www.ijecs.in
International Journal Of Engineering And Computer Science
Volume 8 Issue 6 June 2019, Page No. 24686-24692
ISSN: 2319-7242 DOI: 10.18535/ijecs/v8i06.4327

Digital Signature Verification System to Enhance Customer Services in the Banking Industry

Asogwa Tochukwu Chijindu[1], Ugwu Edith Angela[2], Aniekwe Steven[3]
[1,2]Computer Science, Enugu State University of Science and Technology, Enugu, Nigeria
[3] Computer Science, Institute of Management and Technology, Enugu, Nigeria

Abstract
Recently in most banks (especially in Africa), there exist various cases of banking staff denying services to customer due to signature differences. This has resulted to a lot of misunderstandings, insults, quarrels, and even losses to most financial institutions. This work presents digital signature verification system to enhance customer services in the banking industry, with the aim of improving the staff customer relationship within the banking domain. This will be developed using image acquisition tool, image processing tools and machine learning (clustering technique). The system will be implemented using mathlab as the software development too. The accuracy of 98% was recorded as the system was validated using a prepared testing and training image containing various real and forged signatures.

I. Introduction

Centuries ago, the conventional approach for person identification was simple. Due to low population size then, people are easily recognized by their surname, skin colour, language, gender, occupation, face and height. Over time, a rapid increase in global population was experienced, and thus these traditional means of recognition became unreliable.

Serial and registration numbers were introduced and assigned to clients and customers as a primary key in various enterprises and even in the academic institutions for person identification, but as the numbers keep increasing due to population growth, the problem of identity identification was not solved fully.

The banking industries were one of the major sectors that were affected by the massive population growth of human. This is due to the fact that there is need for a robust technique or system that will be used for customer identification.

Recently, Biometric technology became available to allow recognition and verification of "true" individual identity [1] [2] through physical (face recognition, iris recognition, finger print technology) and behavioral (handwriting, signature, voice) modalities.

However, the current state of art in most banking industries today, especially in micro finance banks are not fully equipped with the biometric technologies inspired by physical modalities even though few commercial banks have finger print verification system, but it is not without its challenges (hardware failure).

Signature has been globally accepted as a general means of official authentication, for legal documents, cheques, bank drafts, tellers, withdrawal slips, deposit slips, receipts, and other official papers. This means has been widely accepted and implemented in all banking sectors due to its simplicity, confidentiality, and unique nature, also compared to other biometric verification systems, human signature is one of the few biological modalities that remain the same over time.

This authenticating means have been abused time and time again through impersonation (identical twins) and forgery, as a result has caused a lot of damages and losses to individuals and financial institutions. This research work redresses this challenge using artificial intelligent technique to

present a novel signature verification system that help authenticate business transactions in all financial institution.

Research Objectives

i. To develop a signature verification system using clustering technique
ii. To improve customer and staff relationship within the banking sector
iii. To provide a reliable and easy means of bank document verification
iv. To prevent theft as a result of forgery and same identity

II. Methodology

This work will use the clustering technique to solve this problem employing image acquisition tools, image processing tools, training image, testing image and unsupervised machine learning technique.

Image acquisition: this is the first step, which involves acquiring the testing signature of the customer using preferably HD scanner (testing documents).

Image processing: this involves various procedures to prepare the signature for feature extraction. The procedures are binarization, segmentation, morphological erosion and dilation, and normalization.

Binarization: this technique is a preliminary processing step that converts the signature image to bi-level format (black and white)

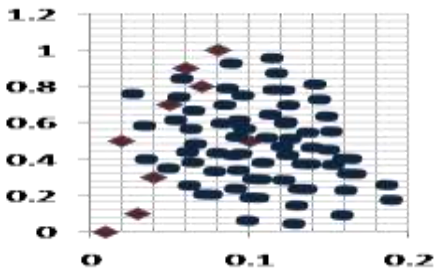

Figure (a)

Verification: this is the final process of the signature verification system using a matching point of the feature descriptor predicted by the exhaustive k-nearest neighbor search method [4] according to the equation 2. However we recommend approximate k-nearest neighbor method can be used in a bigger dataset.

Segmentation: this image processing technique is employed to map the regions, curves and graphological patterns of the signature image.

Morphological dilation and erosion: this technique applies structural element to the signature image, based on the style of the signature and hence create a resultant output of optical character image with similar pattern.

Image Normalization: this procedure not only removes noise from the image but also bring the image to a range of intensity value that is normal for feature extraction process.

