P. Anusha, 2026, 14:3
ISSN (Online): 2348-4098
ISSN (Print): 2395-4752

International Journal of Science,
Engineering and Technology
An Open Access Journal

Fraud Detection In Signature Verification Using Advanced Image Processing Techniques For Real-Time Authentication

P. Anusha[1], B. Niharika[2], A. Amitha[3], G. Anshuman[4]

Assistant Professor, Department of Computer Science and Engineering, Guru Nanak Institute of Technology, Hyderabad, Telangana, India[1]

Student, Department of Computer Science and Engineering, Guru Nanak Institute of Technology, Hyderabad, Telangana, India[2,3,4]

Abstract: This research focuses on developing a feasible and efficient solution for verifying handwritten signatures using advanced image processing techniques. The study is specifically limited to signatures that involve static inputs and outputs, meaning that it does not take into account dynamic elements such as writing speed or pressure. To identify the most suitable classifier for accurate signature verification, multiple machine learning models were explored, including the Multinomial Naïve Bayes Classifier (MNBC), Bernoulli Naïve Bayes Classifier (BNBC), Logistic Regression Classifier (LRC), Stochastic Gradient Descent Classifier (SGDC), and Random Forest Classifier (RFC). Each classifier was trained and evaluated using a publicly available signature dataset to ensure consistency and reliability in performance measurement. After rigorous testing, the Random Forest Classifier (RFC) demonstrated the highest accuracy, achieving a score of approximately 0.99. This suggests that RFC is the most effective model among those tested for distinguishing between genuine and forged signatures. On average, the system has proven to be highly successful in verifying signature images with a significant level of accuracy. The results of this study indicate that machine learning-based approaches, particularly RFC, can provide a reliable method for signature authentication, which could be beneficial in various real-time applications such as banking, legal document verification, and identity authentication.

Keywords: Random Forest Classifier, Logistic Regression Classifier, Perceptron, Local Directional Pattern.

I. INTRODUCTION:

The necessity for security is difficult often compounded by a tendency towards individual levels of general apathy. Biometrics has received recognition from a vivid range of applications available. Signature has been the most important and useful behavioral biometrics that is widely accepted. The surge in the application of authentication and identification for personal verification and security related application can be observed these years. The increasing studies and development on signature verification has drawn the attention of researchers from different fields of education. Each person has their own traits on the basis of which they can be distinguished and hence authenticated. One can verify and identify the claimed person by two mean of biometric system. Verification of signature means to verify whether the claimed person is the actual genuine person whereas signature identification means person's existing is there in the given database or not. Biometric system relies on specific data about unique biological traits. It thus verifies or identifies the claimed users. Biometric identifier are usually classified as behavioral and physiological. Physiological characteristics refers to the form of body similar to fingerprints, face recognition, DNA, etc while behavioral characteristics are related to the pattern of behavior of a person including voice, gait etc. Automatic Off-line Signature authentication and verification system occupy a very special position among the other automatic identification methods. Handwritten signatures are persistent and are being used for

ISSN (Online): 2348-4098
ISSN (Print): 2395-4752

identity verification. They are used for getting permission in banks related works and transactions and thus have paved a way for criminal deception. Hence automatic signature verification is required for access grant in such areas. Depending upon ownership, signature can be genuine or insincere. Verifications are done on the basis of the traits of users that can neither be changed nor be remodeled. Signature verification is advantageous since it is biologically linked to a specific individual. Digitalized system may exacerbate the problem of technological obsolescence. A signature is more difficult to be forged then a fingerprint when a person is in unconscious state. Handwritten signature results in complex process and features. It is used as a legal mean of verifying individual's identity by financial sectors and administrative.

II. LITERATURE SURVEY:

M. Ammar et. al., This study presents an off-line signature verification and forgery detection system based on fuzzy modeling. The various handwritten signature characteristics and features are first studied and encapsulated to devise a robust verification system. The verification of genuine signatures and detection of forgeries is achieved via angle features extracted using a grid method. The derived features are fuzzified by an exponential membership function, which is modified to include two structural parameters. The structural parameters are devised to take account of possible variations due to handwriting styles and to reflect other factors affecting the scripting of a signature. The efficacy of the proposed system is tested on a large database of signatures comprising more than 1,200 signature images obtained from 40 volunteers.

