International Journal of Early Childhood Special Education (INT-JECSE)
DOI:10.48047/INTJECSE/V15I4.91 ISSN: 1308-5581 Vol 15, Issue 04 2023

SIGNATURE VERIFICATION WITH IMAGE PROCESSING USING PYTHON

Mrs. A ANITHA REDDY
Assistant Professor, Department of CSE Sreyas Institute of Engineering and Technology, Telangana, India.
Anitha.a@sreyas.ac.in

MAMIDI PRAFUL REDDY
Department of CSE
Sreyas Institute of Engineering and Technology, Telangana, India.
mamidi.prafulreddy1@gmail.com

PRERANA GANJI
Department of CSE Sreyas Institute of Engineering and Technology, Telangana, India.
ganjiprerana1531@gmail.com

RAMAGALA NAVEEN KUMAR
Department of CSE Sreyas Institute of Engineering and Technology, Telangana, India.
Naveenkumar63025@gmail.com

BHOOMI SUSHMA
Department of CSE Sreyas Institute of Engineering and Technology, Telangana, India.
Sushmabhoomi2002@gmail.com

ABSTRACT

This research was conducted to find a feasible solution to verify handwritten signatures. The scope has been narrowed down to signatures which contain static inputs and outputs. Several classification methods such as Multinomial Naive Bayes Classifier (MNBC), Bernoulli Naive Bayes Classifier (BNBC), Logistic Regression Classifier (LRC), Stochastic Gradient Descent Classifier (SGDC) and Random Forest Classifier (RFC) were implemented to identify the most suitable classifier to verify handwritten signatures. The classifiers were trained and tested using a signature database available for public use. The best performance was obtained from RFC with an accuracy score around 0.99. For an average, the system created has been successful in verifying signature images provided with a considerable accuracy level.

INTRODUCTION

The need for security is sometimes complicated by a proclivity towards individual levels of general disinterest. Biometrics has gained popularity due to the wide variety of applications accessible. The most crucial and helpful feature has been signature. A generally recognized behavioral biometrics. The increased use of authentication and identity for personal purposes. These years have seen an increase in the use of verification and security applications. growing research and development on Signature verification has piqued the interest of educators from all disciplines. Everyone has their own. They have characteristics that allow them to be identified and hence authenticated. The alleged person can be verified and identified. The use of two biometric systems. Signature verification implies determining if the claimed person is the real genuine person, whereas signature identification determines whether the person's existence exists in the supplied database. The biometric system is based on precise facts concerning distinct biological features. As a result, it checks or identifies the claimed users. Biometric identifiers are commonly used. There are two types of classifications: behavioral and physiological. Physiological characteristics are the physical qualities of the body, such as fingerprints and facial features.

DNA, recognition, and so on while behavioral traits, such as voice and movement, are tied to a person's pattern of behavior for example, automatic offline Signature authentication and verification systems are in a class by themselves. Methods for automated identification. Handwritten signatures are durable and are used to verify identification. They are used to obtain approval for bank-related tasks and transactions, paving the door for criminal fraud. Hence Access to such sites requires administrative sectors utilize it as a legal means of authenticating an individual's identification.

PROBLEM STATEMENT

Develop an image processing-based signature verification system that can accurately distinguish between genuine and forged signatures. The system should take a scanned image of a signature as input and employ advanced image processing techniques, such as feature extraction and pattern recognition, to analyze the signature's key characteristics. The goal is to establish a reliable and efficient method for authenticating signatures, ensuring its potential applications in various domains, such as banking, legal documents, and personal identification. The system should be robust enough to handle variations in writing styles, different pen types, and varying image qualities while maintaining a low false acceptance rate and false rejection rate.

LITERATURE SURVEY

TOWARDS AUTOMATED TRANSACTIONS BASED ON THE OFFLINE HANDWRITTEN SIGNATURES.

AUTHORS: Ekladious, George & Granger, Eric.