Feature extraction: this process involves the dimensional reduction of the signature image into a compact feature vector (i and j) using Hough transform.

Clustering technique: this technique compare the extracted feature vectors using the equation presented in [3] equation 1, using the relative angle (**P**) to generate the vector variables (I and j) with RL corresponding to the length of each features (i) in matrix column (mi by n) and (j) in matrix (mj by n). The feature vectors (i and j) are presented in the clustering diagram (a) and (b) respectively. The clustering technique computes the average μi for each row i of (RL, **P**) and the relative distance between each point on the row (Ri, **P** i) as shown in figure (c)

$$R = \frac{\min(\|i\|,\|j\|)}{\max(\|i\|,\|j\|)} \ldots\ldots\text{equation (1)}$$

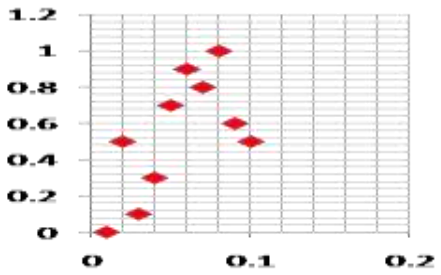

figure (b)

$$q = \underset{q=1,\ldots,k}{\arg min} \sum_{k=1}^{k} T\left(\frac{k}{x}\right) C\left(\frac{q}{k}\right) \ldots\text{equation (2)}$$

Where: q is the predicted classification.
k is the number of classes.
$T\left(\frac{k}{x}\right)$ is the posterior probability of class k for observation i.

$C\ (\frac{q}{k})$ is the cost of classifying an observation as j when its true class is k

Implementing the function given a set i of j points at distance RL in equation (i),) searches for the (k) closest points as outliners in figure (d)

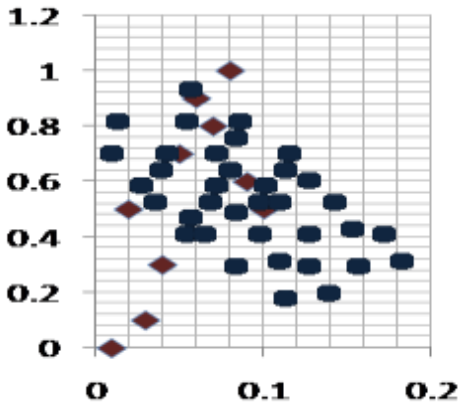

Figure (c)

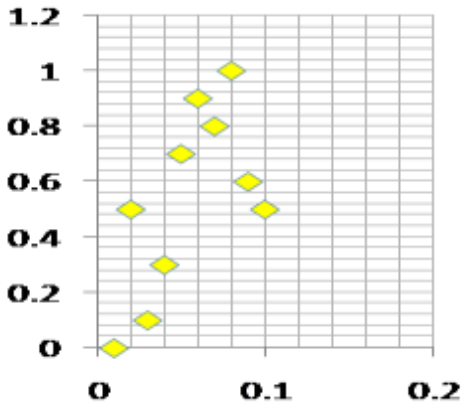

figure (d)

III. System Implementation

This involves the necessary tools employed to bring this novel idea to reality. In this work we employed the optical character recognition technique of image acquisition (scanner) to create our datasets. Then mathlab was used as the software developing tool, this choice was due to its rich image processing features which along the line determines to a high extent the accuracy of the system. From the results presented in the figure (e), the customer signature is scanned and uploaded for image processing. The respective result of the morphological operations, segmentation and normalization process are presented with figure (f) and (g), the matching results are presented in figure (h). Another test was performed using figure (i) between an authentic signature and a forged signature,

the result is presented in figure (j).

