Journal of Experimental Research

September 2019, Vol 7 No 3

Email: editorinchief.erjournal@gmail.com editorialsecretary.erjournal@gmail.com

Received: *3rd January, 2020*
Accepted for Publication: *3rd July, 2019*

Design And Implementation Of Machine Learning-Based Signature Verification System (MLBSVS)

Nwobodo Nzeribe H.N[1].

Department of Computer Engineering[1],
Enugu State University of Science & Technology, Enugu, Nigeria.

***Author for Correspondence:** nnenna.nwobodo@esut.edu.ng

ABSTRACT

Handwritten signature is a behavioral trait in our societal and official life which can be used for human verification and authentication. Although a signature can be accepted only if it comes from an intended person, the possibility of more than one signature made by the same person being exactly the same is less. Some features of the signature may vary even when made by the same person, so detecting a falsified signature from an unauthorized person becomes a challenging task. This research work titled 'Design and Implementation of Machine Learning-Based Signature Verification System (MLBSVS) is aimed at developing an effective and reliable model that detects feature extracts to recognize signature using machine learning tools. The model is trained with datasets of signatures and predictions are made whether a provided signature is from an intended person or forged. This model will enhance *security in organizations for identification of unauthorized persons*. MLBSVS was developed and implemented using MySQL and MATLAB as Software requirements and the hardware requirements which include HP Proliant Micro Server with 6GB Memory, Processor speed of 1.5GHz, 250GB HDD and 1Gbps NIC, Client computer with 2GB Memory, Processor speed of 2.5 GHz, 250GB HDD and 100Mbps NIC, Visual Display Unit, Keyboard, mouse, scanner or camera and Ethernet cables. In conclusion, a system that can learn from signatures and make predictions whether a signature is genuine or forged has been successfully implemented.

Keywords: Signature, Machine learning, Forgery, Password, Verification

INTRODUCTION

In the past days, people were being identified using their names (first name, other name) with their surnames. The use of names for identification grew to the use of physical appearance, such as the skin color, height, face and color of eyes, etc. However, such physical aspects were just not enough for making a clear distinction among different people (Ahmed et al. 2013). Handwritten signature as an act of signing with a writing or marking instrument on a paper for authentication also came into being. Since signature is produced by movement of writing materials on paper, its attributes becomes form, movement and variation. These tend to introduce authentication problems (Zaidi and Mohammed, 2018).

In recent times some preliminary algorithms were designed to study such problems scientifically. With the advent of technology in past few decades, advanced computational tools came into play to become a bit easier means for identification of a particular person signature (Mariano et al. 2014). Some organizations like banks, insurance companies assign passwords and personal identification number to authenticate different users. However, there were two major issues with this approach: either these passwords were easily cracked or majority of these individuals just forgot them. As an immediate remedy, some other identification systems, such as passports or social security numbers (both of which are unique) were introduced (Breebaart et al. 2011). The problem was not fully resolved at this stage because even these passports can be manipulated or stolen.

To overcome the above mentioned challenges, the use of biometrics emerged. Biometrics is a science that examines and quantifies unique biological traits to verify the identity of an individual. Signature verification falls under this category.

Signature verification can be divided into offline and online signature verification depending on what data acquisition method is

used. In offline signature verification, the signature is on a document and is scanned to obtain its digital image representation. Online signature verification uses special hardware, such as a pressure-sensitive digitizing tablet, to record the pen tip movements during writing, while offline signature verification is used to verify signatures on bank checks, forensic studies and documents (Breebaart et al. 2011). Like in other biometric verification systems, first, users are enrolled to the system to create a database. During verification, the user presents a signature which the system compares with those signatures in the database to make an inference to determine the users' signature. If the dissimilarity exceeds a certain entry, the signature is rejected. This research work explores the use of machine learning methods to design and implement an offline signature recognition and verification system using MySQL and MATLAB with its hardware requirements.