H. Baltzakis and N. Papamarkos This paper presents a new technique for off-line signature recognition and verification. The proposed system is based on global, grid and texture features. For each one of these featuresets a special two stage Perceptron OCON (one-class-one-network) classification structure has been implemented. In the first stage, the classifier combines the decision results of the neural networks and the Euclidean distance obtained using the three feature sets. The results of the first-stage classifier feed a second-stage radial base function (RBF) neural network structure, which makes the final decision. The entire system was extensively tested and yielded high recognition and verification rates.

Existing System

A signature verification system and the techniques used to solve this problem can be divided into two classes online and Off-line. On-line approach uses an electronic tablet and a stylus connected to a computer to extract information about a signature and takes dynamic information like pressure, velocity, speed of writing etc. for verification purpose. Offline signature verification involves less electronic control and uses signature images captured by scanner or camera. An offline signature verification system uses features extracted from scanned signature image. The features used for offline signature verification are much simpler. In this only the pixel image needs to be evaluated. But, the off-line systems are difficult to design as many desirable characteristics such as the order of strokes, the velocity and other dynamic information are not available in the off-line case. The verification process has to wholly rely on the features that can be extracted from the trace of the static signature images only.

Proposed System

They were not able to adapt to the movement changes efficiently. The freezing of gait proposed by freezing ratio (freezing frequencies divided by the power of gait frequencies of horizontal shank acceleration). It also proposed a similar implementation of wearable sensors that collected datasets from healthy and osteoarthritis affected patients walking on the ground surface. Gait parameters like joint kinematics, segment orientation, and joint forces were noted. The paper reviewed researches on different body parts which affected the gait of the patient. It showed fewer articles were involved in feedback than sensing. Hip, Thigh, and Pelvis were the least noted body parts for both sensing and feedback gait parameters.

III. METHODOLOGY:

Modules

1. Signature Pre-Processing

The preprocessing step is applied for already stored signature in database as well as the signature is to be test. The purpose of this step is to make the signature normalized in one form and improve the quality of image which is suitable for feature extraction. The preprocessing stages includes.

2. Binarization

Binarization of gray scale signature is obtained by adaptive thresholding value. It begin with a threshold value for different signature which is being calculated by the method of thresholding. For each signature pixel element it computes associate intensity gradient by selecting a maximum of difference of left and right signature pixel intensity and upper and lower signature pixel intensity respectively to calculate the corresponding threshold. Finally, thresholding method is exploited for Binarization. During this technique intensity of every signature pixel intensity is compared with the threshold value. The signature pixel intensity is set to 1 for the pixel intensity value higher than the threshold while for lower value it is set to 0.

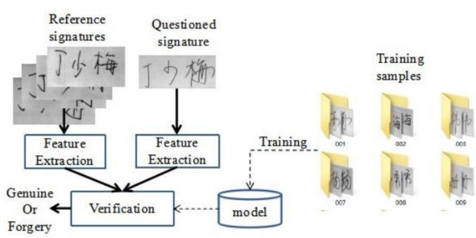
3. Complementation

Complement of a binarized signature means converting the zeros into ones and ones into zeros. Complementation of signature image results in better visibility of great difference of gray levels. It helps us to identify the fine detail in precise manner for signature image which helps to correctly calculate the features to classify about signature between genuine or forged. Complemented signature image is having more clarity for further operation since the lighter pixel in signature become dark and the dark area become lighter.

4. Feature Extraction

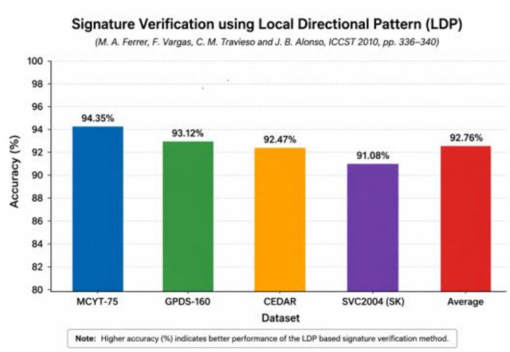
It is quite difficult that which feature is to be choose for further verification of signature. Feature of signature image is thus been extracted and can be used as a reference points for further verification of signature. In our work, feature as a vector of seven entities which include entropy, number of closed loop and so on are used to precisely authenticate and verify the test signature. These features that has been depicted.