Figure (e) query signature from customer

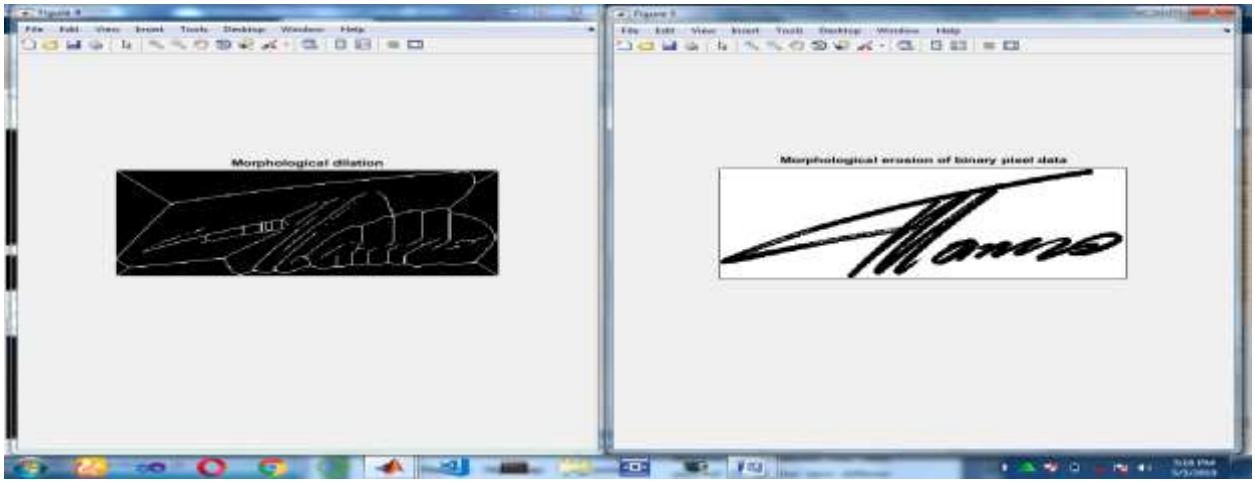

Figure (f) model of the morphological operations result

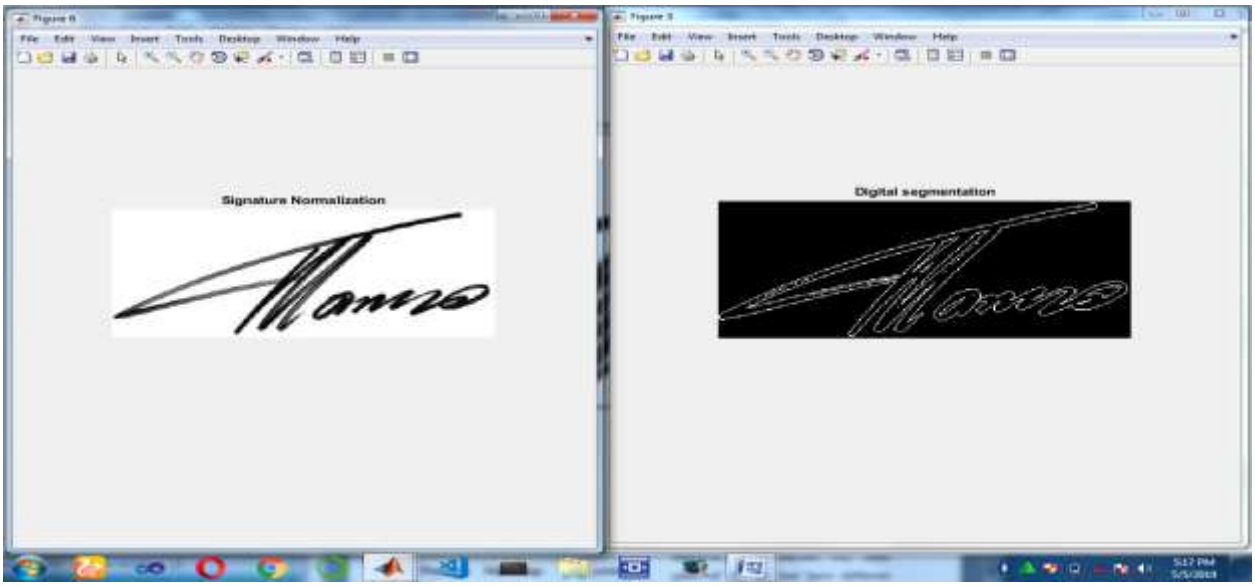