MATERIAL AND METHODS

Signature writing is a behavioral biometric which can change over time. Since this alters over time, verification and authentication of signature may take time and may increase chances of errors over time in some instances. An inconsistent signature of an individual leads to higher false rejection rates (Bromley et al.1993). The methodologies applied include image data acquisition, image pre-prosing and noise removal, segmentation and machine learning feature extraction. This involves software system and hardware requirements.

Software Requirement

The software tools used include MySQL for creating the database and MATLAB used for its implementation. MATLAB is a high-performance language for technical computing machine learning and computer vision technology. It integrates computation, visualization and programming in an easy-to-use environment where problems and solutions are expressed in familiar mathematical notation. MATLAB allows matrix manipulations, plotting of functions and data, implementation of algorithms, creation of user interface and interfacing with programs written in other languages, including C, C++, Java, FORTRAN and Python.

Hardware Requirements include:

HP Proliant Micro Server with 6GB Memory, Processor speed of 1.5GHz, 250GB HDD and 1Gbps NIC., Client computer with 2GB Memory, Processor speed of 2.5GHz, 250GB HDD and 100Mbps NIC, Visual Display Units, Keyboard and mouse, scanner/Camera and Ethernet cables.

Block Diagram of Machine Learning-Based Signature Verification System (MLBSVS)

The block diagram of Machine Learning-Based Signature Verification System (MLBSVS) is as shown in figure 1. The signature is written on a paper and captured in image format using a scanner or camera. Then the image undergoes through pre processing stage where thinning and resizing takes place, then the segmentation. For authentication of signatories in the database, the entire database features are trained and classified using machine learning. During signature verification, the extracted features of the investigated signature are compared with the trained features in the database to determine the original signature from the forged one. The system flowchart is as shown in figure 2

