MAULANA ABUL KALAM AZAD
UNIVERSITY OF TECHNOLOGY,
WEST BENGAL

DESIGN LAB PROJECT
IT-891

TOPIC : ***Offline Signature Verification Using Machine Learning***

BY

1. ***DAMAYANTI GHOSH***

UNIVERSITY ROLL:30000212008
UNIVERSITY REGN:123000110036

2. ***SUMIT KUMAR BARANWAL***

UNIVERSITY ROLL:30000212025
UNIVERSITY REGN:123000110053

Under the supervision of
Dr.Debashis De
Head of Department, CSE & IT Department
MAKAUT-WB

CERTIFICATE

It is certified that the work contained in the project report titled " **Offline Signature Verification using Machine Learning** " by 'Damayanti Ghosh' and 'Sumit Kumar Baranwal' has been carried out under my supervision and that this research work has not been submitted elsewhere for any degree.

Dated: ....

....

Signature of Supervisor

PREFACE

Signature is an extremely important feature in verification of a person’s identity in contemporary world. It is one of the major helps to identify and verify a person. Also it helps in validation of authenticity of any message or document . Hence it is very important to have a signature validated and verified properly to avoid fraudulence, theft or stealing of identification which can incur heavy loss, damage- both monetary and reputational to an individual or organisation.

In this project , we have made an honest attempt to create an “**Offline Signature Verification using Machine Learning** ” which has resulted in 86.73% success in detecting the forged signatures from their rightfully original true counterparts. This offline signature verification system has been modelled with heavy applications of image processing (for extensive feature extractions) and machine learning (for the training and testing of the devised model).

TABLE OF CONTENT

1. ABSTRACT

This project evaluates an efficient approach for Offline Signature Verification using Machine Learning techniques. The proposed algorithm able to identify the original signature and forgery signatures in a skilled way. First going through the preprocessing phase the signature is made noise free and the region of interest portion of the signature is get selected. After preprocessing some useful features such as global features, region based geometrical features and robust features are used to extract for this algorithm. The training and testing phase is done using those extracted feature description vectors of the signatures with the help of machine learning techniques. A comparative study is performed between two well known supervised learning techniques, Support Vector Machine and Single Layer Perceptron in the verification phase of the proposed algorithm.
This proposed algorithm yields percentage accuracy of 97.3% on average for Single layer perceptron and percentage accuracy of 76.16% on average for Support vector machine algorithm. Where Single Layer Perceptron provides an efficient result for this proposed approach.

❖ **KEYWORDS**

Signature Recognition, scaling, feature, Harris Corner Method, Surf Feature

2. INTRODUCTION

Contemporary economy and business transactions are heavily dependant on proper identification. With every passing day, forgery is becoming more advanced and requiring heavy skills technology, immense usage of machine-learning to study and create an authenticated system design for almost flawless verification of signatures as Signature identification and verification is considered among the most popular biometric methods in the area of personal authentication. Signature is a behavioral trait of an individual and forms a special class of hand-writing recognition in which eligible letters may or may not be visible properly.

Biometrics verification has been established as the most prevalent way to prevent unauthorized accesses to all kinds of e-data. Signature is strongly accepted in legally and socially as identification and authentication of a person's identity. But, it is very difficult to verify the signature physically. So, it is needed to design a strong system that verifies the signature of a human automatically and flawlessly. Based on this signature verification has been classified broadly into online and offline signature verification.

Depending on data acquisition mechanism, there are two methods of signature verification - Online or Dynamic and Offline or Static. Online method requires special set of devices and instruments to capture the dynamic features like, number of order of strokes, overall speed of signature, pen movements and pressure. On the other hand, the Offline approach uses an optical scanner to obtain the signature in order to obtain a digital representation composed of $M \times N$ pixels. In offline signature verification, the signature image is considered as a discrete 2D function $f(x, y)$, where $x = 0, 1, 2, \ldots, M$ and $y = 0, 1, 2, \ldots,$. N denote the spatial coordinates. The value of f in any (x, y) corresponds to the grey level in that point. Processing is done on the scanned images.

In the proposed method, we deal with Offline recognition of signatures based on extracting some Global, Region based and Robust features along with heavy applications of machine-learning techniques for the classification purpose. A comparative study between two supervised learning techniques

Support Vector Machine and Single Layer Perceptron, is done in the classification stage for the performance measurement. The algorithm is based on extracting features like density ratio, occupancy ratio etc along with the more critical methods like Harris-Corner method, Surf feature extraction etc. In the preprocessing part of the proposed technique, some useful approaches are followed to perform the crop operation of the Region Of Interest(ROI) area of the signature image. The algorithm gives good recognition rate using machine learning techniques.