Figure (g) model representing the normalized and segmented signature

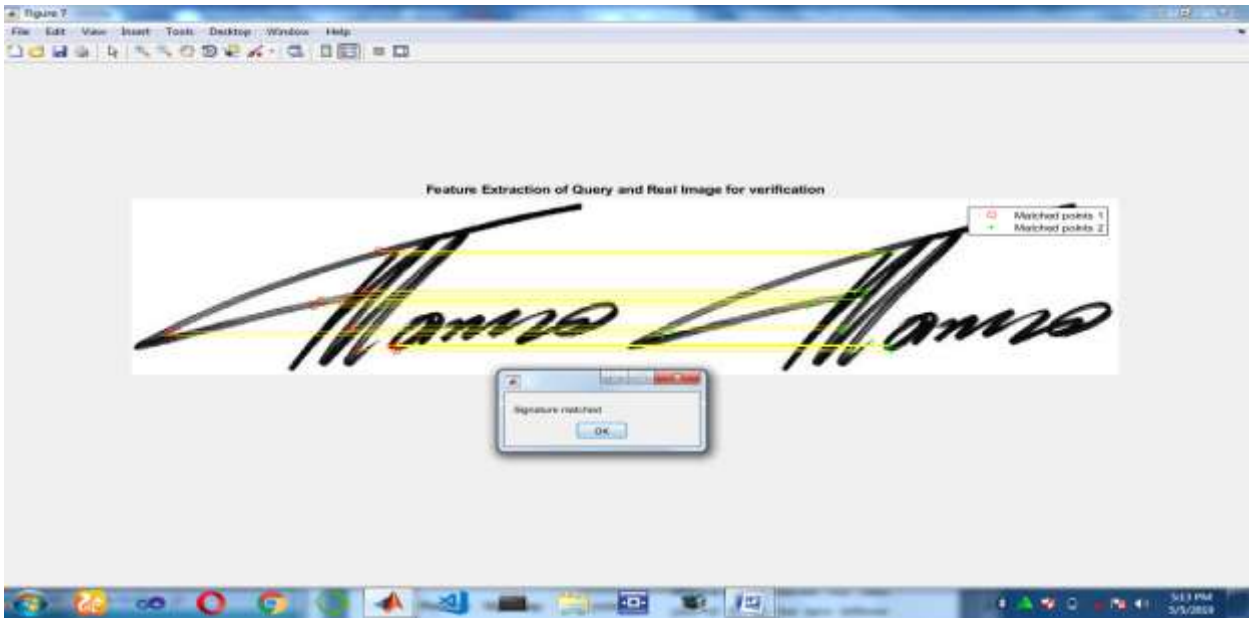

Figure (h) result of matched signatures (showing feature points i and j)