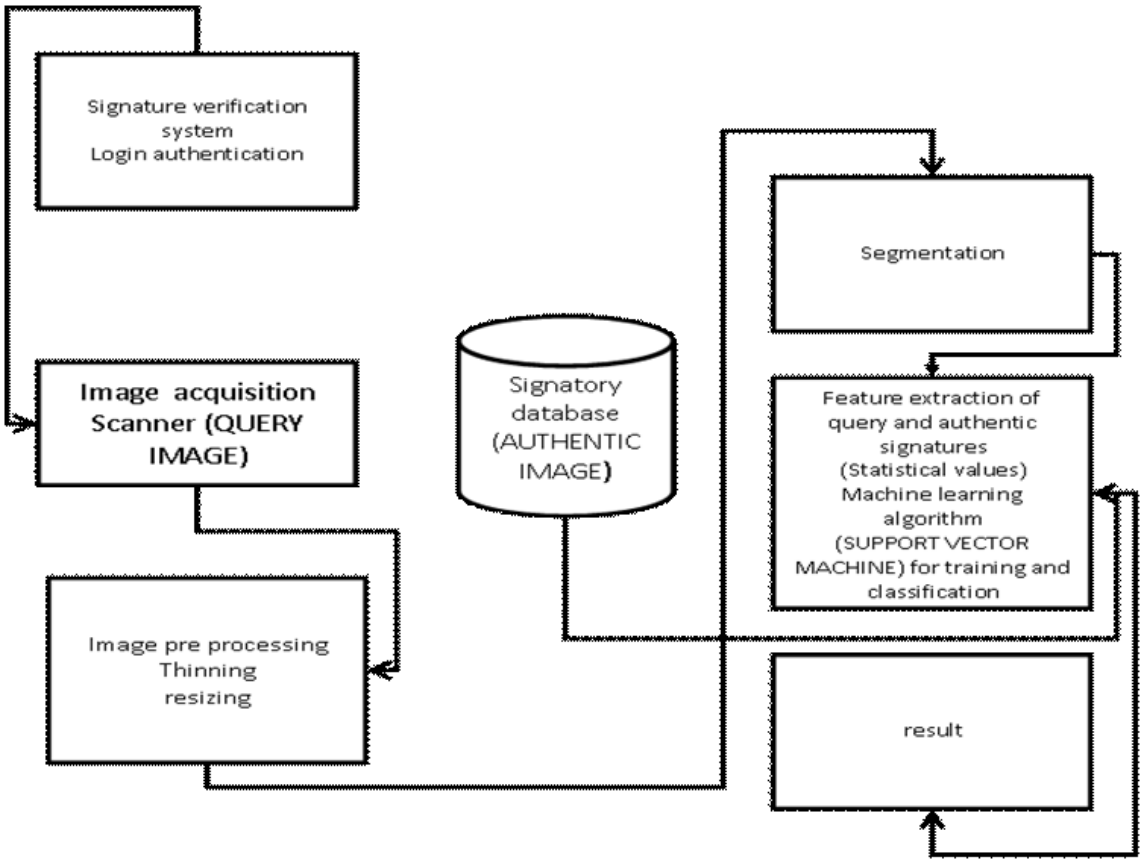

Figure 1: Block diagram of Machine Learning-Based Signature Verification System

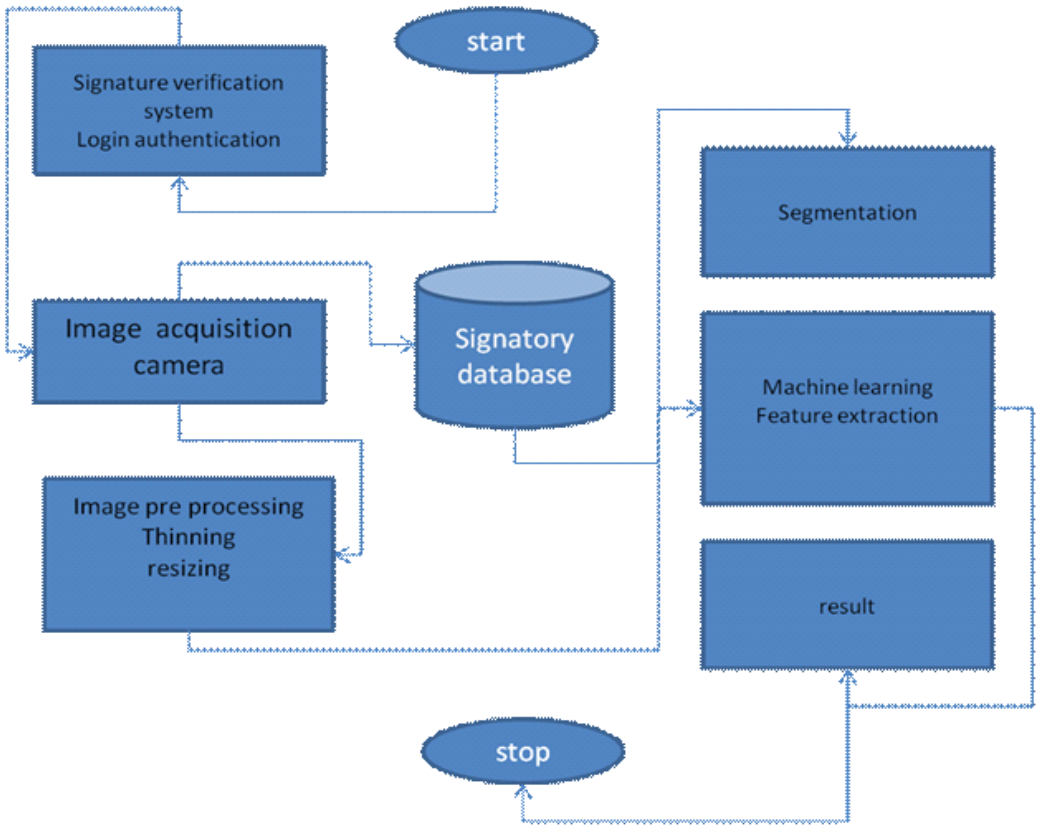

Figure 2: System Flowchart of Machine Learning-Based Signature Verification System