ABSTRACT:

Internet business transactions over the Internet rely on digital signatures, an Automated signature verification. Signatures might vary depending on who owns them. Genuine or? Verifications are performed based on user characteristics that cannot be altered or remodeled. Because signature verification is physiologically tied to a certain individual, it is useful. A digitalized system might aggravate the issue of technological obsolescence. When a person is unconscious, a signature is more difficult to fake than a fingerprint. The technique and elements of a handwritten signature are complex. Financial and replacement of conventional handwritten signatures in paper-based processes. Although they guarantee data integrity and authenticity, digital signatures are not as convenient to users as the manuscript ones. In this paper, a methodology is proposed to produce digital signatures using offline hand-written signatures. This methodology facilitates the automation of business processes, where users continually employ their handwritten signatures for authentication. Users are isolated from the details related to the generation of digital signatures yet benefit from enhanced security. First, signature templates from a user are captured and employed to lock his private key in a fuzzy vault. Then, when the user signs a document by hand, his handwritten signature im- age is employed to unlock his private key. The unlocked key produces a digital signature that is attached to the digitized document. The verification of the digital signature by a recipient implies authenticity of the manuscript signature and integrity of the signed document. Experimental results on the Brazilian offline signature database (that includes various forgeries) confirms the viability of the proposed approach. Private keys of 1024-bits were unlocked by signature images with an Average Error Rate of about 7.8%.

NEW SIGNATURE VERIFICATION TECHNIQUE BASED ON A TWO-STAGE NEURAL NETWORK CLASSIFIER

AUTHORS: Baltzakis, H. & Papamarkos, Nikos.

ABSTRACT:

This study describes a novel method for offline signature identification and verification. The suggested system is built on global, grid, and texture characteristics. A unique two-stage Perceptron OCON (one-class-one-network) classification framework has been created for each of these feature sets. In the first stage, the classifier combines the neural network judgement outputs with the Euclidean distance

calculated using the three feature sets. The first-stage classifier's output is sent into a second-stage radial basis function (RBF) neural network structure, which produces the final judgement. The entire system was thoroughly tested, resulting in excellent identification and verification rates.

DYNAMIC SELECTION OF GENERATIVE- DISCRIMINATIVE ENSEMBLES FOR OFF-LINE SIGNATURE VERIFICATION

AUTHORS: Batista, Luana & Granger, Eric.

ABSTRACT:

In practice, each writer only offers a limited number of signature samples for the purpose of designing a signature verification (SV) system. This study proposes hybrid generative-discriminative ensembles of classifiers (EoCs) to create an off-line SV system from few data, with the classifier selection procedure conducted dynamically. Multiple discrete left-to-right Hidden Markov Models (HMMs) are trained using a varying number of states and codebook sizes to construct the generative stage, allowing the system to learn signatures at different levels of perception. HMM likelihoods are assessed for each training signature and integrated into feature vectors that are utilized to train a diverse pool of two-class classifiers using a specialized Random Subspace Method to build the discriminative step. A novel dynamic selection technique based on the K-nearest-oracles (KNORA) algorithm and Output Profiles picks the most accurate EoCs to categorize a particular input signature during verification. This SV system is suited for learning new signature samples incrementally. Experiments with real-world signature data (including genuine samples as well as random, simple, and skilled forgeries) show that the proposed dynamic selection strategy can significantly reduce overall error rates when compared to other EoCs formed using well-known dynamic and static selection strategies. Furthermore, the performance of the SV system suggested in this research outperforms or is equal to that of equivalent systems discovered in the literature.

A COMPREHENSIVE STUDY ON OFFLINE SIGNATURE VERIFICATION

AUTHORS: Neha Sharma, Sheifali Gupta and Puneet Mehta

ABSTRACT:

Handwritten signatures are a sort of behavioral biometric that is utilized in a variety of applications including banks, credit cards, passports, cheque processing, and financial paperwork, among others. Verifying these signatures is a difficult undertaking, especially when they are signed offline and no information about the signing procedure is available. To eliminate the possibility of theft or fraud, a system that can distinguish between real and faked signatures is required. Many different sorts of studies have been conducted in this field throughout the previous three decades. Previously, this work was accomplished by handmade features, and more recently, deep learning approaches have been used for this purpose, although there is still room for improvement in the system's accuracy. In this article, we give a complete examination of the work done in the subject of offline signature verification, as well as the obstacles that remain in this area.