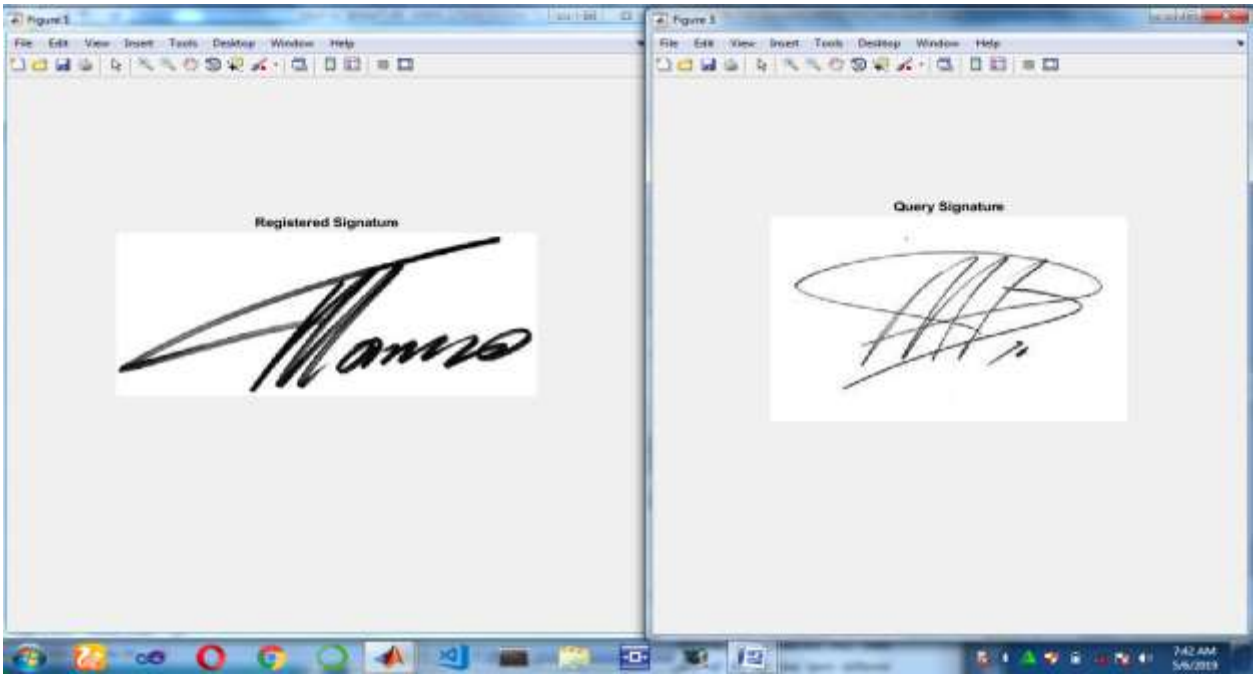

Figure (i) result of the forged and authentic signatures to be verified

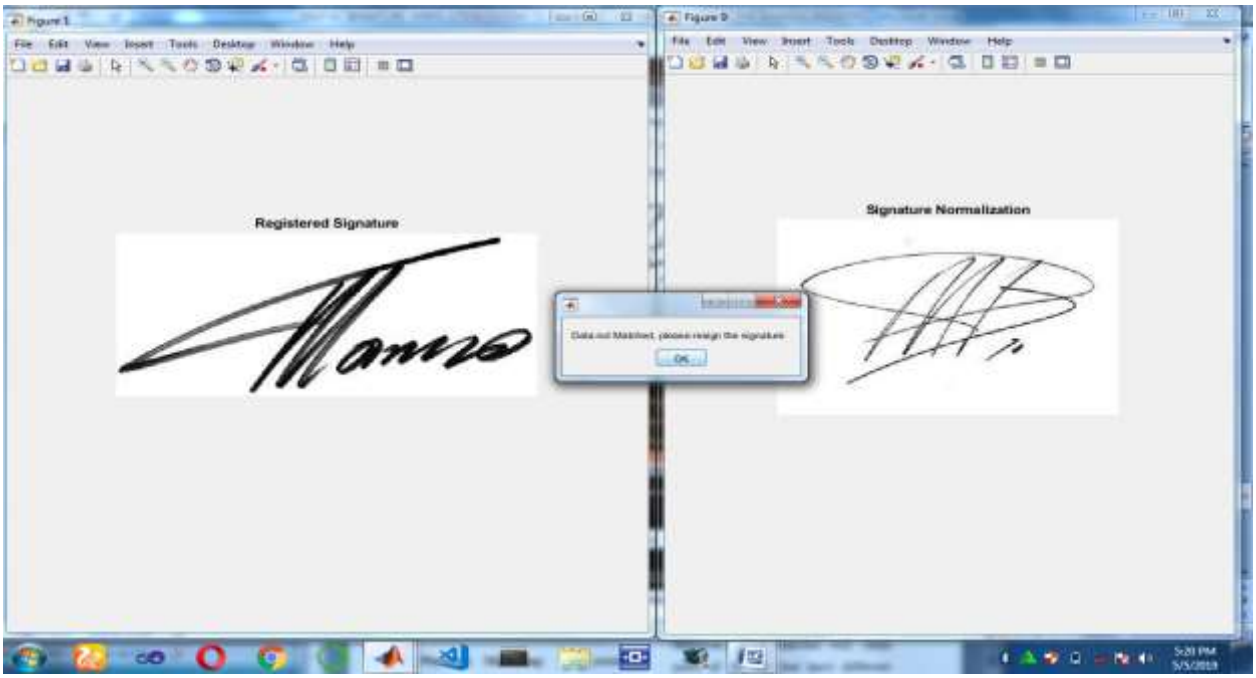

Figure (j) result of not matched signatures

IV. Changeover Style

This refers to the methodology at which the new system is introduced to banks. The parallel changeover style is suggested here for use since the banking system is already designed but lacking this verification technology. According to [5], parallel method is applied when two system are allowed to operate simultaneously. In this case the existing system is still in use while the new system is introduces as a supplement.

