambur, Guntur district, Andhra Pradesh. Area of Interests: Machine learning, Network Security and Image Processing.
2. Chintakrindi Harika – studying B.Tech in the Department of Information Technology, Vasireddy Venkatadri Institute of Technology, Nambur, Guntur district, Andhra Pradesh.
3. Katra Keerthana - studying B.Tech in the Department of Information Technology, Vasireddy Venkatadri Institute of Technology, Nambur, Guntur district, Andhra Pradesh.
4. Arla Tirumala - studying B.Tech in the Department of Information Technology, Vasireddy Venkatadri Institute of Technology, Nambur, Guntur district, Andhra Pradesh