A BIOMETRIC-BASED VERIFICATION SYSTEM FOR HANDWRITTEN IMAGE- BASED SIGNATURES USING AUDIO TO IMAGE MATCHING

AUTHORS: Abdulaziz Almehmadi

ABSTRACT:

Signing a document or a check by hand or using a saved image-based signature is recognized as an acceptable technique for the signer's authentication and authorization. Signature forging, on the other hand, has improved to the point that it may be done expertly, unskillfully, or randomly forging a signature. A situation like this makes it difficult to validate and approve utilizing signatures properly. In this paper, a verification method for handwritten image-based signatures is presented to determine if the image-based signature is legitimate or counterfeit. The system compares the live stream of an audio-based signature to the image-based signature under consideration and delivers the match results.

Matching is accomplished by categorization and/or correlation of the two signatures. If a comparable class or a score above a pre- defined threshold is found, the image-based signature is validated as legitimate; otherwise, it is labelled as fabricated. The experiment included a total of 20 participants, each of whom submitted an authentic signature and faked four other signatures in various contexts. In a double- blind test, the system detected fake vs real signatures with 95% accuracy using a one- class SVM and 100% accuracy using a correlation coefficient.

A SURVEY ON SIGNATURE VERIFICATION SYSTEM USING CNN & CNN

AUTHORS: Robin Nadar, Heet Patel, Abhishek Parab, Akhilesh Nerurkar, Ruchi Chauhan

ABSTRACT:
The most basic and often used technique of validating a person's profile and/or identity is handwritten signature verification. As a result, the objective of this article is to provide an accurate overview of the numerous signature verification systems currently on the market, as well as the various signature databases that may be utilized for training and testing reasons. We also evaluated a number of methods and algorithms that can and are commonly utilized for the construction of Signature Verification Systems. We also conducted a comparison of the accuracy and efficiency of the assessed systems and Signature datasets, as well as their numerous disadvantages.

KEY WORDS: Signature verification system, CNN, SNN, CNN & SNN, Convolutional, Siamese, Neural Networks, Deep Learning.

METHODOLOGIES

- **SIGNATURE PRE- PROCESSING**

The preprocessing stage is used for both already stored signatures in the database and signatures that are to be tested. The goal of this phase is to normalize the signature in one form and increase the picture quality acceptable for feature extraction. The phases of preprocessing include.

- **BINARIZATION**

The binarization of gray scale signatures involves adaptive thresholding, which calculates a threshold value for different signatures. The method computes an intensity gradient for each pixel element, comparing it to the threshold value. The signature pixel intensity is set to 1 for higher intensity values and 0 for lower values.

- **COMPLEMENTATION**

Complementation of binarized signatures converts zeros and ones into ones, improving visibility and identifying fine details. This helps classify signatures as genuine or forged and enhances clarity for further operations.

- **FEATURE EXTRACTION**

Selecting the right feature for signature verification can be challenging. Our work extracts feature from signature images as vectors of seven entities, including entropy and closed loop number, for precise authentication and verification.

Feature	Origina l	Original	Forged	Forged
Autocorrelation	62.9267	62.8221	62.857 5	62.787 6
Contrast	0.1208	0.0988	0.0605	0.0588
Correlation	0.755	0.7857	0.8712	0.8735
Correlation	0.755	0.7857	0.8712	0.8735
Cluster Prominence	38.1143	28.3666	33.220 6	29.477 1
Cluster Shade	-5.4083	-4.5291	-5.1067	-4.7728
Dissimilarity	0.0532	0.053	0.0397	0.0411
Energy	0.9274	0.9113	0.9186	0.9101
Entropy	0.2818	0.324	0.2936	0.3161
Homogeneity	0.9819	0.9798	0.9834	0.9823
Homogeneity	0.9798	0.978	0.9822	0.9812
Maximum probability	0.963	0.9546	0.9584	0.9539
Sum of squares: Variance	62.7398	62.6244	62.640 6	62.57

FIG 1: Extracted features from sample signatures.

PROPOSED SYSTEM

Signature verification is a crucial task in many applications, such as banking, legal documents, and personal identification. Traditional methods of manual signature verification can be time-consuming and error prone. To overcome these limitations, we propose a robust and efficient signature verification system that leverages image processing techniques and Python programming. Our system aims to automate the signature verification process, improving accuracy and speed while reducing human intervention.