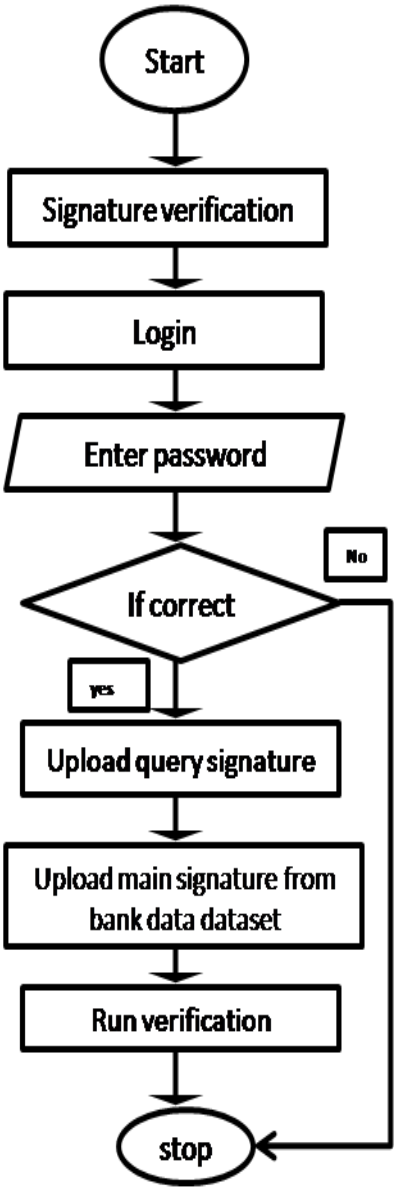

Figure (l): system flow chart.

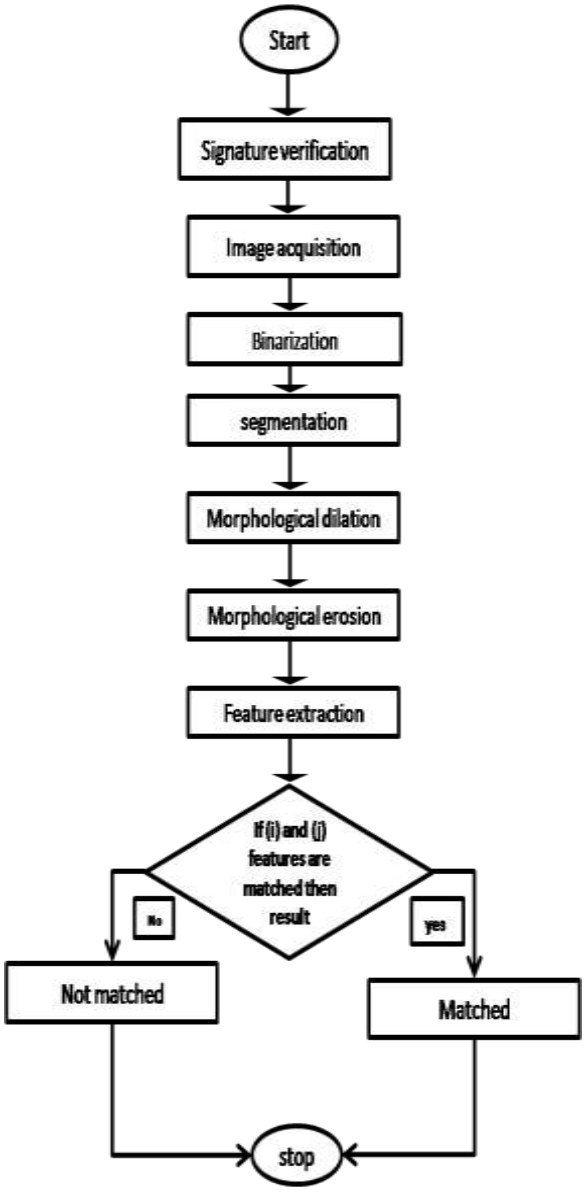

Figure (m): process flow chart

V. Conclusion

The traditional approach for signature verification in the bank uses the human sense organ (eyes), and most times human judgment based on what is sees can be queried, especially in cases of impersonation, forgery, identity manipulation to mention a few. Today the quest for fast money have driven lots of frustrated people into various illegal acts and signature forgery is one of the most common of this act. Banks and their customers occasionally falls victim, due to the fact they lack adequate technology to verify signatures. This research work has successfully developed a new signature verification system with a very high accuracy of 98%.

Reference

1. Chioma O (2018). Implementation Of Daugman's Algorithm And Adaptive Noise Filtering Technique For Digital Recognition Of Identical Twin Using Mathlab,
2. Asogwa T.C and Ituma C. (2018); the application of machine learning for digital recognition of identical twins to support global crime investigation.
3. Anders Hast And Andrea Marchetti (2012). Putative Match Analysis A Repeatable Alternative To Ransac For Matching Of Aerial Images;- International Conference On Computer Vision Theory And Applications..

4. Muja, M., and D. G. Lowe (2009). "Fast Approximate Nearest Neighbors with Automatic Algorithm Configuration." International Conference on Computer Vision Theory and Application; VISAPP.
5. Asogwa T. C (2019) ; Facial recognition system for digital crime management (unpublished)