3. TERMINOLOGIES

- 3.1. In signature verification systems, **forgeries may be classified in three basic types :**

1. **Random forgery:** The forger neither has the knowledge nor has access to the genuine signature or any information about the author's name. Forger reproduces a random signature.
2. **Simple forgery:** The forger has no access to the sample of the signature but knows the author‟s name and the forger produces the signature in own style.
3. **Skilled forgery:** The forger has access to the samples of the genuine signature and thus is able to reproduce it with much perfection.

- 3.2 **Error Rate**

In signature verification systems, the performance is evaluated in terms of error rates . There are two types of errors: **False Rejection** and **False Acceptance**. Also, there are two types of error rates: **False Rejection Rate (FRR)** and **False Acceptance Rate (FAR)**.

False rejection rate (FRR) is related to genuine signatures that are classified as forgeries.

False acceptance rate (FAR) is related to forgeries that are misclassified as genuine signatures.

FRR is known as type 1 and FAR is known as type 2 error.

4. RELATED WORK

Several works are published in offline verification system.
Some of the citations are the following:

1.**Offline Signature Verification** using Euclidian Distance
R Jana, R **Saha**, D Datta - International Journal of Computer Science 2014- Feature Extraction.

2.**Approaches and Issues in Offline Signature Verification System**
Hemanta Saikia,Majitar, Sikkim, International Journal of Computer Applications (0975 – 8887) Volume 42– No.16, March 2012

3.**Offline Signature Verification Using Pixel Matching Technique**
Indrajit Bhattacharya , Prabir Ghosh. Volume 10, 2013, Pages 970-977,First International Conference on Computational Intelligence: Modeling Techniques and Applications (CIMTA) 2013

And for other citations : cited in the reference section

Works differ mainly in feature extraction and classification techniques. Signatures are mainly complex and cursive shapes. Therefore they are described best with shape features. However shapes are considered as global entity and therefore are not widely studied in offline signature verification system.A Robust and efficient Signature verification system is important in many applications like banking where personal identification check is associated with economic and other forms of transaction. Even though several Signature verification schemes have already being proposed, none of the technique is yet proved to be accurate enough to be accepted with assurance in mission critical applications. Hence there remains a huge potential and scope for this field.

★ Softwares used in the project :

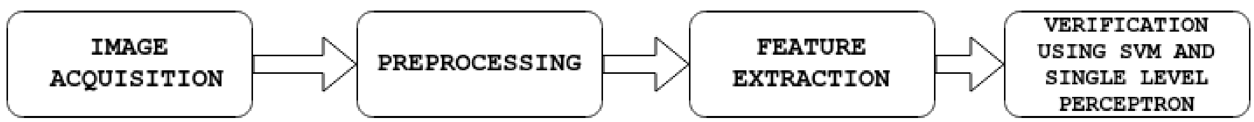
1.**MATLAB** : For the processing and feature extraction procedures from the scanned signature(s) images.

2.**WEKA** : For the implementation of machine learning in the classification and verification of the forged and true signatures based on the features extracted.

5. PROPOSED Method

Offline signature verification is an extensive feature extraction procedure (mostly through image processing) and pattern recognition problem. The procedure is discussed in the following.

The flow-chart diagram of the proposed method is depicted in the following,



5.1 IMAGE ACQUISITION

Collection of samples plays the first and foremost important gateway to the proposed project work. **Image Acquisition** is performed by scanning the signatures and storing it as jpeg format. Signatures have been collected from 15 persons. For the study and extraction of features a minimum of 10 signatures have been collected from each person. Next skilful forged signatures have been collected for each of the person's signature samples.

5.2 PREPROCESSING

Preprocessing is useful to make the signature suitable for easily extract the suitable distinct features and to simplify subsequent operations without loosing relevant processing. The input Signature is converted into grayscale image followed by a Binary image then noise portions like Salt pepper noises are get eliminated by applying median filtering. Next from the filtered image the region of interest portion of the signature image is get cropped out. Advantage of this function is no matter at what angle the signature has been done this function will help focus and deal with only the concerned pixels of the signatures excluding any other irregular pixels.