RESULT AND DISCUSSION

MATLAB functions from the image processing tool and techniques were used to pre-process the signature images and split them into training sets. While using MATLAB in an image processing technique, it stores an intensity image as a single matrix, with each element of the matrix corresponding to one image pixel. The elements in the intensity matrix represent various intensities or gray levels, where the intensity 0 represents black and the intensity 1 represents full intensity or white part of an image.

Figure 3 and figure 4 shows the model of the input and output design the system in respectively in MATLAB environment.

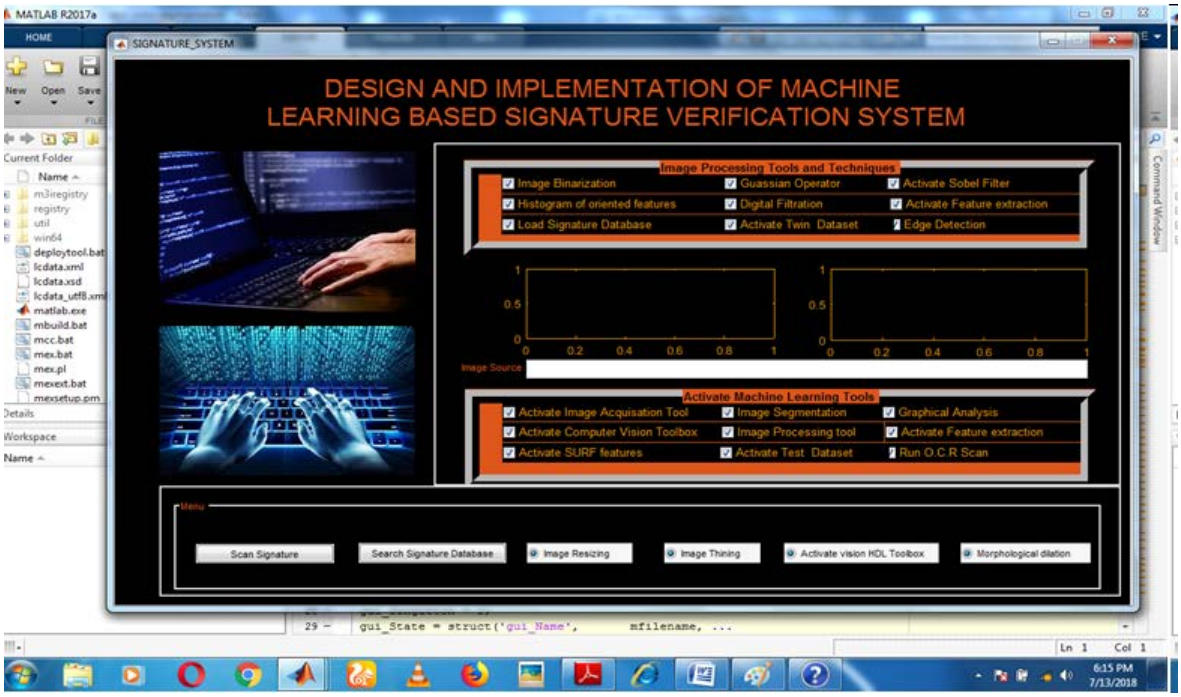

Figure 3: Model of the input design

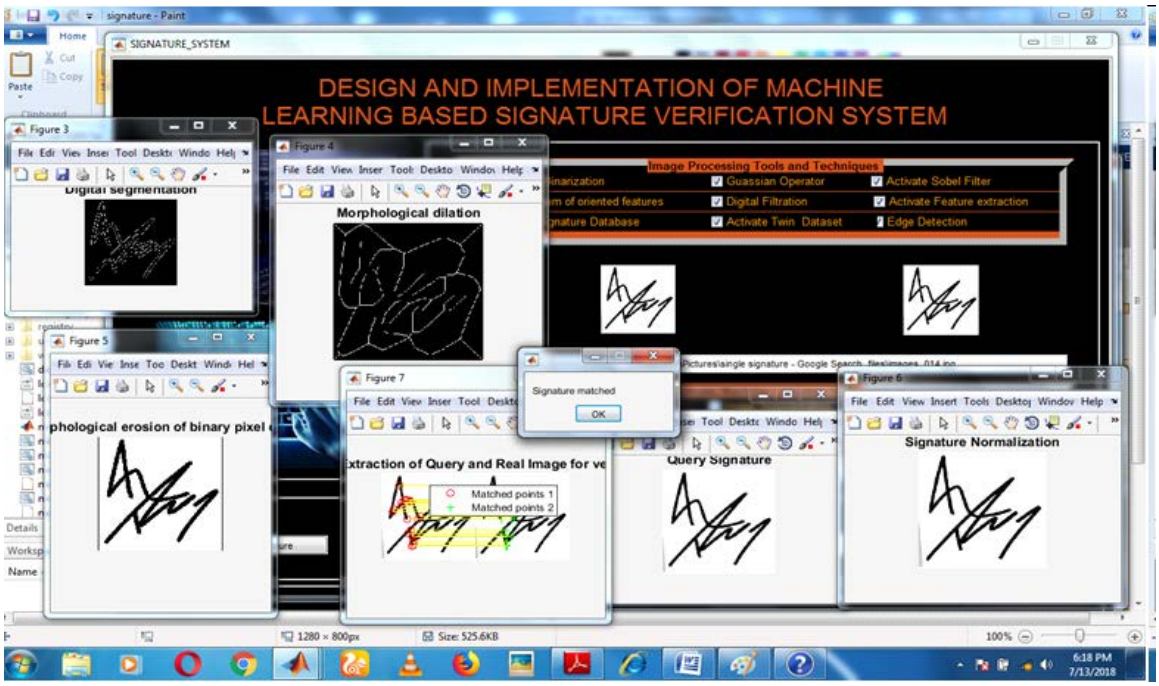

Figure 4: Model of the output design

This work employs a signature database that contains approximately hundred signatures of both genuine and forged signatures for testing and recognition of genuine ones. The result showed that all the genuine signatures were matched and recognized exactly while the unmatched signatures were also identified as forgery by the system.

CONCLUSION:

In conclusion, a system that can learn from signatures and make predictions whether a signature is genuine or forged has been successfully implemented. This model can be deployed in government and private establishments where handwritten signatures are used for verification and authentification of persons to identify forgery.

REFERENCES

Ahmed R, Baena ML, Elizondo D, Rubio EL, Palomo EJ, Watson T. (2013). Assessment of geometric features for individual identification and verification in biometric hand systems Expert Systems with Applications 40(9) pp 3580-3594.

Breebaart J, Buhan I, Groot K, Kelkboom E. (2011). Evaluation of a template protection approach to integrate fingerprint biometrics in a PIN-based payment infrastructure, Electronic Commerce Research and Applications. 10(6) pp 605-614.

Bromley J, Bentz J, Bottou L, Lecun IGY, Moore C, Sackinger E, Shah R. (1993). Signature verification using a siamese time delay neural network, International Journal of Pattern Recognition and Artificial Intelligence 7(4) pp 669-688.

Mariano J, Amaral LM, Lopes AJ, Jansen JM, Faria ACD, Melo PL. (2014). An improved method of early diagnosis of smoking-induced respiratory changes using machine learning algorithms, Computer Methods and Programs in Biomedicine 112(3), pp 441-454.

Zaidi SFA, Mohammed S. (2018). Biometric Handwritten Signature Recognition, TDDD17: Information Security Course , Linkopingsuniversilet Sweden