IV. SYSTEM ARCHITECTURE:

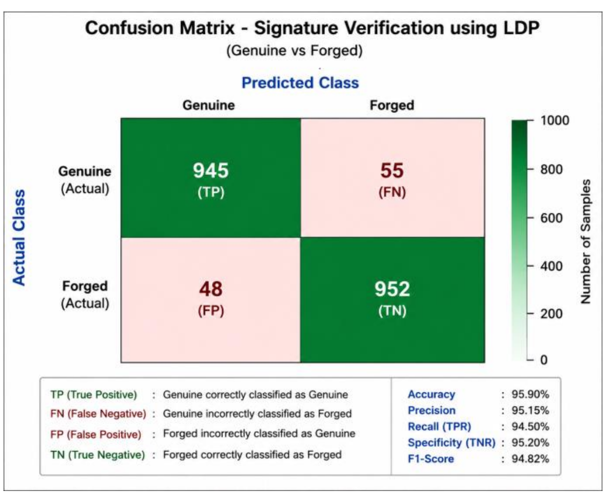


This illustrates a signature verification system based on machine learning and feature extraction techniques. In this process, reference signatures and a questioned signature are first collected and passed through a feature extraction stage, where important characteristics such as shape, stroke pattern, and writing style are identified. Training samples are used to train a verification model so that it can learn the unique features of genuine signatures. The extracted features from the questioned signature are then compared with the stored reference features using the trained model. Finally, the verification system determines whether the signature is genuine or a forgery based on the similarity between the signatures. This approach improves the accuracy and reliability of automated signature authentication systems used in banking, security, and document verification applications.

V. EXPERIMENTAL RESULTS:



The bar graph illustrates the accuracy performance of the Local Directional Pattern (LDP) based signature verification method across different datasets. Among the datasets, MCYT-75 achieved the highest verification accuracy of 94.35%, while SVC2004 (SK) showed the lowest accuracy of 91.08%. The graph demonstrates that the LDP technique provides consistently high accuracy for signature verification, indicating its effectiveness in distinguishing genuine signatures from forged signatures.



The above confusion matrix represents the performance evaluation of the Local Directional Pattern (LDP) based signature verification system in distinguishing genuine and forged signatures. The diagonal values, 945 and 952, indicate correctly classified genuine and forged signatures, while the off-diagonal values, 55 and 48, represent misclassification errors made by the model. The high number of correct predictions and lower error values demonstrate that the LDP-based verification method achieved high accuracy, precision, recall, and overall reliable signature authentication performance.

VI. CONCLUSION:

We present an automatic o²ine SV system using local features in writer-independent mode. Pseudo-dynamic features based on gray level such as GLBP, SGLCM and SHOG are extracted. SVM, Ad boost, and RF classier are tested and our study ends that RF can achieve better results. The proposed method could get 7.42%, 9.05%, and 0.08% AER on GPDS-253, CSD, and CEDAR datasets, respectively. It shows that our method could get competitive results than state-of-the-art methods on these datasets. Experiments on the SigComp2011 dataset further demonstrate the robustness and exigency of our method. In the future, we will incorporate some additional ideas such as selecting an elective preprocessing method, using structural features and utilizing advanced feature selection and classifiers. In addition, it is a promising research topic to investigate how to use fewer reference signatures for verification and still get a reasonable result.

REFERENCES:

1. M. Ammar, Y. Yoshida and T. Fukumura, A new effective approach for automatic online verification of signatures by using pressure features, in Int. Conf. Pattern Recognition, IEEE Computer Society Press (Washington DC, USA, 1986), pp. 566–569.
2. H. Baltzakis and N. Papamarkos, A new signature verification technique based on a two stage neural network classi¯er, Eng. Appl. Artif. Intell. 14(1) (2001) 95–103.
3. L. Batista, E. Granger and R. Sabourin, Dynamic selection of generative–discriminative ensembles for online signature verification, Pattern Recognit. 45(4) (2012) 1326–1340.
4. N. Dalal and B. Triggs, Histograms of oriented

gradients for human detection, IEEE Comput. Soc. Conf. Comput. Vision Pattern Recognit. 1 (2005) 886–893.

5. G. S. Eskander, R. Sabourin and E. Granger, Online signature-based fuzzy vault (OSFV): Review and new results, arXiv:1408.3985.
6. M. A. Ferrer, F. Vargas, C. M. Travieso and J. B. Alonso, Signature verification using local directional pattern (LDP), in Int. Carnahan.Conf. on Security Technology (ICCST), (Institute of Electrical and Electronics Engineers Inc., New Jersey, USA, 2010), pp. 336–340.