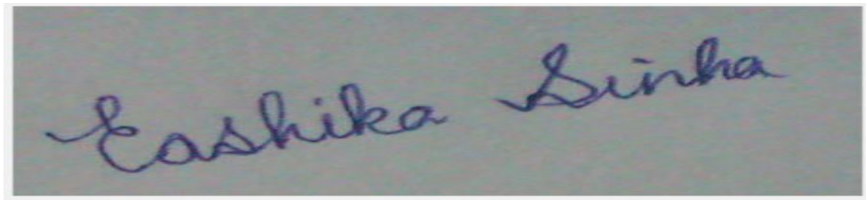


Fig 1:Original Signature(Scanned image)

Fig 2:Gray Image

Fig 3:Binary Image

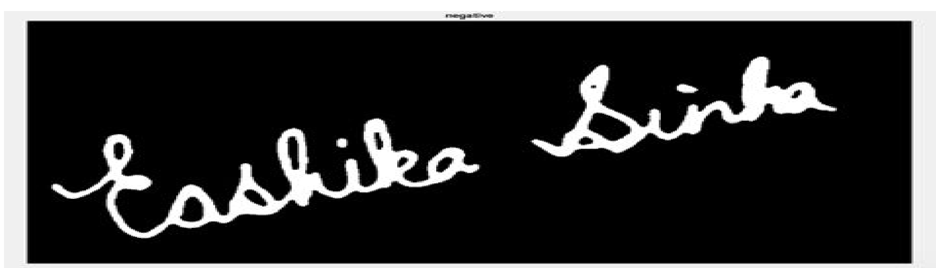


Fig 4:Negative Image

Fig 5:Cropped segmented image

5.3 FEATURE EXTRACTION

Feature Extraction is used to reduce the data by measuring certain "features" are get extracted from the processed image. After the preprocessing of the signatures, now they are ready for the feature extraction. Some useful features are get extracted from the signature portion area that helps to verify the signature of individuals. The different extracted features are discussed below.

1)**Height to Width Ratio** (F1)
The height and width may change however the height to width ratio of the signature area would remain nearly constant.

F1= (number of rows in cropped image / number of column in cropped image)

2)**Signature Occupancy Ratio** (F2)
The occupancy ratio of the image is the amount of space occupied by the signature within the whole image. Hence, it can be defined as the ratio of the number of pixels in the signature to the total Number of pixels in the cropped image.

F2 = (number of pixels comprising signature / number of pixels in the cropped image)

3)**Signature Density Ratio** (F3)
The density ratio of the image is obtained after partitioning the cropped image vertically into 2 equal halves and then calculating individual number of pixels comprising the signature in each of the parts.

F3 = (number of pixels comprising signature in part I /number of pixels comprising signature in part II)

4)Critical Points (F4)
The critical points or the corner pixels of the cropped image are detected using the Harris-corner detection algorithm. Harris Corner Detector provides a very robust way to detect corners in an image. The corner points are recognized by looking through small windows. Shifting a window in a flat region gives no

change of intensity in all directions where shifting a window for an edge gives no change of intensity along the edge direction but shifting a window for a corner region gives change of intensity all directions. Change of intensity for shift {u,v},

$$E(u,v)=\sum w(x,y)[I(x+u,y+v)-I(x,y)]^2$$

Window function

Shifted intensity

Intensity

For making corner detection E(u,v) have to make maximized.

Fig 6 : Negative Image depicting the critical points

19. Harris, C., Stephens, M.: A combined corner and edge detector. In: Proceedings of the 4th Alvey Vision Conference (AVC), pp. 147–151 (1988)

5)**Center of mass** (F5)

The center of mass of the signature gives the pixel where the concentration of the entire image pixel is localized.

$$x_{CM} = \frac{m_1 x_1 + m_2 x_2 + \dots}{m_1 + m_2 + \dots}$$

$$y_{CM} = \frac{m_1 y_1 + m_2 y_2 + \dots}{m_1 + m_2 + \dots}$$

Fig 7:Signature image depicting the center of mass(in red)

6)**<u>Slope of center of mass of two halves of the signature</u>** (F6)
After splitting the signature vertically into two halves the center of mass of each portion is find out and then the slope of the two center of mass is calculated.