- Data Collection and Preprocessing
- Model Development
- Data Split and Model Evaluation
- Thresholding and Decision Making

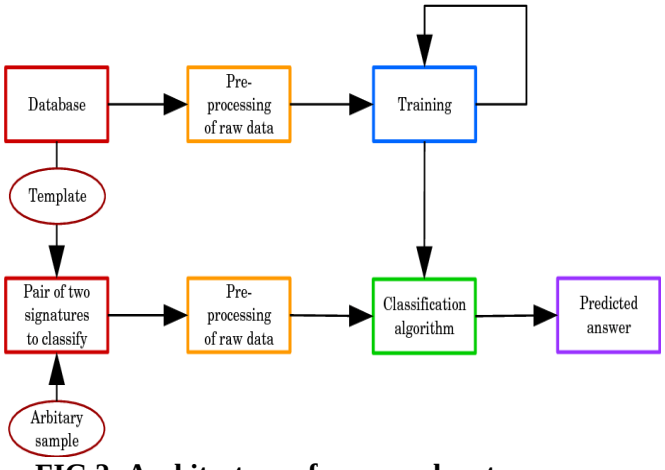

FIG 2: Architecture of proposed system

PYTHON

Python is a flexible and user-friendly programming language noted for its clean and clear syntax. It's extensively utilized in a variety of industries, including web development and data analysis, as well as artificial intelligence and automation. Python, with its extensive library collection and active community, makes it easier to convert ideas into practical code. Its ease of use and broad application make it a good choice for both novice and professional programmers.

TECHNOLOGY

- **RANDOM FOREST CLASSIFIER**

A Random Forest Classifier is a popular machine learning algorithm used for both classification and regression tasks. It is an ensemble learning method that combines the predictions of multiple decision trees to improve accuracy and robustness. The "forest" in Random Forest comes from the fact that it consists of a collection of individual decision trees, where each tree is trained on a different subset of the data.

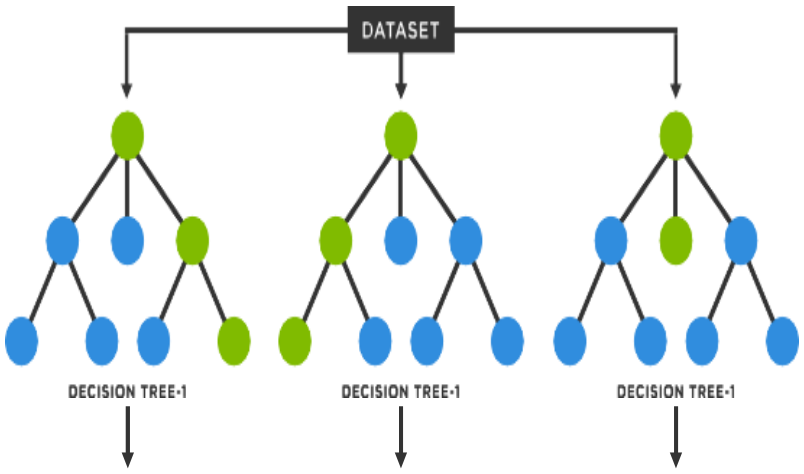

FIG 3: Random Forest Classifier workflow

- **NUMPY**

NumPy, which stands for "Numerical Python," is a sophisticated open-source Python library that supports massive, multi- dimensional arrays and matrices, as well as a wide number of mathematical functions for working with these arrays. It's a core Python package for scientific computing that's frequently used in domains including data analysis, machine learning, artificial intelligence, and numerical simulations.

- **PANDAS**

Pandas is an open-source Python package that provides structured data manipulation and analysis tools. "Pandas" is an abbreviation for "Python Data Analysis Library." Wes McKinney created it, and it was initially published in 2009.Pandas is extensively used in data science, machine learning, and other analytical domains because of its capacity to effectively manage and modify many types of data. The series and data frame data structures are introduced in the library. A Series is a one-dimensional array-like structure that may carry a variety of data kinds, including numbers, strings, and even more complicated things. Each element in a Series has an associated label called an index, which allows for quick and labelled data retrieval. A Data Frame is a two-dimensional table- like structure made up of rows and columns. It's a collection of Series objects, with each column representing a Series. Data Frames are

extremely adaptable and can handle a wide range of data formats. They are frequently used to work with tabular data such as CSV files, Excel spreadsheets, SQL tables, and other formats.

- **SCIKIT-LEARN**

Scikit-learn, sometimes known as sklearn, is a popular open-source machine learning package written in Python. It includes a variety of tools and methods for performing different machine learning tasks such as classification, regression, clustering, dimensionality reduction, model selection.

CONCLUSION

We present an automatic online 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 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 classifier. In addition, it is a promising research topic to investigate how to use fewer reference signatures for verification and still get a reasonable result. Incorporating image processing techniques within a Python environment for signature verification provides a versatile and customizable solution. While the process involves several technical steps, the potential benefits in terms of fraud prevention, security enhancement, and efficiency make it a valuable endeavor for organizations and individuals alike. As technology advances and machine learning techniques improve, signature verification systems are likely to become even more accurate and reliable, contributing to a safer digital landscape.

REFERENCES

[1]. M. Ammar, Y. Yoshida and T. Fukumura, A new executive 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 classifier, 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 Recognition. 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 Recognition. 1 (2005) 886–893. [5]. D. Doermann and A. Rosenfeld, Recovery of temporal information from static images of handwriting, Int. J. Comput. Vision 15(1–2) (2001) 143–164.

[6]. G. S. Eskander, R. Sabourin and E. Granger, Dissimilarity representation for handwritten signature verification, in 2nd Int. Workshop on Automated Forensic Handwriting Analysis (AFHA) (2013), pp. 26–30.

[7]. G. S. Eskander, R. Sabourin and E. Granger, A dissimilarity-based approach for biometric fuzzy vaults-application to handwritten signature images, Int. Workshop on Emerging Aspects in Handwritten Signature Processing (ICIAP 2013, Springer Verlag, Berlin, Germany), pp. 95–102.

[8]. G. S. Eskander, R. Sabourin and E. Granger, towards automated transactions based on the online handwritten signatures, in 9th Int. Conf. Machine Learning and Data Mining (MLDM), (Springer Verlag, Berlin, Germany, 2013), pp. 141–150.

[9]. G. S. Eskander, R. Sabourin and E. Granger, On the dissimilarity representation and prototype selection for signature-based bio-cryptographic systems, in 2nd Intel Workshop on Similarity- Based Pattern Analysis and Recognition (SIMBAD) (Springer Verlag, Berlin, Germany, 2013), pp. 265–280.

[10]. G. S. Eskander, R. Sabourin and E. Granger, improving signature-based biometric cryptosystems using cascaded signature verification-fuzzy vault (SV-FV) approach, in the 14th Int. Conf. Frontiers in Handwriting Recognition (ICFHR) (Institute of Electrical and Electronics Engineers Inc., New Jersey, USA, 2014), pp. 187–192.

[11]. G. S. Eskander, R. Sabourin and E. Granger, Online signature-based fuzzy vault (OSFV): Review and new results, arxiv:1408.3985.

[12]. 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.

[13]. Z. Fu, X. Sun, Q. Liu, L. Zhou and J. Shu, achieving efficient cloud search services: Multikey word ranked search over encrypted cloud data supporting parallel computing, IEICE Trans. Commun. E98-B(1) (2015) 190–200.

[14]. B. Gu, V. S. Sheng, K. Y. Tay, W. Romano and S. Li, Incremental support vector learning for ordinal regression, IEEE Trans. Neural Netws. Learn. Syst. 26(7) (2015) 1403–1416.

[15]. B. Gu, V. S. Sheng, Z. Wang, D. Ho, S. Osman and S. Li, Incremental learning for support vector regression, Neural Netws. 67 (2015) 140–150.

[16]. Y. Guerbai, Y. Chibani and B. Hadjadji, the executive use of the one-class SVM classifier for handwritten signature verification based on writer-independent parameters, Pattern Recognition 48(1) (2015) 103–113.

[17]. J. Guo, D. Doermann and A. Rosenfeld, Forgery detection by local correspondence, Int. J. Pattern Recognition. Artif. Intell. 15(4) (2001) 579–641.

[18]. A. Hamadene, Y. Chibani and H. Nemmour, online handwritten signature verification using contourlet transform and cooccurrence matrix, in Int. Conf. on Frontiers in Handwriting Recognition (ICFHR), (IEEE Computer Society, Washington, USA, 2012), pp. 343–347. [19]. J. Hu and Y. Chen, Fusion of features and classifiers for online handwritten signature verification, in Asian Conf. Pattern Recognition (IEEE Computer Society, Washington, USA, 2011), pp. 174–178.