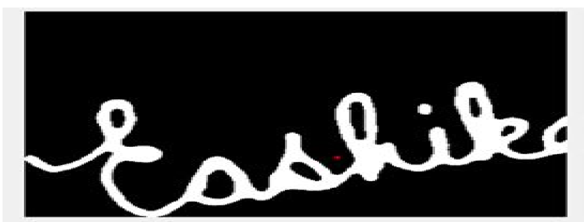


Fig 8:Com of left half

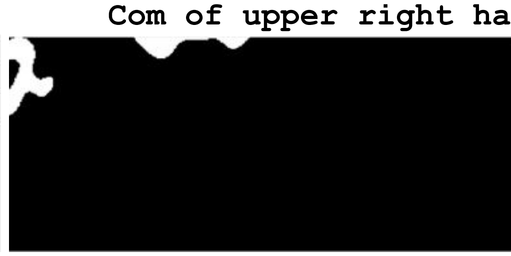
Fig 9:Com of right half

7)**<u>Center of mass of the sub-segments</u>** (F7)
For more critical analysis, the vertically splitted each two halves of signature portion is again splitted horizontally into two halves and the center of masses of those portions is get calculated.

Com of upper left half

Com of upper right half

Com of lower left half



Com of lower right half

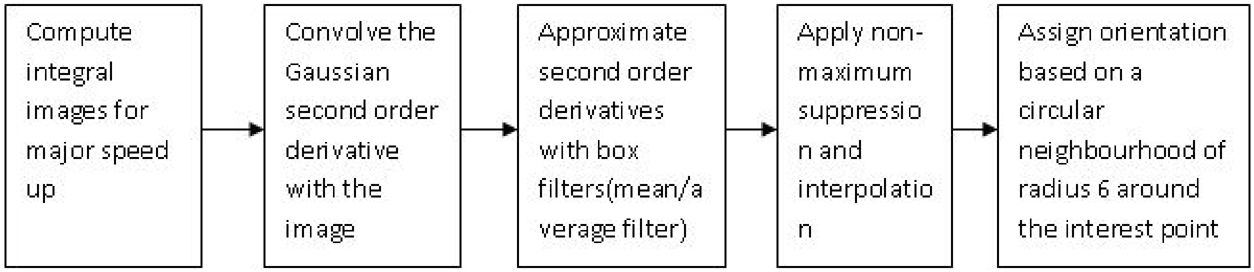
Fig 10

8)**Region Based Features** **(F8)**
First the connected region portions are find out from each signatures then some useful geometrical based features like are extracted from the each region portions of the signatures.

Fig 11 : Image depicting the regions

9)Speed Up Robust (SURF) Features **(F9)**
SURF is robust to the changes in viewing conditions, rotations and scale. SURF represents some useful feature points.

Fig 12 : Image depicting the surf-regions



5.4. Verification using Machine Learning Algorithms

The extracted feature vectors are used for the verification process of the signature using supervised machine learning algorithms like Support Vector Machine (SVM), Single Level Perceptron.

A) <u>Support Vector Machine(SVM):</u>

A Support Vector Machine (**SVM**) is a discriminative classifier formally defined by a separating hyperplane. In other words, given labeled training data (supervised learning), the algorithm outputs an optimal hyperplane which categorizes new examples in the classified categories.
In this project we trained the SVM model in weka with the acquired feature data to test them with the forged signature and thus evaluate the efficiency of the extracted features on the designed model.

B) <u>Single Level Perceptron:</u>

In machine learning, the perceptron is an algorithm for supervised learning of binary classifiers: functions that can decide whether an input (represented by a vector of numbers) belongs to one class or another. Perceptron which is popularly known as Single level Perceptron consists of only 2 layers.
Here, we have trained a single level perceptron model with the data acquired through feature extraction to detect any forged signature based on the trained learning.

From the features extracted from the testing data, SVM & Single Level Perceptron is trained and the corresponding trained models are now tested to detect the forged samples in Weka . Following are the Performance Tables showing the corresponding FRR and FAR percentages which gives light to the accuracy and efficiency of the devised models.

7. RESULT

I.Performance Analysis using Support Vector Machine: (same Table)

	Training Data	Testing Data	FRR %	FAR %	Accuracy
Person 1	10	13	21.39	78.61	76.7
Person 2	10	14	9.09	90.91	86.2
Person 3	10	11	25	75	83.4
Person 4	10	15	22.4	77.6	88.1
Person 5	10	14	15.34	84.66	85.4
Person 6	10	12	14.28	85.71	82.1
Person 7	10	13	16.67	83.39	88.3
Person 8	10	15	17.69	88.31	87.8
Person 9	10	11	16.67	83.34	84.3
Person 10	10	11	18.18	81.82	81.4

➔ As it can well be observed from the performance table , the devised model for verification gives an average rate of 76.16.3% accuracy on detecting the forged ones from the original true signatures.

II.Performance Analysis using Single Level Perceptron:

	Training Data	Testing Data	FRR %	FAR %	Accuracy
Person 1	10	13	15.38	84.62	96.7
Person 2	10	12	8.34	91.66	99.2
Person 3	10	15	20	80	97.4
Person 4	10	11	7.69	92.31	98.1
Person 5	10	14	9.09	90.91	95.4
Person 6	10	12	14.28	85.71	93.4
Person 7	10	13	16.67	83.39	98.3
Person 8	10	15	7.69	98.31	97.8
Person 9	10	11	6.67	93.34	97.3
Person 10	10	11	18.18	81.82	99.4

➔ As it can well be observed from the performance table , the devised model for verification gives an average rate of

97.3% accuracy on detecting the forged ones from the original true signatures.

8. CONcLUsioNs

This project has successfully achieved an offline signature verification model with extensive applications of machine learning . Training and testing model using Support Vector Machine & Single Level perceptron with success rate of 86.73%. This research work has been implemented with heavy applications in the fields of image processing and the contemporary popular machine learning . It presents a perfect model of combination of extensive applications of machine learning along with a holistic approach towards recognizing the unique features to be observed in a signature.

9. FUTURE WORK

This paper has focused on the offline signatures and the techniques that are used for the verification of signature for the classification of them into the genuine or forgery. The verification of signature is carried out on the basis of the features of signature that are extracted using different static image processing techniques and the statistical results obtained after implementing machine learning . As this paper contains the proposed model for offline signature verification engine in continuation to this the next objective will be to propose some new model that will reduce the FAR and FRR .

9. ACKNOWLEDGEMENT

This project has been successfully completed by our team under the watchful supervision of Dr Debasis De . We would like to express our deep gratitude to Miss Rituparna Saha and Professor Debasis De, our research supervisors, for their patient guidance, enthusiastic encouragement and useful critiques of this research work. I would also like to thank Timam Ghosh, for his advice and assistance in keeping our progress on schedule. My grateful thanks are also extended to Mr.Deepsubhra for his encouragement and regular updation of our progress to Dr. Debasis De.

We would also like to extend our thanks to the technicians of the laboratory of the computer science department for their help in offering the resources in completion of the project.

Finally, we would like to thank parents and friends for their support and encouragement throughout the progress of study and completion of the project successfully well within the deadline.

10. REFERENCE

[1]. N. Papamarkos, H. Baltzakis. Off-line signature verification using multiple neural network classification structures.

[2] R. Plamondon, G. Lorette, "Automatic Signature Verification and Writer Identification The State of the Art, Pattern Recognition" 22 (2) (1989) 107-131.
[3] Gonzalez R.C., Woods E., 'Digital Image Processing', Addison-Wesley,
[4] G. Dimauro, S. Impedovo, M.G.Lucchese, R.Modugno and G. Pirlo "Recent Advancements in Automatic Signature Verification", Proceedings of the 9th Int'l Workshop on Frontiers in Handwriting Recognition
[5] H. Baltzakis, N. Papamarkos, "A new signature verification technique based on a two-stage neural network classifier", Engineering Application of AI, Vol. 14 , 2001, pp. 95-103.
[6] R. Sabourin, R. Plamondon, L. Beaumier, "Structural interpretation of handwritten signature images", IJPRAI, Vol. 8, 3, 1994, pp.709-748.
[7] Banshidhar Majhi, Y Santhosh Reddy, D Prasanna Babu, "Novel Features for Off-line Signature Verification" International Journal of Computers, Communications & Control, Vol. I, No. 1, pp. 17-24, 2006.
[8] Migual A. Ferrer, Jesus B. Alonso and Carlos M. Travieso, "Off-line Geometric Parameters for Automatic Signature Verification Using Fixed-Point Arithmetic", IEEE Tran. on Pattern Analysis and Machine Intelligence, vol.27, no.6, June 2005.
[9] Debasish Jena, Banshidhar Majhi, Saroj Kumar Panigrahy, Sanjay Kumar Jena "Improved Offline Signature Verification Scheme Using Feature Point Extraction Method". [4] T.Y.Zhang, C.Y. Ceun "A fast algorithm for Thinning Digital Patterns".Communications of ACM, March 1988 Concepts of Image Processing.

18. Bay, H., Tuytelaars, T., Gool, L.V.: Surf: speeded-up robust features. Computer Vision—ECCV 2006. Lecture Notes in Computer Science, vol. 3951, pp. 404–417 (2006)